Sommaire

Remerciements

Je tiens à remercier particulièrement le « Comité des sages » que j'avais constitué, composé d'éminentes personnalités (dont les noms suivent), expertes sur ce thème, et qui m'a apporté compétence et expérience.

M. Roger **Baleras**, ancien directeur des applications militaires du CEA.

M. Jean-Paul **Gillybœuf**, IGA, chargé de mission pour la mise en place d'une direction générale des systèmes d'information et de communication au ministère de la Défense.

M. Michel **Lacarrière**, directeur de l'administration centrale honoraire.

M. Jean **Rannou**, général.

M. Dominique **Roux**, professeur à l'université de Paris Dauphine.

M. Jacques **Stern**, professeur à l'École normale supérieure ULM, directeur du département informatique.

M. Jean-Pierre **Vuillerme**, directeur des services environnement et prévention du groupe Michelin.

Je voudrais également remercier les membres du groupe de travail qui ont participé activement à la réalisation de ce rapport. Leur disponibilité, leur compétence technique et leur détermination ont été un atout précieux.

Enfin, je tiens à remercier les personnalités, les administrations, les entreprises et les organisations qui ont bien voulu apporter leur contribution lors des auditions ou des échanges nombreux et fructueux.

Avertissement

Les noms des sociétés citées, en particulier dans le chapitre III du présent rapport, le sont à titre exclusivement indicatif et ne sont en aucune manière une recommandation de l'auteur.

Introduction

Les systèmes d'information font désormais partie intégrante du fonctionnement des administrations publiques, de l'activité des entreprises et du mode de vie des citoyens. Les services qu'ils assurent nous sont tout aussi indispensables que l'approvisionnement en eau ou en électricité.

La communication, qui occupe une place de choix dans nos sociétés contemporaines à la recherche d'une productivité sans cesse croissante, nécessite la maîtrise de l'information économique, sociale et culturelle. L'explosion mondiale d'Internet a considérablement modifié la donne et conféré aux systèmes d'information une dimension incontournable au développement même de l'économie et de la société.

C'est dire si la sécurité des systèmes d'information (SSI) est un enjeu à l'échelle de la Nation tout entière.

Les États-Unis ont parfaitement saisi, et ce depuis longtemps, tout l'intérêt stratégique et politique d'un contrôle absolu de l'information. L'objectif de l'« information dominance » est sans équivoque. « L'aptitude à prendre connaissance des communications secrètes de nos adversaires tout en protégeant nos propres communications, capacité dans laquelle les États-Unis dominent le monde, donne à notre nation un avantage unique » [1].

Pour l'État il s'agit d'un enjeu de souveraineté nationale. Il a, en effet, la responsabilité de garantir la sécurité de ses propres systèmes d'information, la continuité de fonctionnement des institutions et des infrastructures vitales pour les activités socio-économiques du pays et la protection des entreprises et des citoyens.

De leur côté, les entreprises doivent protéger de la concurrence et de la malveillance leur système d'information qui irrigue l'ensemble de

1. L'executive order 12333 du 4 décembre 1981. « The ability to understand the secret communications of our foreign adversaries while protecting our own communications, a capability in which the United States leads the world, gives our nation a unique advantage ». *Traduction de courtoisie*.

leur patrimoine (propriété intellectuelle et savoir-faire) et porte leur stratégie de développement.

L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'ouverture des réseaux et leur complexité croissante associant des acteurs aux multiples profils, ont renforcé la vulnérabilité des systèmes d'information.

Détruire, altérer, accéder à des données sensibles dans le but de les modifier ou de nuire au bon fonctionnement des réseaux : les motivations sont diverses et fonction de la nature des informations recherchées et de l'organisme visé.

Quelles formes prennent les attaques ? De qui émanent-elles ? Quelle est leur finalité ?

Tous les utilisateurs identifient au quotidien la menace constante des virus et des vers qui submergent Internet. Leur nombre a explosé au cours de ces dernières années et ceux-ci deviennent de plus en plus sophistiqués. Les outils nécessaires aux pirates sont aisément accessibles en ligne et il existe un échange constant d'information et de savoir-faire au sein de la communauté des pirates pour rendre ces attaques de plus en plus efficaces. Cependant, leur désir de performance cède de plus en plus le pas au développement d'entreprises criminelles dont les activités en ligne se sont accrues parallèlement à la dimension économique d'Internet. Le nombre de fraudes se traduit chaque année par des coûts s'élevant à des milliards d'euros, en particulier pour les banques et les entreprises.

En tant qu'outil de propagande et de communication, les réseaux terroristes utilisent déjà largement Internet. Plus la lutte contre le terrorisme verrouille les lignes traditionnelles de communication, plus ces réseaux trouvent l'accessibilité et l'anonymat d'Internet attrayants.

S'il n'y a jamais eu officiellement de cyber-attaque majeure motivée par des considérations politiques ou terroristes contre des systèmes d'information, rien ne permet d'exclure pour autant qu'une telle attaque ne se produira pas. Susceptibles d'affecter un système d'information critique, les attaques ou les incidents majeurs pourraient avoir de graves répercussions, notamment sur les infrastructures qui fournissent des services à l'ensemble de la société.

L'espionnage d'État ou industriel visant à intercepter des informations d'adversaires ou de concurrents constitue une autre pratique. Au-delà de la dimension offensive propre aux agences de sécurité gouvernementales, les atteintes au secret industriel sont de plus en plus systématisées. Le vol des secrets commerciaux est, lui aussi, en constante augmentation. Il représentait aux États-Unis, en 2001, un préjudice de 59 milliards de dollars aux mille premières entreprises américaines. L'exemple le plus spectaculaire porte sur la révélation [1], en juin 2005, des agissements d'une entreprise israélienne qui « louait »

1. http://solutions.journaldunet.com/0506/050603_espionnage_industriel_israel.shtml

un cheval de Troie [1] à ses clients ; une affaire qui a conduit à l'arrestation de plusieurs dirigeants d'entreprises à travers le monde. En s'adressant à cette société, un client demandait tout simplement à ce que le produit soit installé dans le système d'information de la cible, pour en extraire en toute impunité toutes les informations qu'il désirait.

L'analyse des menaces constitue la première partie du rapport. Le caractère fortement évolutif de l'objet de l'étude appellerait une actualisation permanente.

La deuxième partie présente les dispositions prises aujourd'hui par les différents acteurs afin d'assurer la sécurité de leur système d'information, et apporte des indications sur leur niveau de protection et leur sensibilité aux enjeux de sécurité. Un examen sans détour est fait de l'organisation et du pilotage de ces questions sensibles au niveau gouvernemental, des différents ministères et des grandes entreprises. Le champ d'étude a été élargi à d'autres pays et à des organisations internationales.

Cette étape de l'analyse a permis d'identifier certains points sensibles sur lesquels le présent rapport attire l'attention et qui permettent de tracer des pistes d'action destinées à améliorer la SSI dans notre pays. Elle montre en effet, au-delà d'une très forte disparité et d'un manque de coordination ente les acteurs publics et privés, la nécessité pour l'État d'une adaptation nouvelle et urgente, dans la logique de l'État stratège.

Les préoccupations de souveraineté nationale et de performance économique de la France ont conduit enfin à s'interroger sur la maîtrise des moyens informatiques nécessaires à la mise en œuvre d'une SSI efficace et, partant, à s'intéresser au secteur économique qui les produit. Le rapport évalue le positionnement de la France sur le marché mondial de la SSI et esquisse des orientations pour renforcer notre tissu d'entreprises dans un domaine à forte valeur ajoutée pourvoyeur d'emplois hautement qualifiés.

La sécurité des systèmes d'information est un véritable défi, à la fois technologique et économique.

Si l'effort pour améliorer la sécurité des systèmes d'information représente incontestablement un coût, il est sans commune mesure avec des investissements traditionnels de défense consentis par le pays. La préservation de notre indépendance est à ce prix. C'est un exercice réel d'un « patriotisme économique » retrouvé, nécessaire pour créer les conditions favorables à l'instauration d'une économie de confiance dans la société de l'information.

1. Cheval de Troie : programme qui exécute des instructions sans l'autorisation de l'utilisateur, instructions qui lui sont généralement nuisibles en communiquant par exemple à l'extérieur. Il prend l'apparence d'un programme valide mais il contient en réalité une fonction illicite cachée, grâce à laquelle il contourne les sécurités informatiques. Il pénètre ainsi par effraction dans les fichiers de l'utilisateur pour les modifier, les consulter ou même les détruire. Le cheval de Troie, contrairement au ver, ne se réplique pas et il peut rester inoffensif pendant quelques jours, semaines ou mois et se mettre en action à la date programmée.

Enfin, au moment où l'ensemble des forces vives de la Nation se mobilise pour l'emploi, la protection du patrimoine et de la compétitivité de nos entreprises par la SSI concourt directement à la préservation et au développement de nos emplois.

Synthèse

Sécurité des systèmes d'information Un enjeu majeur pour la France

Pour les besoins de ce document, on appelle « système d'information (SI) » un ensemble de machines connectées entre elles de façon permanente ou temporaire permettant à une communauté de personnes physiques ou morales d'échanger des données (sons, images, textes, etc.). Selon cette définition, des systèmes aussi variés que le réseau d'un opérateur de téléphonie, le site Internet d'un ministère, l'ordinateur individuel du particulier ou le réseau de commandement des forces armées sont des systèmes d'information.

Une menace qui doit être prise au sérieux

L'information gérée par les systèmes d'information fait l'objet de convoitises. Elle peut être exposée à des attaques qui exploitent des éléments vulnérables du système d'information. La sécurité des systèmes d'information a pour objet de contrer ces menaces par des mesures proportionnées aux risques pouvant peser sur la confidentialité de l'information, son intégrité, sa disponibilité ou la possibilité d'en authentifier la source et de la signer.

Les attaques sont une réalité. Les plus médiatisées sont les virus, vers, *phising*, *spyware*, ou les défigurations de site Web. Autrefois imputables à quelques agitateurs, elles sont désormais le fait d'organisations criminelles organisées avec des finalités notamment financières.

L'organisation (recours à l'externalisation, absence de classification des informations...), la faiblesse des acteurs humains (inconscience, insouciance, naïveté), les réseaux de communication (risques de saturation, d'interception...), les logiciels dont la complexité croissante est

source d'erreurs difficiles à détecter, ou les composants matériels, sont autant de sources de vulnérabilités.

Le risque peut être quantifié : il est fonction de la valeur attachée aux informations manipulées, de l'importance des vulnérabilités et de la probabilité d'exploitation de ces vulnérabilités par un attaquant.

Pour un système donné, le risque peut être réduit en limitant la sensibilité des informations qu'il manipule, en réduisant la vulnérabilité de chaque entité du système et en multipliant les éléments de défense convenablement architecturés pour compliquer la tâche des attaquants potentiels. Il est également nécessaire de mettre en œuvre une politique de sécurité applicable à l'ensemble des entités d'un domaine géographique ou fonctionnel, qui regroupe l'ensemble des règles et des recommandations à appliquer pour protéger les ressources informationnelles.

Les citoyens, les entreprises, le monde académique, les infrastructures vitales et l'État lui-même sont des cibles. Compte tenu de l'interconnexion entre les réseaux, ces cibles sont de plus en plus interdépendantes. Il importe donc de se préoccuper de la sécurité de tous les acteurs.

Les réponses organisationnelles et techniques

Aux côtés d'un acteur dédié, le SGDN, d'autres acteurs publics interviennent dans le secteur de la SSI.

Au sein du **SGDN** [1], la **DCSSI** [2] est chargée d'organiser les travaux interministériels et de préparer les mesures que le Secrétaire général de la Défense nationale propose au Premier ministre ; elle prépare les dossiers en vue des autorisations, agréments, cautions ou homologations, et en suit l'exécution ; elle met en œuvre les procédures d'évaluation et de certification ; elle participe aux négociations internationales ; elle assiste les services publics dans le domaine de la SSI (conseil, audit, veille et alerte sur les vulnérabilités et les attaques, réponse aux incidents) ; elle assure la formation des personnels qualifiés dans son centre de formation (CFSSI).

La DCSSI mène également des inspections dans les systèmes d'information des ministères. Aux dessus du CERTA [3], elle a mis en place un centre opérationnel de la sécurité des systèmes d'information (COSSI), activé en permanence et chargé d'assurer la coordination interministérielle des actions de prévention et de protection face aux attaques sur les systèmes d'information. Elle a également mis en place un nouveau label ainsi qu'une cellule chargée d'entretenir des relations avec le tissu des entreprises de SSI.

1. Secrétariat général de la défense nationale.
2. Direction centrale de la sécurité des systèmes d'information.
3. Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques.

L'effectif de la DCSSI est d'une centaine de personnes, en majorité de formation scientifique et technique. Les auditions menées ont montré en particulier que :
– la faiblesse de l'effectif conduit à limiter la capacité d'inspection de la DCSSI à seulement une vingtaine de déplacements par an sur site, ce qui est insuffisant ;
– son rôle de conseil aux entreprises est insuffisamment développé et se révèle peu en phase avec les attentes du monde économique ;
– les formations du CFSSI [1], considérées comme de très grande qualité, sont malheureusement réservées aux personnels de l'administration exerçant directement dans le domaine de l'informatique ou de la SSI et souffrent d'un manque de notoriété.

Le ministère de la Défense est un acteur important pour les produits gouvernementaux de haut niveau de sécurité. Il est maître d'œuvre des équipements ou moyens destinés à protéger les systèmes d'information gouvernementaux. Il a également la capacité d'apporter son concours aux contrôles et mesures que peuvent nécessiter les systèmes d'information en service dans les départements civils. Enfin, il est chargé de doter l'État des équipes et laboratoires de mesures propres à satisfaire l'ensemble des besoins gouvernementaux. En outre la Direction générale de la sécurité extérieure (DGSE), rattachée au ministère de la Défense, apporte sa connaissance des menaces étrangères sur les systèmes d'information. La Direction de la protection et de la sécurité de la défense (DPSD) assure de son côté une veille sur la sécurité des industries de défense.

Le ministère de l'Économie, **des Finances et de l'Industrie** a pour mission l'animation du développement industriel d'équipements de sécurité non-gouvernementaux. Le service des technologies et de la société de l'information (STSI) de la direction générale des entreprises (DGE) du ministère a un bureau du multimédia et de la sécurité qui suit le domaine SSI et finance des projets SSI au travers des appels à projets Oppidum. Enfin, comme pour les autres domaines technologiques, le MinEFI contribue au financement de l'innovation dans les PME par divers mécanismes d'aide, en particulier le crédit impôt-recherche, et au travers d'OSEO-ANVAR dont il assure la tutelle.

L'ADAE [2] assure la maîtrise d'ouvrage des services opérationnels d'interconnexion et de partage des ressources pour l'administration électronique, dont le volet sécurité regroupe toutes les activités nécessaires à la mise en place de l'infrastructure de confiance (outils, référentiels, guides méthodologiques et expertise). Alors que la SSI est une composante importante de ce type de projets, la DCSSI n'est pas citée dans le décret instituant l'ADAE.

Le ministère de l'Intérieur est chargé de la lutte contre la cyber-criminalité. Dans le cadre de ses missions, la Direction de la surveil-

1. Centre de formation à la sécurité des systèmes d'information.
2. Agence pour le développement de l'administration électronique, rattachée au ministre chargé du Budget et de la réforme de l'État.

lance du territoire (DST) assure des prestations techniques et informatiques autour de trois volets : la prévention, la répression et la sécurité informatique. L'OCLCTIC [1] est une structure à vocation interministérielle placée au sein de la Direction de la police judiciaire (DCPJ). Elle lutte contre les auteurs d'infractions liées aux TIC, enquête à la demande de l'autorité judiciaire, centralise et diffuse l'information sur les infractions à l'ensemble des services répressifs. La Police parisienne dispose d'un service similaire, le BEFTI.

La CNIL, en matière de sécurité des systèmes d'information, s'intéresse essentiellement à la protection des données personnelles. La loi du le 6 août 2004 lui donne une mission de labellisation de produits et de procédures. La CNIL a un pouvoir d'imposer que n'a pas la DCSSI. La CNIL et la DCSSI ont commencé à travailler ensemble.

La multiplication des acteurs publics, dont les missions se chevauchent et dont les textes fondateurs sont peu précis, donne une impression générale de confusion et d'éparpillement des moyens et des hommes. Dans cette nébuleuse, l'acteur public dédié, le SGDN et plus précisément la DCSSI, souffre d'un manque d'autorité et parfois de crédibilité auprès des publics concernés. Ces deux facteurs, l'éparpillement des moyens et le manque d'autorité du SGDN, nuisent à l'efficacité de l'État dans la définition et la mise en œuvre de la politique globale de SSI.

De plus, les disparités dans la mise en œuvre d'une organisation type, au sein de l'administration, des difficultés à mobiliser les ressources nécessaires et l'absence d'autorité des acteurs de la SSI, peuvent rendre cette organisation inopérante. Face aux difficultés de recrutement de personnels, des ministères sont conduits à recourir à l'externalisation. Il est fréquent de constater que les services informatiques ne suivent pas les recommandations des HFD [2] lors de choix de solutions pour des applications sensibles, sous couvert d'une stricte application du code des marchés publics. Toutefois certains ministères ont mieux intégré la problématique SSI et s'appuient sur des équipes compétentes et motivées.

Une analyse comparative de l'organisation, du budget consacré à la SSI, de l'existence de schémas directeurs opérationnels, de la classification des données sensibles et de la mise en place de chartes utilisateurs, effectuée dans cinq ministères, révèle une hétérogénéité pour chacun de ces domaines.

De plus, aucune politique « produits » globale n'existe dans le domaine de la SSI.

Le rapport analyse la situation de plusieurs pays (États-Unis, Royaume-Uni, Allemagne, Suède, Corée du Sud et Israël) et aborde les initiatives multilatérales (Union européenne, OCDE, ONU, G8, réseaux de veille et d'alerte). On ne retiendra dans cette synthèse que le cas de l'Allemagne.

1. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.
2. Haut fonctionnaire de défense.

L'Allemagne a adopté en juillet dernier un plan national pour la protection des infrastructures d'information (NPSI) qui s'appuie notamment sur l'homologue de la DCSSl, le BSI. Le BSI mène des actions de sensibilisation à destination des citoyens et des PME, analyse les tendances et les risques futurs ; il apporte une aide à la sécurisation des administrations mais aussi des entreprises (tenue à jour d'un standard professionnel de bonnes pratiques, conseils et support technique, tests d'intrusion, protection des infrastructures critiques) ; il analyse les risques, évalue et certifie des produits et donne l'autorisation des applications classifiées. Il participe au développement des produits et des technologies et joue un rôle actif dans les comités nationaux et internationaux de normalisation et de standardisation relatifs à la SSI.

Pour assurer l'ensemble de ces missions, le BSI emploie 430 personnes (contre 100 à la DCSSI) en croissance régulière depuis 2001. Il dispose d'un budget significatif de 51 millions d'euros en augmentation régulière depuis 2002. La part consacrée aux développements représente 19 % de ce budget (10 M€) et celle consacrée aux études 17 % (9 M€). Ces ressources sont sans commune mesure avec celles de la DCSSI.

Le système d'information de l'entreprise est désormais déployé dans un contexte d'entreprise étendue permettant un travail en réseau avec ses clients ou usagers, ses fournisseurs, ses donneurs d'ordre, ses partenaires ou les représentants de l'administration. Ces interconnexions génèrent des vulnérabilités nouvelles pour les systèmes d'information de l'entreprise. En outre, la généralisation des outils nomades (téléphones mobiles, PDA, ordinateurs portables...) et le passage au tout numérique gomment la frontière entre espace professionnel et espace privé, accentuant très significativement les risques. Les enquêtes montrent que de nombreux sinistres ont été identifiés, avec des incidences considérables sur la production, l'équilibre financier ou l'image des entreprises. De plus, des actions d'espionnage industriel peuvent se traduire par une perte de compétitivité avec une incidence négative sur l'emploi.

Cependant, sécuriser les systèmes d'information requiert de mobiliser des ressources financières et humaines dont le retour sur investissement est souvent difficile à justifier. Les PME ont notamment du mal, du fait de leur faible taille, à disposer des ressources nécessaires.

Si l'intégration de la SSI dans le modèle culturel de l'entreprise reste une exception, certaines grandes entreprises internationalisées montrent une maîtrise remarquable de la SSI : politique de sécurité imposée au plus au haut niveau, organisation efficace, sensibilisation et responsabilisation des personnels, choix d'architectures et d'équipements adaptés à la sécurisation des informations stratégiques, etc.

Les entreprises attendent de l'État des services de support efficaces et accessibles, comme un guichet unique pour les aider à résoudre leurs problèmes de SSI, des préconisations de produits de sécurité, un soutien spécifique lorsqu'elles sortent des frontières, etc. Divers organismes publics et privés ont élaboré à l'attention des entreprises d'excellents guides.

Base industrielle et technologique

Les États-Unis disposent d'une domination sans partage sur la plupart des segments du marché de la SSI. Pourtant, la sécurité des systèmes d'information est un enjeu national à caractère stratégique, politique et économique. Dans une logique de souveraineté, la France et l'Europe peuvent-elles aujourd'hui se doter des moyens d'assurer de manière autonome la protection de leurs infrastructures et de leurs systèmes ?

Les technologies de sécurité sont à la base du développement des produits et conditionnent ainsi directement la qualité de la SSI. La conception d'architectures de sécurité, l'ingénierie logicielle, la preuve de programmes et de protocoles et les méthodes d'évaluation, la cryptographie, les dispositifs électroniques de protection de secrets (cartes à puces...) et les méthodes applicatives de filtrage (antispam, antivirus...), de modélisation du comportement et de détection d'intrusions, sont globalement bien maîtrisées au niveau national contrairement aux systèmes d'exploitation et aux circuits intégrés sécurisés, technologies pourtant essentielles à la sécurité de la plupart des équipements. C'est sur elles que devrait porter un effort massif de recherche et de développement.

Quelques centres et instituts en France ont des activités orientées SSI, en logiciels ou matériels, pour certains de grande réputation. Toutefois l'absence de grands leaders industriels en France, une insuffisance de fonds publics dédiés et la contrainte des publications ne permettent pas à la recherche nationale en SSI d'être au niveau des meilleurs mondiaux.

Une coopération accrue avec des leaders étrangers présenterait des risques mais permettrait, dans le cadre de partenariats réellement équilibrés, de mettre les chercheurs français au contact de ces leaders.

Le marché de la SSI est en forte croissance mais reste de faible volume.

Le tissu industriel national en SSI est constitué de quelques grands groupes, souvent liés au marché de l'armement, d'intégrateurs, de nombreuses SSII de toutes tailles, d'une centaine de petites et moyennes entreprises, souvent à forte valeur technologique, qui peinent pour la plupart à survivre, et de leaders mondiaux dans le domaine de la carte à microprocesseurs. Cependant, l'offre nationale et européenne est éclatée. *Des actions visant au rapprochement de ces activités, en s'inspirant de ce qui a été fait dans la Défense et l'Aéronautique, deviennent impératives.*

Les politiques d'achat de l'État et des grands donneurs d'ordres ne sont pas favorables aux PME innovantes. À l'exception du pacte PME proposé par le Comité Richelieu en association avec OSEO-Anvar, il n'y a pas de réelle dynamique de la part des grands donneurs d'ordres.

Les PME de la SSI ne disposent pas des ressources suffisantes pour affronter la concurrence des offres étrangères. Elles ont des difficultés à financer leurs investissements, que ce soit en fonds propres (le sec-

teur n'attire pas les investisseurs nationaux) ou par des crédits bancaires. Il faudrait développer des fonds d'investissement spécifiques, adaptés à des entreprises de croissance modérée, à même d'assurer un financement stable sur une durée supérieure à 10 ans.

Le financement public de la R&D est insuffisant dans les TIC en général. Si différentes sources de financement existent, plus ou mois accessibles aux PME : l'Anvar, l'ANR (Agence nationale de la recherche), l'A2I (Agence de l'innovation industrielle), les ministères chargés de l'Industrie et de la Recherche et l'Union européenne, ces financements sont insuffisants et mal coordonnés.

Enfin, si l'environnement juridique et fiscal des entrepreneurs est en amélioration, il demeure perfectible.

Labellisation des produits de sécurité. La France fait partie des pays fondateurs des critères communs et des accords de reconnaissance mutuelle. Il est toutefois regrettable de constater que sa compétence et son expérience particulière (en particulier de ses centres d'évaluation) sont trop peu connues et reconnues à l'étranger.

– Une évaluation est conduite par un laboratoire privé, CESTI, agréé par la DCSSI.
– Le processus de certification est jugé trop long et trop coûteux par beaucoup d'industriels, a fortiori pour les PME.
– La qualification par la DCSSI est donnée à un produit qui a été évalué et certifié à partir d'une « cible de sécurité » qu'elle a approuvée au préalable. 10 produits ont déjà été qualifiés et 7 sont en cours de qualification. La moitié de ces produits est développée par des PME.
– L'agrément est l'attestation délivrée par la DCSSI qu'un produit de chiffrement est apte à protéger des informations classifiées de défense, après évaluation par le Celar et par la DCSSI. C'est un label national.

La normalisation facilite les choix stratégiques de l'entreprise, favorise la protection des consommateurs et l'application de la réglementation. La présence de la France dans la normalisation et la standardisation est notoirement insuffisante.

Une des voies pour faciliter l'acquisition des produits qualifiés est de donner à des profils de protection le statut de normes françaises homologuées. Le projet de convention entre la DCSSI et l'AFNOR pour mener à terme une action de normalisation est toujours en discussion. Il y faudrait une nouvelle impulsion.

Six recommandations

Les six recommandations proposées correspondent à une **double ambition : renforcer la posture stratégique de l'État en matière de TIC et de SSI et assurer la mise en œuvre opérationnelle des politiques et des décisions de l'État en matière de SSI.**

Axe 1. Sensibiliser et former à la sécurité des systèmes d'information

Organiser une grande campagne de communication s'inscrivant dans la durée à destination de tous.

• Mettre en place un portail Internet pour mettre à la disposition des utilisateurs – citoyens, administrations et entreprises – des informations d'actualité, des guides de bonnes pratiques, des contacts, des alertes sur les menaces...
• Proposer au système éducatif – du primaire à l'enseignement supérieur – et au système de formation continue, des canevas modulaires de formation en SSI.
• Informer l'utilisateur : à l'instar du port de la ceinture pour l'utilisation d'un véhicule automobile, imposer que la documentation utilisateur qui accompagne les produits personnels de communication mentionne les risques principaux encourus vis-à-vis de la protection des informations, les points de vigilance pour l'utilisateur et les recommandations types à mettre en œuvre (exemple : activer un pare-feu, protéger et changer régulièrement son mot de passe...)

Axe 2. Responsabiliser les acteurs

• Établir de manière obligatoire des chartes à l'usage des utilisateurs, annexées au contrat de travail – public et privé – ou aux règlements intérieurs des entreprises.
• Labelliser les entreprises fournisseurs de produits ou services de SSI qui respectent un cahier des charges à établir.

Axe 3. Renforcer la politique de développement de technologies et de produits de SSI et définir une politique d'achat public en cohérence

• Identifier les maillons des systèmes d'information qui exigent des produits qualifiés.
• Établir et tenir à jour un catalogue des produits de sécurité nationaux qualifiés et des produits européens adaptés aux différents niveaux de sécurité à assurer.
• Développer les financements publics de R&D.
• Favoriser le développement des PME innovantes dans la SSI et renforcer les fonds d'investissement en capital développement.
• Développer la politique de certification et de qualification par une augmentation des produits certifiés et qualifiés et une réduction des délais et des coûts de certification.
• Accroître la présence et l'influence française dans les groupes de standardisation et les comités de normalisation.
• Définir et mettre en œuvre une politique d'achat public, fondée sur le principe d'autonomie compétitive. Inciter les grandes entreprises à travers le pacte PME à faire confiance aux PME SSI.

Axe 4. Rendre accessible la SSI à toutes les entreprises

• Inciter les entreprises à assurer leur SSI par la mise en place d'aides publiques.
• Créer un centre d'aide et de conseil dans une logique de guichet unique.
• Diffuser aux PME, sous une forme adaptée, les informations de veille, d'alerte et de réponse disponibles au niveau des CERT nationaux.
• Initier et animer des forums thématiques public – privé favorisant la circulation d'informations, les retours d'expériences, le partage des bonnes pratiques...

Axe 5. Accroître la mobilisation des moyens judiciaires

• Reconnaître la spécificité des contentieux liés aux systèmes d'information.
• Aggraver les peines prévues au code pénal en matière d'atteinte à la SSI.
• Introduire une exception au principe d'interdiction de la rétro-conception dans le code de la propriété intellectuelle pour des motifs de sécurité.
• Assurer la sensibilisation des magistrats et des forces de sécurité par la formation initiale et continue.
• Constituer un pôle judiciaire spécialisé et centralisé de compétence nationale.
• Renforcer les coopérations internationales.

Axe 6. Assurer la sécurité de l'État et des infrastructures vitales

• Mettre à jour les politiques de SSI et les schémas directeurs de chaque ministère et les valider par une autorité centrale.
• Conseiller en amont les maîtrises d'ouvrage de l'État pour des projets sensibles tels que par exemple la carte nationale d'identité ou le dossier médical.
• Confier à une autorité centrale le rôle d'approuver formellement le lancement de ces projets sensibles.
• Faire contrôler par une autorité centrale l'application de ces prescriptions par des inspections sur site et des tests d'intrusion sans préavis.
• Mettre en place et animer une filière SSI transverse dans laquelle la mobilité sera organisée, tant à l'intérieur de la fonction publique qu'au travers de passerelles avec les entreprises et les centres de recherche.
• Définir les profils de postes des responsables SSI. Renforcer leur autorité et leur responsabilité ; ils devront être indépendants des directions des systèmes d'information.
• Pour les opérateurs d'infrastructures vitales : valider la politique de sécurité par l'autorité centrale et conduire des inspections et des tests d'intrusion ;
• Pour les entreprises sensibles, faire à la demande des audits et des tests d'intrusion.

* * *

Il est à noter que certaines recommandations du rapport rejoignent les mesures proposées dans le Plan de renforcement de la sécurité des systèmes d'information de l'État en 2004.

Un impératif : refondre l'organisation de la SSI de l'État

En complément aux six axes de recommandations, afin d'amener notre pays à un niveau plus élevé de sécurité et d'autonomie, il faut renforcer l'action de l'État et ses moyens humains et financiers en matière de SSI, rationaliser l'organisation des services de l'État et accroître la cohérence des actions des différents acteurs.

Le renforcement significatif des missions actuelles de la DCSSI qui en découlent, en particulier les plus opérationnelles, amène également à remettre en cause l'organisation mise en place en 1995 et qui ne semble plus adaptée aux enjeux actuels.

Il est ainsi proposé :

– de recentrer le dispositif étatique sous l'autorité du Premier ministre afin de garantir la mise en œuvre des axes stratégiques et d'assurer la dimension interministérielle du dispositif ;

– de séparer les fonctions opérationnelles des fonctions d'autorité :
• les fonctions d'autorité resteraient au sein du SGDN qui, pour le compte et sous l'autorité du Premier ministre, serait notamment en charge de l'élaboration de la politique nationale de la SSI, de la validation des politiques SSI des ministères et des organismes sous tutelle, d'évaluer les résultats de la mise en œuvre opérationnelle, d'assurer une veille stratégique sur l'évolution des risques, d'initier le renforcement de la dimension judiciaire et les actions interministérielles en matière de politique d'achat.
• à partir des fonctions opérationnelles de la DCSSI renforcées, une structure opérationnelle rattachée au Premier ministre, dédiée et centralisée, ayant une culture de résultats pourrait être mise en place.

Cette structure assurerait la mise en œuvre opérationnelle des politiques SSI et constituerait un centre d'expertises et de moyens au service des fonctions d'autorité. Constituées autour des équipes de l'actuelle DCSSI les ressources de la structure opérationnelle seraient renforcées par des compléments de ressources pluridisciplinaires permanentes et des apports d'expertises ponctuelles externes publiques ou privées.

La structure opérationnelle pourrait bénéficier d'un statut de type EPIC. Comme le BSI allemand, elle pourrait être dotée de principes de gouvernance garantissant la confiance, l'implication des personnels, la transparence et la neutralité, ainsi qu'être évaluée sur ses activités, notamment de support, de communication et de formation, selon des critères de performance et de qualité.

Chapitre 1

L'augmentation des menaces et des vulnérabilités pèse fortement sur la sécurité des systèmes d'information

Pour les besoins de ce document, on appelle **« système d'information »** un ensemble de machines connectées entre elles, de façon permanente ou temporaire et permettant à une communauté de personnes physiques ou morales d'échanger des données (sons, images, textes, etc.).

Selon cette définition, des systèmes aussi variés que le réseau d'un opérateur de téléphonie fixe ou mobile, le site Internet d'une entité (ministère, entreprise, institut de recherche, etc.), l'ordinateur individuel du particulier tout comme l'infrastructure de son fournisseur d'accès, le réseau de commandement des forces armées constituent des systèmes d'information.

Ainsi, une segmentation des systèmes d'information en trois sous-systèmes principaux permet de mieux appréhender les champs couverts et leur complexité (voir schéma en annexe IV) et en corollaire les enjeux de sécurité sous-jacents :

• Les réseaux informatiques :
– Internet et donc corrélativement toutes les applications ou services qui y sont associées (commerce électronique, banques en ligne...) et les équipements nécessaires à son fonctionnement (serveurs, routeurs...) ;
– les réseaux locaux d'entreprises et intra-entreprises ;
– les réseaux de l'État et des organisations publiques ;
– les réseaux des infrastructures critiques ;
– les équipements individuels des particuliers.

• Les réseaux de communication :
– les réseaux de satellites de communication ;
– les réseaux sans fil (Wimax, Wifi, Bluetooth...) ;
– les réseaux de localisation GPS ou Galileo ;
– les réseaux téléphoniques filaires ;
– les réseaux d'opérateurs de téléphonie mobile (GSM, GPRS, UMTS).

• Les réseaux de diffusion de télévision (TNT, câble) et de radio.
La disponibilité de nouveaux supports physiques de transmission ou l'optimisation de la bande passante sur ceux qui existent (modulations radioélectriques, câbles sous-marins, câbles optiques, satellites, multiplexage sur

la paire de cuivres, etc.) offrent de grandes possibilités techniques (amélioration des interconnexions, des débits, etc.).

Couplées à la standardisation et à l'utilisation étendue de certains protocoles de transmission (IP), ces possibilités font naître des « offres » de services qui rencontrent des « opportunités » d'application ou des « demandes » issues de nos modes de vie. Assez fréquemment, les opportunités ou les demandes sont motivées par des considérations économiques (réduction du coût de fonctionnement d'un service existant) et pratiques (gain de rapidité, de commodité pour ce service).

Ainsi :
– La dématérialisation des relations entre une administration et ses administrés en donne un bon exemple. L'utilisation et l'envoi électronique d'imprimés administratifs sur Internet permettent de réduire significativement les coûts de traitement des procédures manuelles (allégement de la masse salariale des agents publics). Dans le même temps, le traitement central et automatisé d'une procédure permet d'escompter un gain d'efficacité (statistiques et prévisions quasi-immédiate pour l'administration).
– Un programme d'armement visant à assurer un flux continu d'information entre un état-major de forces et des militaires œuvrant sur un théâtre d'opérations est à même de donner au commandement une visibilité totale et instantanée des actions et des mouvements entrepris par le fantassin sur le champ de bataille.
– Quant à l'ordinateur individuel connecté à Internet, il offre de nouveaux loisirs et un confort de vie : parcourir un supermarché virtuel, payer et se faire livrer à domicile la commande.

Les risques qui pèsent sur la sécurité des systèmes d'information sont fonction de la combinaison des menaces qui pèsent sur les ressources à protéger, des vulnérabilités inhérentes à ces ressources et de la sensibilité du flux d'information qui passe dans ces ressources.

Évaluer sa sécurité demande de savoir vers quoi on veut tendre et contre quoi on cherche à se protéger. Il apparaît que la sécurité des systèmes d'information s'apparente à de la gestion de risques.

Rappel des objectifs et de la politique de sécurité des systèmes d'information

Analyser et comprendre les menaces et les vulnérabilités nécessite au préalable de préciser deux éléments inhérents à la politique de sécurité :

– Il y a asymétrie entre les moyens de l'attaquant (sans limite) et ceux du défenseur (très contraint). Le défenseur doit tout imaginer sans pouvoir riposter (c'est le principe de la vision de Clausewitz) car il n'y a

pas de légitime défense en SSI [1] tandis que l'attaquant s'autorise tout ce qui est possible.

– La sécurité n'est pas une fin en soi mais résulte toujours d'un compromis entre :
· un besoin de protection ;
· le besoin opérationnel qui prime sur la sécurité (coopérations, interconnexions...) ;
· les fonctionnalités toujours plus tentantes offertes par les technologies (sans fil, VoIP...) ;
· un besoin de mobilité (technologies mobiles...) ;
· des ressources financières et des limitations techniques.

La sécurité n'a de sens que par rapport à ce qu'on cherche à protéger. Ici, la cible principale des convoitises est l'information, qu'il s'agisse de la manipuler ou de la détruire, de l'extraire ou d'en restreindre l'accès, voire de la rendre inaccessible. On peut également chercher à protéger des puissances de calcul, ou encore de la connectivité. La SSI a donc pour objet de proposer des solutions organisationnelles et/ou techniques susceptibles de protéger les informations les plus sensibles en priorité mais également les autres.

La gestion du risque et la SSI participent d'une même démarche globale, fondée sur l'identification des attaques potentielles, mais également sur l'idée qu'aucun système d'information n'est invulnérable car :
– il n'est pas possible d'envisager de se protéger à 100 % des codes malveillants (comme par exemple les virus ou les chevaux de Troie) ;
– les pare-feux protègent uniquement des attaques résiduelles (*i. e.* qui ne correspondent pas aux services offerts) [2] ;
– les algorithmes cryptographiques secrets ne sont pas tous fiables ;
– les solutions de détection d'intrusion peuvent être trompées ;
– la SSI repose sur des outils mais également sur un facteur humain ;
– il n'est pas possible de tester les systèmes et les applications dans des délais raisonnables au regard de leur déploiement auprès des utilisateurs.

La sécurité des systèmes d'information vise généralement cinq objectifs :
– **la confidentialité** : il s'agit de garantir que l'accès aux données n'est possible que pour les personnes dûment autorisées à les connaître ;
– **l'intégrité** : il s'agit de garantir que les fonctions et données sensibles ne sont pas altérées, et conservent toute leur pertinence ;
– **la disponibilité** : il s'agit de garantir qu'une ressource sera accessible au moment précis où quelqu'un souhaitera s'en servir ;
– **l'authentification** a pour but de vérifier qu'une entité est bien celle qu'elle prétend être ;
– **la non-répudiation** vise à interdire à une entité de pouvoir nier avoir pris part à une action (cela est fortement lié à la notion juridique d'imputabilité).

1. Stanislas de Maupeou, in *Revue Défense nationale*, novembre 2003
2. Lire à ce propos la note du CERTA : « Tunnel et pare feu : une cohabitation difficile » (http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003/) ;

Afin d'atteindre ces objectifs de sécurité, il est nécessaire de mettre en œuvre une **politique de sécurité**, applicable à l'ensemble des entités à l'intérieur d'un domaine géographique ou fonctionnel qui explicitera l'ensemble des règles et des recommandations afin de protéger les ressources et les informations contre tout préjudice et également de prévoir le cas de la faillite de la protection.

Pour être mise en œuvre sur un plan opérationnel, cette politique de sécurité s'appuie sur un certain nombre de **fonctions de sécurité**, telles que : l'identification et l'authentification des entités, le contrôle d'accès, la traçabilité des sujets et des opérations, l'audit des systèmes, la protection des contenus et la gestion de la sécurité.

Ces fonctions font l'objet de menaces particulières et peuvent présenter des vulnérabilités susceptibles d'être exploitées par des attaquants motivés ou non.

Cette politique de sécurité, associée à la gestion des risques, permet de prononcer une homologation de sécurité.

La sensibilité de l'information à prendre en compte

Les informations qui doivent demeurer confidentielles, celles qui doivent absolument être disponibles ou celles qui peuvent représenter un attrait pour une tierce partie, sont appelées sensibles (cf. Annexe V).

• L'AFNOR [1] distingue trois types d'informations :
– « L'information aisément et licitement accessible » que certains appellent *l'information blanche* est ouverte à tous. Elle se trouve dans la presse, sur Internet, etc.
– « L'information licitement accessible mais caractérisée par des difficultés dans la connaissance de son existence et de son accès ». Cette *information grise*, pour la trouver, il faut d'abord savoir la chercher. Elle se rapproche davantage du renseignement.
– « L'information à diffusion restreinte et dont l'accès et l'usage sont expressément protégés ». Il s'agit ici de *l'information noire* qui est protégée par un contrat ou une loi. Seules quelques personnes sont autorisées à y accéder.

• Les deux mentions préconisées par la Directive 901 : *confidentiel* et *diffusion limitée*

Aux termes de l'art. 4, portant sur les informations sensibles, non-classifiées *Défense*, il est recommandé que ces informations reçoivent une mention rappelant leur sensibilité en considération de la gravité des

1. Association française de normalisation.

conséquences qui résulterait de leur divulgation, de leur altération, de leur indisponibilité ou de leur destruction.

À cette fin, une distinction est opérée par deux mentions désignant le niveau de protection qu'il faut assurer à l'information : *confidentiel* et *diffusion limitée*.

Chacune de ces mentions de sensibilité peut être assortie d'une mention spécifique, caractéristique du domaine protégé : *personnel* (information nominative au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) ; *professionnel* (protégé par l'article 226-13 du code pénal) ; *industriel* ; *commercial* ; nom d'une société ou d'un organisme ; nom de deux partenaires ; nom d'un programme.

La mention spécifique assure le cloisonnement de l'information, en réservant son accès aux seules personnes ayant besoin de les connaître pour l'accomplissement de leur fonction ou de leur mission.

Des attaques sophistiquées, portant atteintes aux enjeux économiques et d'intelligence économique

Les principales menaces effectives pesant sur les systèmes d'information sont de nature distincte mais tout aussi préjudiciable à la protection de l'information :
– **l'utilisateur** : il n'est pas généralement une menace : il peut se retrouver face à une gestion de la complexité à laquelle il n'a pas été préparé (le particulier n'est pas un administrateur informatique). L'exemple typique est la mauvaise utilisation de SSL ou encore le *phishing* ;
– **les programmes malveillants** : un logiciel destiné à nuire ou à abuser des ressources du système est installé sur le système (par mégarde ou par malveillance), ouvrant la porte à des intrusions ou modifiant les données ;
– **l'intrusion** : une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès ;
– **un sinistre** (vol, incendie, dégât des eaux...) génère une perte de matériel et/ou de données ;

La sécurité des systèmes d'information est partie intégrante de la sécurité globale visant à se protéger des attaques :
– **physiques** : ces attaques (vols ou destructions par exemple) visent les infrastructures physiques des systèmes d'information, tels les câbles ou les ordinateurs eux-mêmes ;
– **électroniques** : il s'agit par exemple de l'interception ou du brouillage des communications ;

– **logicielles** : ces attaques regroupent l'intrusion, l'exploration, l'altération, la destruction et la saturation des systèmes informatiques par des moyens logiques ;
– **humaines** : l'homme est un acteur clef d'un système d'information. Il constitue à ce titre une cible privilégiée et peut faire l'objet de manipulation afin de lui soutirer de l'information via l'« ingénierie sociale » [1] par exemple ;
– **organisationnelles** : un attaquant cherchera à abuser des défauts de l'organisation et de sa sécurité pour accéder à ses ressources sensibles.

Ces types d'attaques sont des éléments indissociables parfois utilisés simultanément pour une attaque sophistiquée qu'il convient d'intégrer dans un plan de sécurité globale. *Ne traiter qu'un seul de ces points pourrait être comparé à installer une porte blindée à l'entrée d'une maison, mais en laissant les fenêtres ouvertes*.

Des attaquants aux profils et aux motivations hétérogènes

En 1983, à l'époque où la micro-informatique commence à peine à se développer, le cinéaste américain John Badham réalise *War Games*. Dans ce film, il imagine un jeune touche-à-tout de génie pénétrant l'ordinateur de contrôle des missiles intercontinentaux américains (ordinateur accessible en ligne ! ! ce qui n'a pas beaucoup de sens...). Pensant avoir à faire à un jeu, il déclenche une guerre thermonucléaire globale...

Si le mythe de l'adolescent pénétrant les sites du Pentagone a la vie dure, les attaquants sont de profils hétérogènes et obéissent à des motivations très différentes.

Dans ce rapport, il est convenu d'appeler *attaquant* toute personne physique ou morale (État, organisation, service, groupe de pensée, etc.) portant atteinte ou cherchant à porter atteinte à un système d'information, de façon délibérée et quelles que soient ses motivations.

Les principaux objectifs d'un attaquant sont de cinq ordres :
– désinformer ;
– empêcher l'accès à une ressource sur le système d'information ;
– prendre le contrôle du système par exemple pour l'utiliser ultérieurement ;
– récupérer de l'information présente sur le système ;
– utiliser le système compromis pour rebondir vers un système voisin.

Il est toujours difficile de connaître les motivations d'un acte, même si ces dernières, telles que le besoin de reconnaissance, l'admiration, la curiosité, le pouvoir, l'argent et la vengeance sont le plus souvent les moteurs de ces actes délictueux. Il est cependant utile de chercher à les comprendre pour mettre en place des stratégies et des tactiques de réponses adaptées.

1. Ingénierie sociale ou « Social Engineering » : l'art de manipuler un humain pour lui soutirer des informations. En pratique, un pirate peut tenter, par exemple, de se faire passer pour un responsable et demander son mot de passe à un utilisateur naïf.

On distingue traditionnellement 4 types d'attaques qu'ils nous semble utile de rappeler ici à un public non-averti :

– **Ludique** : les attaquants sont motivés par la recherche d'une prouesse technique valorisante, cherchent à démontrer la fragilité d'un système et se recrutent souvent parmi de jeunes informaticiens.

Défiguration ludique :

Le 16 juillet 2005, le site www.expatries.diplomatie.gouv.fr était défiguré [1] : une de ses pages était remplacée a priori par une référence au groupe de pirates.

– **Cupide** : des groupes ou des individus cherchent à obtenir un gain financier important et rapide. Les victimes détiennent de l'argent ou ont accès à des flux financiers importants (banques, paris en ligne...). Le chantage est devenu une pratique courante, comme l'illustre l'exemple des virus Smitfraud. C et PGP coder qui demandent explicitement à l'utilisateur de payer pour rétablir le bon fonctionnement du système.

– **Terroriste** : des groupes organisés, voire un État, veulent frapper l'opinion par un chantage ou par une action spectaculaire, amplifiée par l'impact des médias, telle que le sabotage d'infrastructures vitales, mais il fait souligner que cela n'a encore jamais été rapporté.

– **Stratégique :** un État, des groupes organisés ou des entreprises, peuvent utiliser avec efficacité les faiblesses éventuelles des systèmes d'information afin de prendre connaissance d'informations sensibles ou confidentielles, notamment en accédant frauduleusement à des banques de données. L'attaque massive de systèmes vitaux d'un pays ou d'une entreprise afin de les neutraliser ou de les paralyser constitue une autre hypothèse. La désinformation et la déstabilisation sont des moyens très puissants et faciles à mettre en œuvre avec un effet multiplicatif dû à notre dépendance vis-à-vis de l'information.

Cette typologie prend en compte à la fois les niveaux de compétence et les niveaux de détermination des auteurs. Il est à noter que les motivations peuvent être croisées et ou combinées ; par exemple un intérêt cupide et stratégique.

1. Archive de Zone-H :
http://www.zone-h.org/en/defacements/mirror/id=2595669/

Profils des attaquants

Sans détailler tous les profils (cf. Annexe VI), on retiendra le plus connu ; les hackers [1] qui interviennent individuellement ou via des organisations. Différentes catégories de *hackers* existent en fonction de leur champ d'implication (légal ou illégal) ou de leur impact sur les réseaux informatiques : les chapeaux blancs, certains consultants en sécurité, administrateurs réseaux ou cyber-policiers, ont un sens de l'éthique et de la déontologie ; les chapeaux gris pénètrent les systèmes sans y être autorisés, pour faire la preuve de leur habileté mais ne connaissant pas la conséquence de leurs actes ; les chapeaux noirs, diffuseurs volontaires de virus, cyber-espions, cyber-terroristes et cyber-escrocs, correspondent à la définition du pirate. Ces catégories peuvent être subdivisées en fonction des spécialités. Ainsi, le *craker*, s'occupe de casser la protection des logiciels, le *carder*, les systèmes de protection des cartes à puces, le *phreaker*, les protections des systèmes téléphoniques.

Les infrastructures vitales, l'État, les entreprises, les entités académiques et les citoyens : des cibles interdépendantes

Compte tenu de l'interconnexion entre les réseaux constituant les systèmes d'information les cibles sont devenues de plus en plus interdépendantes.

- **Les infrastructures vitales, un enjeu de sécurité nationale**

Le fonctionnement du pays est dépendant d'infrastructures informatisées, cible de menaces cupides, stratégiques et terroristes.

La Commission européenne, dans une communication en date d'octobre 2004 (« Protection des infrastructures critiques [2] dans le cadre de la lutte contre le terrorisme » [3]), propose la définition suivante :
« Les infrastructures critiques sont des installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des États membres. Les infrastructures critiques se trouvent dans de nombreux secteurs de l'économie, y compris le secteur bancaire et des finances, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires et les communications, ainsi que certains services administratifs de base. »

1. Un *hacker* est un expert technique/scientifique, sans connotation morale particulière, contrairement au langage usuel. C'est pourquoi, dans ce rapport, les termes de pirates ou d'intrus pour désigner une personne employant des moyens illégaux pour rentrer et/ou se maintenir dans un système d'information seront préférés.
2. Il est opportun de préciser la distinction faite entre la terminologie française « infrastructures vitales » et son homologue anglo-saxonne « *critical infrastructures* ».
3. http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/com/2004/com2004_0702fr01.pdf

Indispensables au bon fonctionnement du pays, elles constituent des cibles privilégiées : il s'agit de la distribution d'énergie électrique (auprès d'autres infrastructures : hôpitaux, etc.) ; la production d'énergie électrique en particulier nucléaire ; les réseaux d'alimentation et de production des raffineries ; la distribution et production d'eau douce ; les réseaux de transport (réservations billets d'avions, contrôle aérien, réseaux de signalisation des voies ferrées, etc.) ; les réseaux de communication (téléphone filaire, cellulaires, réseau Internet, etc.) y compris ceux des forces de police et de la défense.

L'interdépendance entre certaines de ces infrastructures génère également des facteurs de risques en terme de réaction en chaîne qui doivent conduire l'État en accord avec les opérateurs d'infrastructures vitales à définir des politiques de sécurité qui envisagent la sécurité de manière globale et solidaire.

Ces attaques, si elles aboutissaient, pourraient avoir des conséquences particulièrement graves, qu'elles soient économiques, sociales, écologiques voire humaines.

Les réseaux nationaux britanniques victimes d'attaques ?

Le 16 juin 2005, le National Infrastructure Security Coordination Center *(NISCC) du Royaume-Uni émettait, à travers la presse nationale, une alerte concernant des virus qui s'attaqueraient aux réseaux informatiques d'entités publiques et privées dans plusieurs secteurs clés : énergie, communications, transport, santé, finances et organismes gouvernementaux.*

Il s'agissait, selon le NISCC, d'un type d'attaque de haut niveau, combinant une large variété de techniques connues mais difficiles à détecter et qui visait certaines infrastructures critiques.

En amont de l'attaque se pose le problème de la décision de connecter imprudemment et sans analyse de risque préalable, des réseaux sensibles. Des travaux sur la résilience de tels systèmes devraient être engagés. Dans ce domaine comme dans d'autres, le CERTA (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques) rappelle très régulièrement que, selon le principe de défense en profondeur, la sécurité des systèmes d'information ne saurait reposer sur les seuls outils de sécurité comme les antivirus ou les pare-feux mais que la vigilance de l'utilisateur est également primordiale ainsi qu'une véritable politique de mise à jour des applications.

• **L'État : une cible de choix**

À titre d'exemple, le ministère de la Défense américain (*Department of defense*) est le plus attaqué au monde, avant Microsoft [1]. Preuve en est aussi le succès des sites gouvernementaux (extension *.gov* aux États-Unis, *.gouv.fr* en France) sur les pages référençant les défigurations, « considérées spéciales » [2].

Si la défiguration d'un site peut sembler banale et sans conséquence autre que celle touchant son image de marque, le CERTA observe que la défiguration en elle-même est souvent l'arbre qui cache la forêt. La plupart du temps les attaquants cachent leur attaque principale sous le couvert de la défiguration. Ainsi, se contenter de rendre au site son aspect originel revient à sous-estimer la portée de l'attaque et ne règle rien sur le fond.

• **Les entreprises : des cibles de plus en plus attractives**

Les entreprises sont confrontées à des menaces à finalité ludique, cupide ou stratégique.

Ainsi, en juin 2005, des révélations [3] sur une entreprise israélienne qui « louait » un cheval de Troie à ses clients ont conduit à l'arrestation de plusieurs dirigeants d'entreprises à travers le monde. En s'adressant à cette société, un client demandait tout simplement à ce que le produit soit installé dans le système d'information de la cible, et pouvait ensuite en extraire en toute impunité les informations qu'il désirait.

Si les entreprises ont davantage de moyens pour se protéger, la complexité croissante des systèmes d'information et les contraintes de coûts rendent d'autant plus difficile la sécurisation des systèmes.

• **Les entités académiques, universités, centres de recherche, écoles d'ingénieurs**

Moins sensibilisés à la sécurité des systèmes d'information, les organismes de formation de recherche sont victimes de nombreuses attaques, comme l'affirment certains témoignages recueillis au cours de la mission.

• **Les citoyens, des cibles vulnérables**

Les données à protéger pour un citoyen sont de deux types : d'une part celles qu'il produit lui-même : e-mail, blogs, forums, et d'autre part celles qu'il ne maîtrise pas, comme ses connexions Web chez son fournisseur d'accès Internet ou à travers une borne Wifi, la localisation de son mobile à travers les relais téléphoniques, son passage devant des caméras de vidéosurveillance sur IP ou non.

De plus, les machines des citoyens peuvent servir de relais pour conduire des attaques.

1. Source : auditions
2. Défigurations spéciales : http : //www.zone-h.com/en/defacements/special
3. http://solutions.journaldunet.com/0506/050603_espionnage_industriel_israel.shtml

Tous les éléments d'un système d'information sont menacés

Tous les éléments constitutifs d'un système d'information peuvent être la cible d'attaques. Nous nous limiterons ici à quelques aspects matériels :

• **Routeurs :** la connexion d'un site, à Internet ou à des réseaux internes, repose sur les routeurs. Leur fiabilité doit être à toute épreuve, leur sécurisation renforcée, et leur surveillance assurée. En effet, toute perturbation de l'équipement peut isoler un site du reste du monde, ou engendrer une compromission de l'intégralité des données transitant par l'équipement.

• **Liens physiques** : ils permettent le transit de l'information et, à titre de comparaison, sont tout aussi importants que les voies de communications en temps de guerre. Ils peuvent être mis sur écoute, rompus (accidentellement ou non), détournés. Il faut par ailleurs prévoir de la redondance dans les technologies utilisées (satellite, câble).

Liaisons transatlantiques

Le réseau TAT-14 [1], assure une partie du transit Internet entre l'Europe et les États-Unis. Toute rupture des fibres optiques entraîne des perturbations importantes des communications transatlantiques. Ce fut accidentellement le cas en novembre 2003, à cause d'un chalutier.

• **Serveurs** : ils assurent des services d'une extrême importance au bon fonctionnement de toute structure utilisant les réseaux tels que le service de messagerie électronique devenu indispensable en tant qu'outil de communication, service Web – portail de communication et emblème de l'organisme vis-à-vis de l'extérieur, service de fichiers aux contenus sensibles ou pas. Il est à noter le danger de rendre le service de messagerie indispensable quand on songe qu'il n'y a pas de garantie structurelle que le courrier est bien délivré.

1. À propos de TAT-14 : https://www.tat-14.com/tat14/

• **Postes clients** : utilisés à tout niveau de la hiérarchie, ils permettent à tous de s'acquitter de ses tâches quotidiennes et stockent des informations potentiellement précieuses. Ils sont surtout en première ligne face aux maladresses ou malveillances des employés sur leur lieu de travail ou des utilisateurs domestiques. Ils sont considérés, à l'état actuel de l'art, comme très difficiles à sécuriser.

• **Équipements mobiles :** d'une utilisation croissante au sein de l'entreprise et de la vie quotidienne, les équipements mobiles constituent des éléments du système d'information, et surtout des cibles en puissance : ordinateur portable, PDA, téléphone portable sont de plus en plus vulnérables à cause de technologies dangereuses (wifi, bluetooth®, etc.) et donc de plus en plus attaquables.

Les vecteurs d'attaque sont multiples et témoignent d'une complexité croissante

Les attaques physiques sont à traiter en priorité

Cette dénomination recouvre les menaces pouvant aboutir à la compromission matérielle du système de traitement de données ou du réseau de communication. Les conséquences identifiées sont la paralysie du système d'information, par exemple en empêchant l'accès à certaines zones ou ressources névralgiques ou la destruction.

Parer les menaces physiques peut nécessiter des dépenses d'infrastructure importantes (construction d'enclaves de sécurité, de zones protégées, mise en place de systèmes de surveillance et d'alerte, etc.), **mais le contrôle de l'accès physique aux ressources du système d'information est aujourd'hui indispensable** parce qu'il serait vain de se lancer dans le déploiement de systèmes d'authentification et d'autorisation complexes (par exemple à base de certificats) si l'on est incapable de contrôler l'accès physique à un serveur. Dans le même temps, il est inutile et illusoire de faire l'effort sur la sécurité physique quand il y a un accès réseau dont le périmètre n'est pas contrôlé ou maîtrisé.

La miniaturisation des moyens de stockage, comme les clés USB [1], et leur facilité d'emploi plaident également en faveur du renforcement de ce contrôle. Il est possible, à partir d'une clé USB modifiée, de prendre le contrôle d'un poste et d'y insérer un programme indésirable ou d'en extraire des données. **Aucun ordinateur ayant accès à des données sensibles, et *a fortiori* relevant du secret de défense, ne devrait être laissé sans surveillance, en particulier lorsque des tiers** (agents d'entretien, visiteurs, concurrents potentiels, etc.) **ont accès aux locaux**.

1. Une faille de sécurité concernant l'utilisation des clefs USB a été mise en évidence en août 2005. Cette faille permet d'ouvrir une session sur une machine protégée par mot de passe à partir d'une simple clef USB spécifiquement programmée dans ce but. Un opérateur malveillant serait ainsi en mesure d'obtenir un accès illimité à la machine et d'y consulter toutes les données qu'elle contient. Cette faille est propre à la technologie USB et non au système d'exploitation, ce qui signifie que tous les systèmes sont potentiellement vulnérables.

Les menaces électroniques demeurent encore sous-estimées

Les moyens de communications internes et externes des systèmes d'information ne suscitent pas la même attention que les moyens informatiques. Pourtant leur vulnérabilité les rend sensibles aux attaques pouvant entraîner : le déni de service par brouillage ou saturation ; l'atteinte à l'intégrité des communications par injection de données malicieuses et à la confidentialité par écoute des émissions radioélectriques du réseau.

- **La menace Tempest** [1]

La menace Tempest est la menace que représente l'interception des signaux parasites compromettants, émis par tout équipement traitant des informations sous forme électronique, en vue de reconstituer les informations traitées.
Il est possible de tirer parti des signaux émis par un système électronique, perceptible jusqu'à plus d'une centaine de mètres. Les tensions électriques peuvent aussi révéler des informations intéressantes, par conduction, soit sur les conducteurs d'alimentation de l'appareil cible, soit sur des conducteurs passant à proximité, L'analyse des signaux parasites compromettants classiques s'est enrichie, en 2004, d'une nouvelle technique de cryptanalyse acoustique des cœurs d'unités centrales *(Core Process Units)*. La menace Tempest, connue des services de renseignement et de protection, l'est moins du grand public. La parer est difficile et coûteux : il convient de placer tous les équipements sensibles dans des cages de Faraday ou d'acquérir des matériels conçus pour émettre un minimum de signaux.
L'utilisation croissante des moyens de communications sans-fil : réseaux Wifi, communications bluetooth® ou puces RFID sont autant de technologies qui multiplient les vecteurs d'attaque possibles. Une transmission Wifi ou bluetooth® non-sécurisée, utilisée dans un sous-système identification biométrique, donc supposé donner une bonne garantie sur l'identité d'un utilisateur, non seulement détruit de facto toute sorte de garantie, mais peut, si elle est exploitée, mettre à mal l'ensemble du système d'information.

L'exemple des puces RFID *(Radio-Frequency Identification)*

Les étiquettes d'identification radio (ou RFID) sont des puces sans contact transmettant des données à distance par moyens radioélectriques. On les appelle aussi étiquettes intelligentes*, ou encore parfois* étiquettes transpondeurs*. C'est, par exemple, ce type de puces qui est utilisé dans le système* Navigo *dans les transports en Île-de-France ou pour le marquage des animaux. Les utilisations potentielles de ce genre de technologie sont nombreuses : gestion de stocks, grands magasins, télépéages d'autoroutes, nouveaux passeports, etc.*

1. Tout système électronique émet des signaux dont le rayonnement peut être perceptible jusqu'à une centaine de mètres et en révéler le contenu. Le terme TEMPEST désigne la menace que représente cette vulnérabilité.

Avec des moyens de détection un peu sophistiqués, la distance d'accès effective aux étiquettes RFID peut atteindre jusqu'à quelques dizaines de mètres). La plupart des dispositifs ne chiffrant pas (ou mal) les données transmises, les informations peuvent donc être interceptées à cette distance.

Considérant, par exemple, l'intérêt que pourrait trouver un concurrent à lire à distance l'ensemble du flux logistique de distribution d'un industriel et, dans la mesure où ce type de technologie est envisagé pour transmettre des données personnelles (sur des passeports par exemple) l'emploi de la technologie RFID pour des données à caractère personnel ou dans des systèmes de haute sécurité nécessite une analyse poussée des risques.

Les menaces logicielles sont en évolutions constantes

Tout utilisateur standard d'un ordinateur personnel est confronté à la réalité des attaques possibles comme par exemple des vers et virus informatiques, des courriers électroniques non-sollicités ou spam, de tentatives de fraudes informatisées.

Plusieurs modes d'attaques logiciels peuvent se combiner ou se succéder afin d'atteindre l'objectif souhaité :

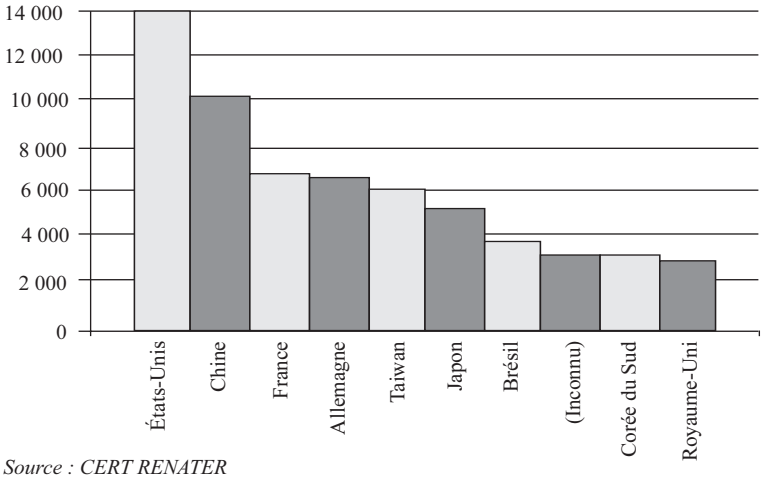
• **La reconnaissance :** l'attaquant va déployer tous les procédés à sa portée pour regrouper quantité d'informations sur le système ou réseau ciblé. À cette fin, il pourra le sonder et le cartographier (ce que l'on appelle un « scan »), et dans certains cas capturer du trafic légitime pour en tirer des éléments pertinents, ou encore exploiter la gigantesque base de connaissances que sont les moteurs de recherche sur Internet.

• **L'intrusion :** en utilisant une vulnérabilité identifiée du système ciblé, l'attaquant va tenter d'obtenir un accès sur celui-ci, ou des privilèges accrus. Pour cela, il pourra usurper l'identité d'un utilisateur légitime, exploiter une faille du système d'exploitation ou un trou de sécurité applicatif, introduire un cheval de Troie, utiliser une porte dérobée.

• **L'altération et la destruction :** il peut s'agir d'altérer ou de détruire des données stockées sur le système, ou bien le système lui-même, avec des finalités diverses. Au-delà des implications financières et industrielles évidentes, le but poursuivi peut être la dégradation des mécanismes de protection en vue d'attaques ultérieures. Cela peut être atténué par des mécanismes de sauvegarde et des plans de continuité.

• **La saturation :** plus connue sous la dénomination de déni de service, l'attaque consiste à provoquer la saturation d'une des ressources du système d'information : bande passante, puissance de calcul, capacité de stockage, dans l'intention de rendre l'ensemble inutilisable. De nos jours, cette activité est très répandue sur Internet.

Provenance des « scans »



Source : CERT RENATER

Au mois d'octobre 2005, 104 219 sources distinctes ont sondé des machines sur le réseau RENATER [1].

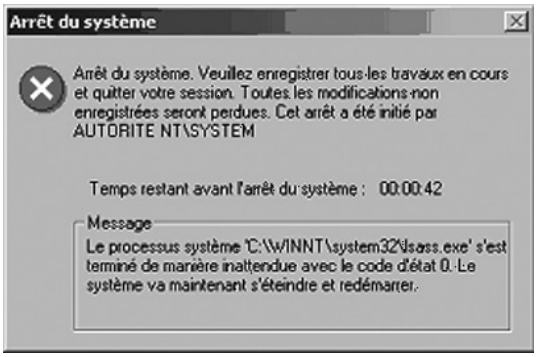
Il peut s'agir de tentatives de propagations virales, ou de phases de reconnaissance pré-attaque de pirates ou encore de mauvaises configurations système.

Quelques exemples parmi les plus connus :

• **Un ver** est un logiciel malveillant indépendant qui se transmet d'ordinateur à ordinateur par l'Internet ou tout autre réseau en utilisant les failles existantes et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. Contrairement au virus, le ver ne s'implante pas au sein d'un autre programme.
Les tout premiers vers sont apparus en 1982. On retiendra la déferlante médiatique de ***I love you*** en mai 2000 et en 2002-2003, ***Slammer*** fait son apparition. Des dizaines de milliers de serveurs ont été touchés en quelques dizaines de minutes. *Slammer* a eu comme conséquences un ralentissement mondial de l'Internet, des arrêts de certains services pouvant aboutir, par exemple dans les aéroports américains, à reporter ou annuler des vols, compte tenu de répercussions négatives sur les systèmes de réservations automatisées en ligne. Les pertes économiques directes et indirectes ont été estimées à 1 milliard de dollars. S'agissant de **Blaster**, une **grande entreprise française a chiffré à 1,5 M€ les conséquences de ce ver sur ses propres systèmes d'information [2].**

1. RENATER : Réseau national de télécommunications pour la technologie l'enseignement et la recherche.
2. Source : auditions.

Un ver bien ordinaire



*Si vous avez déjà vu cette fenêtre, sans doute faites-vous partie des quelques **millions** d'internautes à travers le monde à avoir été infectés par le ver **Sasser** [1].*
Se propageant entre PC sous Windows sans firewall grâce aux connexions réseau, il a longuement fait parler de lui en mai 2004.

• **Un virus** est un logiciel malveillant, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un événement donné.
À titre d'exemple, dans un grand groupe [2], 5 % des courriels échangés en 2004 ont été interceptés et éradiqués. Mais il faut aussi et surtout tenir compte de tout ce qui ne se détecte pas à cause de mises à jour non-effectuées ou de vulnérabilité encore inconnue. Les antivirus agissent par définition *a posteriori*. C'est précisément pour cela que la protection contre les virus ne peut et ne doit pas se limiter à un antivirus mais que l'utilisateur doit être formé et rester vigilant.
2004 a vu l'explosion du nombre de variantes virales, avec plus de **10 000 nouveaux virus** identifiés [3] comme MyDoom, ciblant les systèmes d'exploitation Windows, avec pour objectif de lancer des attaques comme par exemple des dénis de service.

• **Le phishing** consiste à duper l'internaute (page factice d'un site bancaire ou de e-commerce) pour qu'il communique des informations confidentielles (nom, mot de passe, numéro PIN...). Ces données sont utilisées pour obtenir de l'argent. Cette menace est un frein au développement de la banque et de l'administration en ligne.

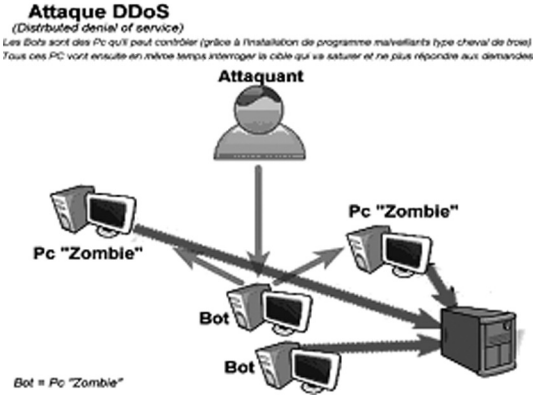
• **Les réseaux de robots** visent à donner la possibilité à un pirate de contrôler des machines, en vue d'une exploitation malveillante.

1. http://www.sophos.fr/virusinfo/analyses/w32sassera.html
2. Source : auditions.
3. Source : Sophos et Clusif.

Ils peuvent provoquer des redémarrages intempestifs ou empêcher le téléchargement de correctifs tout en bloquant l'accès à certains sites Internet.

Pour ne pas être détectés et préserver leur anonymat, les attaquants dont la motivation est souvent financière ont de plus en plus tendance à mettre en place un réseau de machines devant rester invisible et leur permettant, le moment venu, de relayer de manière massive à partir des machines infectées l'attaque désirée : des spams, des virus, ou des attaques en déni de service. Les réseaux de robots (***botnets***) peuvent mettre en œuvre entre 3 000 et 10 000 ordinateurs ***zombies***. Au premier semestre 2005, en moyenne 10 352 ordinateurs de réseaux de bots ont été actifs, par jour, soit **une augmentation de 140 %** par rapport au semestre précédent [1].

Les serveurs racines, cibles d'une attaque d'envergure



En 2002, pendant une heure, les treize serveurs de noms racine (dont 10 aux États-Unis), qui permettent directement ou indirectement, à tous les navigateurs de trouver les pages Web demandées, à tous les e-mails d'arriver à destination, ont été la cible d'une attaque de déni de service coordonnée. Le problème n'est pas tant la géographie physique mais qui concrètement contrôle ces serveurs (contenu, mise à jour, etc.).

Ces serveurs sont le centre nerveux d'Internet et en même temps son talon d'Achille.

Pour les contrer, il est nécessaire d'agir au niveau préventif, en évitant, dans toute la mesure du possible, la contamination des machines.

1. Rapport « Internet Security Threat Report » de la société Symantec.

• **Un spam** est un courrier électronique d'exemplaires identiques, envoyé en nombre, de façon automatique et non-sollicité [1].
En 2004, il y a eu une inondation graduelle du Net par les spams. De ce fait, nombre de responsables sécurité ont dû mobiliser leurs équipes sur le sujet des spam pour répondre à la pression de leur direction et des utilisateurs face à la saturation de leurs messageries. À titre d'exemple un grand groupe français [2] dans lequel 500 000 mails sont échangés chaque jour, en rejette 60 000, dont 31 000 spams et 29 000 virus. Au premier semestre 2005 le spam a représenté **61 % de la totalité du trafic de courriers électroniques** (51 % de tous les spams diffusés à travers le monde provenaient des États-Unis) [3]. Cependant, le spam occasionne plus de désagréments que de dégâts, et s'il est parfois qualifié d'ennemi logique numéro un, ce n'est pas du fait de sa dangerosité.

• **Un *spyware*** est un code qui permet de transmettre les habitudes d'un internaute, que l'on peut qualifier de logiciel espion avec des objectifs de commerce et de renseignement (études marketing, etc.). Il peut intégrer des programmes malveillants de toutes sortes mais également affecter la confidentialité des données de l'internaute. En 2004, 50 % des remontées « Dr Watson » (remontée des problèmes informatiques à Microsoft) étaient dues à des *spywares* ! Les logiciels espions et publicitaires ***adware*** sont en expansion.

Des attaques humaines

Dans la typologie des menaces, le facteur humain est essentiel et revêt deux formes :
– l**'ingénierie sociale :** afin de contourner des systèmes de protection, ou d'obtenir des informations normalement confidentielles, un attaquant peut tenter d'abuser de la naïveté d'un utilisateur peu sensibilisé ;
– **la manipulation d'individus :** « MICE » : *Money, Ideology, Compromise, Ego*. Cet acronyme anglophone résume les différents moyens pouvant permettre de s'assurer le concours de quelqu'un. Qu'il soit attiré par l'argent, une idéologie commune (religieuse ou politique), sous l'emprise d'une compromission ou de son ego, un individu peut être manipulé.

Les attaques organisationnelles

L'utilisation des failles intrinsèques à l'organisation de la sécurité procédurale d'une entité permet d'accéder à ses informations sensibles. Les sous-traitants, ou prestataires de services, constituent des vecteurs privilégiés pour s'introduire au sein du périmètre physique d'un organisme et y perpétrer ses méfaits.

1. Le CERTA a émis en 2005 une recommandation complète à ce sujet (limiter l'impact du Spam : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004.pdf).
2. Source : auditions.
3. Rapport « Internet Security Threat Report » de la société Symantec.

Les vulnérabilités inhérentes aux systèmes d'information créent un environnement propice aux attaques

La conjonction de phénomènes tels que l'ouverture vers l'extérieur, l'interconnexion des réseaux, la possibilité offerte à un utilisateur de se connecter, par voie filaire ou hertzienne, à distance, la mobilité des liaisons, la miniaturisation des ordinateurs et des supports d'information crée un environnement plus propice encore aux attaques. Toutes ces vulnérabilités doivent être vues sous l'angle de la gestion des risques et de l'homologation de sécurité.

Des vulnérabilités techniques multiples en évolution permanente

Lorsqu'elles sont identifiées, les vulnérabilités peuvent être communiquées directement à l'éditeur, mais peuvent également faire l'objet d'une publicité, avant la publication d'un correctif (un *patch*). Le temps qui sépare la publication d'une vulnérabilité de l'apparition du code d'exploitation correspondant diminue, exposant d'autant les systèmes jusqu'à la publication du correctif ; le danger étant le *0-day* : des vulnérabilités inconnues avec des codes d'exploitation disponibles.

Au cours du premier semestre 2005, **on estime à environ 2000 le nombre de nouvelles vulnérabilités.** 97 % de ces vulnérabilités étaient considérées comme modérées à très graves. Cependant, cette appréciation de criticité doit être réévaluée en fonction des environnements des différents systèmes concernés.

On comprend la nécessité de tenir à jour son système, d'assurer une veille sur les vulnérabilités et une gestion rigoureuse des correctifs appliqués.

Certaines vulnérabilités, gardées secrètes, sont l'apanage d'organismes aux moyens plus importants (industriels, étatiques ou mafieux) et sont utilisées dans des optiques plus graves : espionnage, lutte informatique offensive, déstabilisation (cf. Annexe VII).

Cependant, il faut ajouter une notion relativement nouvelle mais déjà très répandue d'économie des vulnérabilités qui consiste à rémunérer les personnes découvrant de nouvelles vulnérabilités.

• **Les risques liés à l'utilisation d'infrastructures spontanées** [1]

Les risques de ces infrastructures spontanées sont liés au fait qu'elles s'appuient le plus souvent sur des standards propriétaires ou sur des modèles ou des architectures de sécurité **non-validées** qui peuvent amener à **contourner la politique de sécurité**.

C'est la raison pour laquelle les responsables de sécurité de plusieurs organisations, conscients des risques sous-jacents, limitent ou interdisent l'emploi de ces systèmes [2], le plus souvent sans succès. D'autres imposent pour l'emploi de tels outils d'utiliser des courriels sécurisés, le contenu confidentiel est dans un fichier attaché crypté [3].

• **La menace des périphériques externes**

La prolifération de périphériques de stockage externes de grande capacité constitue une menace. On retiendra en particulier : les clés USB, les assistants numériques personnels (PDA), les lecteurs et graveurs de CD et de DVD amovibles, les téléphones mobiles dotés d'une capacité de stockage de données.

Il y a deux grandes catégories de risques, l'introduction de codes malveillants sur le réseau et la perte ou le vol de données de l'entreprise alors que des mesures simples concernant l'utilisation de ces périphériques et leur traçabilité permettront de réduire sensiblement le niveau de risque.

D'après une enquête IDC [4], 71 % des sondés jugent très préoccupante l'utilisation en privé d'équipements mobiles en particulier par les dirigeants.

Les organisations sources de vulnérabilités

L'utilisation des failles inhérentes à l'organisation d'une entité est également un moyen d'accéder à ces informations sensibles. Les sous-traitants ou prestataires de services, par exemple, sont des vecteurs privilégiés pour s'introduire au sein du périmètre physique d'un organisme et, ainsi, y perpétrer leurs méfaits.

Plus les entreprises ont d'expérience en matière de sécurité, plus elles considèrent que la priorité doit être donnée au renforcement des procédures, plutôt qu'à l'acquisition de nouvelles solutions techniques. Concrètement, les entreprises se sont concentrées en 2005 sur trois types de procédures : les normes politiques et techniques (28,8 %), les réactions en cas de crise ou d'incident (22,2 %) et les stratégies de sécurité pour les utilisateurs et les terminaux mobiles (14,6 %).

1. Une infrastructure spontanée est une nouvelle couche réseau mise en place à l'insu de l'administrateur réseau ou qu'il ne peut réellement contrôler. On peut citer par exemple les offres de services de convergence, susceptibles d'intéresser des particuliers ou des PME qui sont depuis 2004 en pleine croissance. C'est par exemple le cas des offres Blackberry ou Skype (téléphonie sur IP).
2. Source : auditions.
3. Source : auditions.
4. Livre blanc IDC France – Internet Security System (ISS) sur la sécurité des systèmes d'information -100 entretiens auprès d'entreprises et d'administrations françaises – avril 2005.

U**ne organisation trop permissive** et **insuffisamment structurée**, risque de ne pouvoir identifier l'information critique pour son fonctionnement ; ni cerner sa vraie valeur ; ni « optimiser » les échanges d'informations entre ses entités. Par construction, elle restera donc plus vulnérable.

• **L'externalisation favorise les vulnérabilités**

L'entreprise qui recourt à l'externalisation doit s'assurer qu'elle dispose, vis-à-vis de son prestataire, des moyens et garanties permettant d'assurer la sécurité de son système d'information, notamment à travers l'éventuelle chaîne de sous-traitance...

Les principaux risques identifiés sont de nature :

– **informationnelle :** des données peuvent être dérobées ou manipulées et les systèmes d'information peuvent être neutralisés ;
– **juridique :** les sociétés utilisant des entreprises d'infogérance étrangère doivent prendre garde à la législation en vigueur dans le pays qui héberge leur informatique ainsi qu'à sa stabilité ;
– **économique :** un coût de transfert sous-évalué et une baisse de la qualité de services. Une perte définitive de savoir-faire en matière d'administration de systèmes ;
– **organisationnelle :** la réversibilité éventuelle du transfert doit être clairement prévue contractuellement et organisée.

Les organisations qui externalisent leurs infrastructures informatiques et leur SSI doivent bien intégrer que **l'ensemble des données de leur système d'information sera accessible à un tiers, dans le cadre d'un marché pour lequel il n'y a, à ce jour, aucune contrainte réglementaire spécifique.**

Les vulnérabilités humaines peuvent être liées à :

– une mise en réseau déraisonnable et systématique ;

– **une méconnaissance de la menace** (formation inadaptée, sensibilisation insuffisante) qui peut engendrer de nouveaux risques, dans le cas notamment :
· de l'utilisation d'architectures spontanées ;
· face à des attaques d'ingénierie sociale ;
· de la manipulation d'individus.

– **un mauvais climat social** susceptible de générer des mécontentements ou des vindictes ;

– **une insouciance des salariés, voire même de la direction, utilisateurs** de moyens informatiques ;

– **une utilisation mal contrôlée** : le risque résultant d'une connexion permanente « haut débit » à Internet (ADSL ou par câble) est supérieur à celui qui existait lorsque la consultation et les échanges se faisaient à travers un modem (modulateur-démodulateur) ;

– **une ergonomie inadaptée** : elle peut avoir des conséquences dramatiques (perte de données, diffusion d'informations secrètes, découragement des utilisateurs).

D'une façon générale, l'informatique actuelle est beaucoup plus complexe que l'idée généralement répandue et diffusée : la formation doit être développée.

Les vulnérabilités extérieures

Les vulnérabilités extérieures d'un système d'information sont induites par les circonstances périphériques sur lesquelles nous n'avons que peu ou pas de contrôle comme ceux liés à l'environnement (incendie, inondation...). Sauvegarder l'ensemble des informations dans un site secondaire distant et sécurisé est une nécessité pour se prémunir.

Des enjeux futurs en matière de SSI

Les aspects techniques

• **Le développement d'attaques plus performantes**

De nouvelles attaques apparaissent isolées ou combinées, comme les **attaques** dites **en essaim** (*swarming*). Dans ce type d'actions, un groupe attaque de manière très coordonnée une cible pouvant être une infrastructure critique ou une organisation.

• **L'indispensable sécurisation du poste client**

Parmi les tendances actuelles identifiées, le CERT-IST et le CERTA notent que les attaques visent préférentiellement les utilisateurs finaux, plutôt que les serveurs d'entreprise, mieux protégés.
La porte d'entrée du système d'information pour les *hackers* se déplace progressivement vers des équipements périmétriques, comme les lignes Internet protégées par des pare-feux, vers les postes de travail. « Il existe un lien très fort entre la sécurité individuelle des postes de travail et la sécurité informatique de l'entreprise. En protégeant son propre poste, on protège aussi les autres » [1].

Les enjeux de l'architecture et du développement d'un système

Il existe une analogie entre la démarche visant à assurer la sécurité d'un système d'information et celle qui permet de construire et d'assurer sa qualité.

1. Source : auditions.

L'expression du besoin en matière de sécurité pour un système nouveau devra faire apparaître les menaces dont il doit se protéger, les intentions de l'adversaire qu'il s'agit de prévenir et les formes que ses agressions peuvent prendre. En outre, avant d'entreprendre le développement du système, les spécifications fonctionnelles devront traiter des fonctionnalités du système à mettre en œuvre, de sa disponibilité, de la fiabilité attendue des informations et des conséquences d'une divulgation d'informations.

Une fois le développement terminé, avant de mettre en service le système, il faut soumettre toutes ses fonctions de sécurité à l'**examen d'un organisme différent de l'organisme qui l'a développé** pour éviter que les mêmes soient juges et parties dans la qualification du développement et pour s'assurer de la clarté et de la lisibilité de la conception.

Un grand groupe auditionné a insisté sur **la séparation nécessaire entre l'équipe qui réalise et celle qui préconise.** Autrement dit, **le maître d'œuvre de la SSI ne peut pas être le donneur d'ordre** [1]**.**

Lors de la mise en service opérationnelle, il faut enfin gérer la configuration du système avec soin. Il va sans dire qu'il faut apporter une attention particulière à la maintenance pour éviter qu'elle ne soit l'occasion d'ouverture de failles dans la sécurité.

Des enjeux politiques de souveraineté et de développement de l'économie nationale

• **Un enjeu de souveraineté nationale** : l'État doit garantir sa capacité à prendre des décisions de façon autonome afin de préserver les intérêts du pays. Pour cela il doit s'assurer de la continuité et de l'intégrité des données des systèmes d'information de l'État, des infrastructures vitales, et des entreprises sensibles.

En effet, l'État doit disposer en toute confidentialité de l'information nécessaire à l'exercice du pouvoir, préserver l'indépendance de sa décision qui repose sur la qualité et l'efficacité des sources d'informations ainsi que sur leur protection. Il doit également permettre aux entreprises d'évoluer dans un environnement sécurisé et de bénéficier ainsi des gains de productivité générés par la dématérialisation ou aux individus d'accéder à l'information et aux services, tout en les protégeant des risques créés par l'utilisation d'une toile « universelle ».

• **Les champs d'actions de la SSI et de l'Intelligence économique, se recoupent pour partie,** car ils font la synthèse de l'économie de la connaissance, et donc de l'information. Pour être efficace, une politique volontariste d'intelligence économique doit notamment s'appuyer sur des systèmes d'information fiables de l'État et des entreprises.

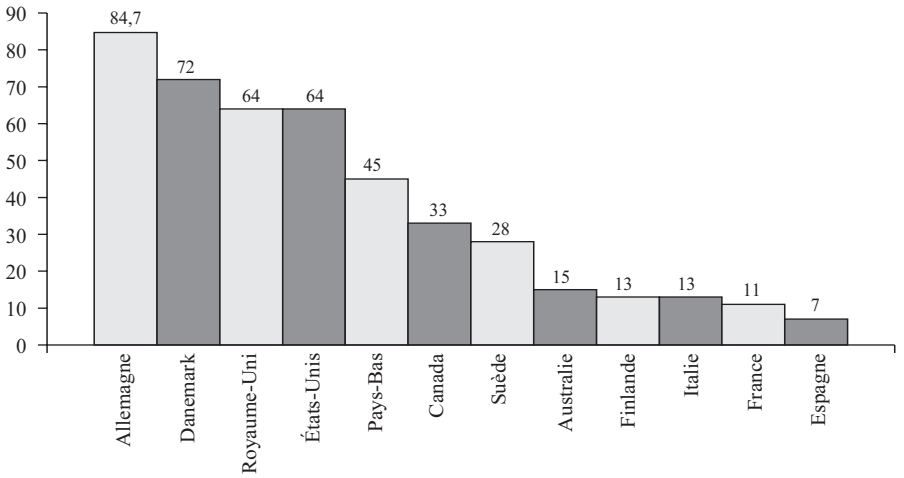
1. Source : auditions.

Par exemple, dans le domaine militaire, le besoin d'interopérabilité entre alliés conduit à adopter des normes qui, jusqu'à présent, sont fortement influencées par les États-Unis. Si la maîtrise de la réalisation des produits n'est pas équitablement partagée, il convient de s'interroger sur les conséquences induites sur la souveraineté de notre pays en particulier. Il en va de même des systèmes d'information utilisés par les forces de police et les services de renseignement.

• **Un enjeu économique** : un environnement sécurisé est nécessaire afin d'accompagner le rattrapage français dans l'usage des TIC, indispensable pour la croissance française, par les citoyens et les entreprises françaises.

Selon le tableau de bord du commerce électronique de décembre 2004 [1], malgré un taux d'équipements comparable pour les entreprises, des retards persistants demeurent par rapport aux concurrents en matière **d'usage**. Retenons quelques données de cette étude de 2002 qui reste cependant d'actualité.

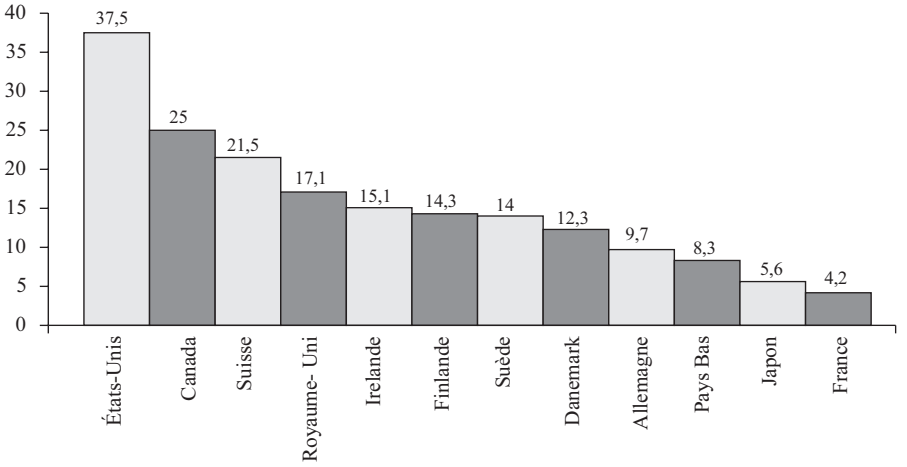
• En juillet 2002, on comptait en moyenne 31,4 sites Web pour 1000 habitants contre 17,2 sites en juillet 2000. Des écarts importants entre pays peuvent être constatés.



Nombre de sites pour 1000 habitants en juillet 2002

• Pour accomplir des transactions d'achat et de vente sur l'Internet, le commerce électronique a besoin de moyens sécurisés. Le nombre de serveurs sécurisés pour 100 000 habitants permet ainsi de mettre en évidence les pays les plus avancés dans l'utilisation du commerce électronique.

1. Mission pour l'économie numérique – tableau de bord du commerce électronique de décembre 2004 – 6e édition – Services des études et des statistiques industrielles (SESSI) – Ministère délégué à l'Industrie.



Nombre de serveurs sécurisés pour 100 000 habitants en juillet 2002

D'autres statistiques, dans cette étude relative aux citoyens, montrent certes une progression française sur les équipements et les usages, mais toujours des retards importants par rapport aux pays concurrents y compris en Asie.

Or, la contribution en points de croissance de l'usage des TIC est avérée, en particulier avec l'exemple des États-Unis où **la contribution des TIC à la croissance était de 1,3 à 1,5 pt contre 0,7 pt pour la France entre 1995 et 2000.** La contribution des industries productrices de TIC n'explique pas tout. En effet, d'autres pays qui ne disposent pas d'industries productrices de TIC plus importantes que la France sont en avance.

Dans un contexte de mondialisation croissante de l'économie et de concurrence soutenue, les entreprises françaises, mais aussi l'État, ont l'obligation de poursuivre et d'accélérer leurs investissements en TIC notamment pour améliorer leur productivité et favoriser leur développement commercial pour les premiers.

Cette politique volontariste pourra d'autant plus être mise en œuvre que l'environnement de ces acteurs aura été sécurisé, permettant ainsi de préserver la disponibilité, l'intégrité et la confidentialité de leurs activités.

Chapitre II

Les réponses organisationnelles et techniques

Comment l'État est-il organisé pour assurer la SSI ?

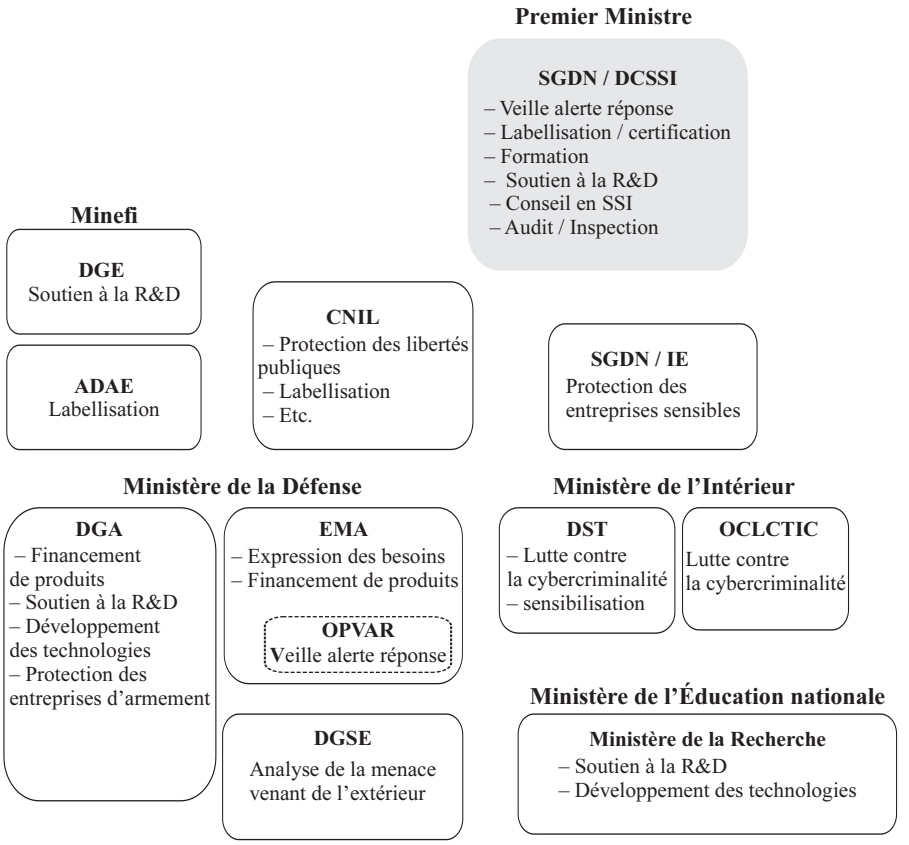
La sécurité est l'affaire de tous, mais l'État a un rôle essentiel à jouer. Par nature, il doit protéger les citoyens et les entreprises et, pour assurer la continuité de ses missions, protéger ses propres services, contre les menaces et les risques qui pourraient porter atteinte à leur intégrité. La difficulté du sujet qui nous intéresse ici est que la menace et les risques qui pèsent sur les systèmes d'information, s'ils ont des conséquences bien réelles, sont dématérialisés et donc moins visibles. Le développement de ce nouveau domaine sur lequel repose désormais le bon fonctionnement de notre société nécessite d'apporter des réponses nouvelles en matière de sécurité. Pour ce faire, l'État doit s'appuyer sur une organisation efficace et réactive. Si des structures existent il semble cependant qu'elles ne soient pas à la mesure de l'enjeu.

La réglementation en sécurité des systèmes d'information (SSI)

La réglementation en sécurité des systèmes d'information (SSI) n'existe pas sous la forme d'un code législatif ou réglementaire. La SSI n'est d'ailleurs pas même définie d'un point de vue juridique. En fait, le domaine de la SSI fait référence à une multitude de textes de niveaux juridiques très divers relatifs à l'organisation institutionnelle, à la protection des systèmes d'information, au développement de l'administration électronique, à la cryptologie, à la signature électronique ou à la cybercriminalité, (cf. Annexe IX).

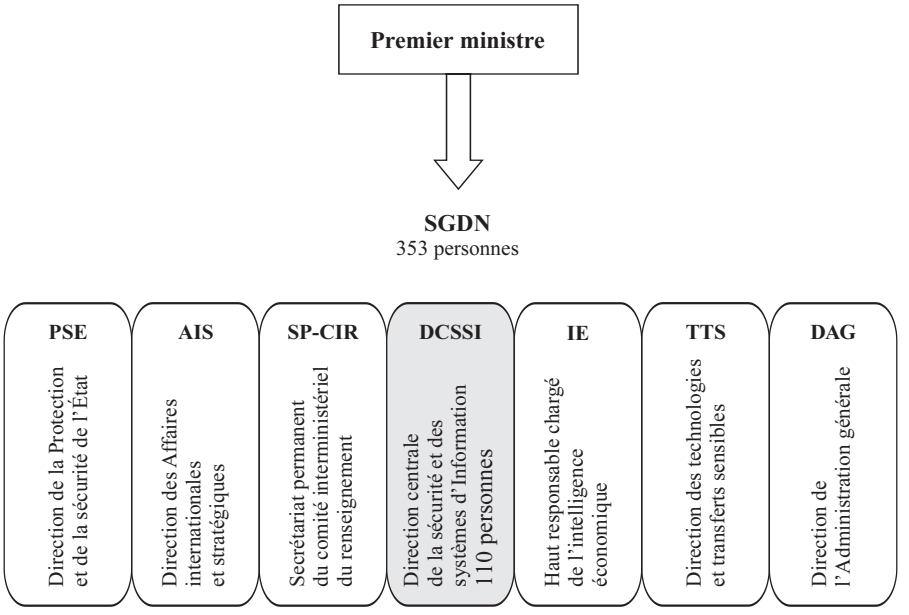
Une dispersion des moyens, des compétences et des politiques au niveau national

Principaux acteurs de la politique SSI



Une organisation dédiée, sous l'autorité du Premier ministre : le SGDN

Les missions du Secrétaire général de la Défense nationale (SGDN) fixées par le décret du 25 janvier 1978, sont réparties en cinq grandes directions auxquelles s'ajoutent le secrétariat permanent du comité interministériel du renseignement et l'équipe du Haut responsable chargé de l'intelligence économique.



Le décret n° 96-67 [1] *prévoit que le Secrétaire général de la Défense nationale veille à la cohérence des actions entreprises en matière de sécurité des systèmes d'information (article 1). Il suit l'exécution des directives et instructions du Premier ministre et propose les mesures que l'intérêt national rend souhaitables. Il coordonne l'activité de tous les organismes concernés et assure que les relations entre ceux-ci répondent aux objectifs définis par le Premier ministre. Il veille au respect des procédures applicables à des utilisateurs privés en matière de sécurité des systèmes d'information. Il participe à l'orientation des études confiées aux industriels et suit leur financement (article 2). Il est tenu informé des besoins et des programmes d'équipement des départements ministériels et veille à ce que ceux-ci soient harmonisés.*

Plus précisément, **la DCSSI** [2] (Direction centrale de la sécurité des systèmes d'information) assiste le Secrétaire général de la défense nationale dans ses missions de sécurité des systèmes d'information qui répondent à deux objectifs principaux :

1 – **Assurer la sécurité des systèmes d'information de l'État** (administrations et infrastructures vitales).
2 – **Créer les conditions d'un environnement de confiance** et de sécurité propice au développement de la société de l'information en France et en Europe.

1. Décret nº 96-67 du 29 janvier 1996 relatif aux compétences du secrétaire général de la défense nationale dans le domaine de la sécurité des systèmes d'information (NOR : PRMX 9600002D).
2. Le décret 2001-693 précise les missions de la DCSSI.

Le budget 2005 du SGDN est de 56,7 M€ avec un effectif de 353 personnes, parmi lesquelles 110, en majorité de formation scientifique et technique, sont affectées à la DCSSI.

La DCSSI :

• **Contribue à la définition et à l'expression de la politique gouvernementale** dans le domaine de la SSI. au sein de la Commission interministérielle pour la sécurité des systèmes d'information **(CISSI)** [1], présidée par le SGDN.

• **Assure la fonction d'autorité nationale de régulation** dans le domaine de la SSI.
Dans ce cadre, la DCSSI :
– organise les travaux interministériels et prépare les mesures que le Secrétaire général de la Défense nationale propose au Premier ministre ;
– prépare les dossiers en vue des autorisations, agréments, cautions ou homologations délivrés par le Premier ministre, notamment pour l'application de la réglementation de la cryptologie, et en suit l'exécution ;
– met en œuvre les procédures d'évaluation et de certification du décret 2002-535 (certifications ITSEC et Critères communs) ;
– participe aux négociations internationales ;
– entretient des relations avec le tissu des entreprises de SSI.

• **Assiste les services publics dans le domaine de la SSI** : audit, veille et alerte d'incidents, conseil.
– **Audit et inspection** : chaque ministère et chaque grande entreprise a sa propre politique d'audit et d'inspection, effectuée par des ressources internes ou sous-traitée aux nombreuses sociétés privées commercialisant une telle offre. La DCSSI dispose d'une équipe chargée d'inspecter systématiquement la sécurité des systèmes d'information des ministères sur un cycle de trois ans. 8 personnes sont affectées à ces missions. La faiblesse de l'effectif conduit à limiter le nombre de ces inspections à seulement une vingtaine de déplacements par an sur les sites locaux et les organismes sous tutelles. Ces relevés ponctuels et les inspections de l'administration centrale aboutissent à des recommandations adressées au Directeur de cabinet du ministre concerné et du Premier ministre qui ont la responsabilité d'y donner suites.
– **Veille, alerte, réponse :** la DCSSI dispose d'un centre opérationnel de la sécurité des systèmes d'information, le **COSSI**, activé 24 heures/24 -7 jours/7, et créé dans le cadre de l'élaboration des plans de vigilance (VIGIPIRATE) volet SSI et (PIRANET). Le COSSI est chargé d'assurer la coordination interministérielle des actions de prévention et de protection face aux attaques sur les systèmes d'information. Il est composé d'une unité de Conduite & Synthèse (CEVECS) et d'une unité technique, le CERTA [2] (centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques). Chacune de ces unités regroupe une dizaine

1. Le décret n° 2001-694 précise le rôle de la CISSI.
2. Il existe d'autres Computer Emergency Response Teams (CERTs) français (CERT IST financé par des grands groupes industriels, CERT Renater pour les réseaux de recherche).

de personnes. Les ministères et les opérateurs d'infrastructures vitales sont invités à signaler au COSSI les attaques dont ils sont victimes.
– Conseil : la DCSSI conseille les ministères qui en font la demande dans l'analyse de risque, la préparation d'appels d'offres ou le suivi de grands projets. Le caractère facultatif du recours à la DCSSI est particulièrement préjudiciable à une prise en compte systématique de la SSI dans les grands projets. Elle peut également conseiller ponctuellement des groupes industriels. Cependant, il ressort des auditions que l'offre de conseil aux entreprises est insuffisamment développée et se révèle peu en phase avec les attentes du monde économique.

• **Développe une expertise scientifique et technique**. La DCSSI procède à l'évaluation des dispositifs de protection des services de l'État, analyse les besoins et propose des solutions propres à les satisfaire ; elle participe à l'orientation des études et du développement des produits ; elle formule une appréciation sur les produits qui lui sont soumis. Cette mission est menée par une équipe de spécialistes répartis dans trois laboratoires : cryptologie, signaux compromettants et architecture de systèmes.

• **Organise la formation dans le domaine de la SSI**
Sensibilisation et formation : la formation des personnels de l'Administration incombe principalement au Centre de formation à la sécurité des systèmes d'information (CFSSI) [1], même si des initiatives de contractualisation dans le domaine de la formation ont été entreprises en partenariat avec des grandes écoles sur le modèle de celle, très complète, de sensibilisation, délivrée à l'attention des cadres du secteur privé par les écoles du GET regroupant l'ENST, l'ENST Bretagne et l'INT.

L'objectif du CFSSI est double : dispenser une formation adaptée aux différents acteurs publics de la SSI et créer un réseau informel d'échanges avec les établissements d'enseignement supérieur et les centres de formations continues. À titre d'exemples le CFSSI propose plusieurs degrés de stages [2], allant de la simple sensibilisation au haut niveau de spécialisation, d'une durée d'une journée jusqu'à deux années de formation (c'est le cas pour le Brevet d'études supérieures de la sécurité des systèmes d'information (BESSSI) par exemple). En 2004, pas moins de 898 stagiaires avaient suivi l'une ou l'autre des formations [3].

De très grande qualité, d'après un grand groupe d'infrastructures vitales, celles-ci sont malheureusement restreintes aux personnels exerçant directement dans le domaine de l'informatique ou de la SSI. De plus, un déficit de notoriété de l'offre du CFSSI limite le recours à cette opportunité.

1. Décret 87-354 du 25 mai 1987.
2. cfssi@sgdn.pm.gouv.fr et www.formations.ssi.gouv.fr.
3. Source : auditions.

Une multiplicité d'acteurs insuffisamment coordonnés

Au-delà du SGDN, d'autres acteurs étatiques, en raison de leurs missions propres, interviennent dans la sphère de la société de l'information, développant des compétences dans le domaine de la sécurité. Cette partie, qui n'a pas vocation à être exhaustive, s'efforce de présenter les exemples les plus significatifs, ou résultant d'auditions.

Le ministère de la Défense, un acteur majeur à distinguer

Le ministère de la Défense assure deux missions SSI distinctes :
– une mission de sécurité interne, comme dans tous les ministères ;
– une mission technique chargée de la prise en compte de la sécurité dans les programmes d'armement et de la réalisation de produits de sécurité à vocation ministérielle ou interministérielle.

Contrairement aux autres ministères, le ministère de la Défense n'a pas de haut fonctionnaire de Défense (HFD) [1] et la responsabilité de la prise en compte de la SSI au ministère est dévolue aux autorités qualifiées (CEMA, DGA, SGA, CEMAT, CEMM, CEMAA, DGGN, DGSE, DPSD) [2], aux bureaux centraux de SSI, aux officiers de sécurité des systèmes d'information (OSSI) d'organismes centraux ou locaux et aux responsables de la sécurité des systèmes d'information (RSSI) de programmes ou de projets.

Une autorité qualifiée est responsable devant le ministre de la capacité des systèmes mis en œuvre à traiter les informations protégées (ou sensibles) au niveau de sécurité requis. Cette reconnaissance se traduit par la délivrance d'une homologation par l'autorité qualifiée.

La politique SSI du ministère de la Défense est intégrée dans la politique générale des systèmes d'information définie par le Secrétariat du Directoire des systèmes d'information [3].

Les Armées et la DGA possèdent chacune une entité constituée de spécialistes de la SSI, chargée en particulier de procéder aux audits des systèmes d'information dépendant de l'autorité qualifiée correspondante.

Chaque armée décline sa voie fonctionnelle SSI jusqu'à chacune de ses entités élémentaires, et affecte des personnels à l'OPVAR, organisation permanente de veille alerte réponse, au niveau de l'administration centrale.

Des missions particulières sont confiées au ministère de la Défense en SSI, dépassant son propre périmètre, c'est-à-dire l'emploi ou la préparation des forces. Accompagnée de l'instruction [77], la recommandation [4201] précise que le ministre de la Défense :
– est « maître d'œuvre des équipements ou moyens destinés à protéger les systèmes d'information gouvernementaux lorsque ces équipements ou

1. Cf. *infra*, p. 59.
2. Voir glossaire.
3. Bientôt DGSIC.

moyens sont susceptibles de satisfaire un besoin commun à plusieurs départements ministériels ou, lorsque le besoin est particulier, sur demande du département intéressé » ;
– a « la capacité d'apporter son concours aux contrôles et mesures que peuvent nécessiter les systèmes d'information en service dans les départements civils » ;
– est chargé de « doter l'État des équipes et laboratoires de mesures propres à satisfaire l'ensemble des besoins gouvernementaux. »

Au sein de la DGA, ces responsabilités particulières sont confiées au SPOTI, service de programmes de la DGA dédié à la conduite des programmes spatiaux, aux systèmes d'information et de commandement. Pour les travaux de réalisation des mécanismes cryptographiques, de réalisation des circuits, d'expertise technique sur la réalisation de produits et systèmes et d'évaluation, la DGA dispose d'une division du CELAR.

Au total, la voie technique SSI représente plus de 120 personnes, majoritairement ingénieurs et techniciens. Leur activité porte en priorité sur les solutions de sécurité destinées à protéger des informations classifiées de défense.

La DGSE (Direction générale de la sécurité extérieure) a pour mission d'évaluer la menace provenant de l'étranger qui pèse sur les systèmes d'information.

Exemples d'autres acteurs publics intervenant en matière de SSI

• Le ministère de l'Intérieur, de la Sécurité intérieure et de l'Aménagement du territoire

– **La DST** (Direction de la surveillance du territoire) : Dans le cadre de ses missions de lutte contre l'espionnage, de la lutte antiterroriste et de la protection du patrimoine économique et scientifique, la Direction de la surveillance du territoire (DST) assure des prestations techniques et informatiques, autour de trois volets : la prévention, la répression et la sécurité informatique.
L'activité de prévention de la DST s'exerce dans quatre domaines distincts qui représentent les pôles de compétence du service : la téléphonie, la criminalité informatique, les satellites et les matériels soumis à une réglementation (art R226 du code pénal). Pour ce faire, la DST entretient des relations avec les opérateurs de télécommunication (téléphonie, satellites, fournisseurs d'accès à Internet) et les sociétés de SSI, commercialisant des matériels pouvant porter atteinte à la vie privée, et les sociétés de cryptologie.
La DST assure également une veille permanente dans le domaine des TIC.
En matière de répression la DST dispose de pouvoirs de police judiciaire spécialisés concernant la sécurité des réseaux gouvernementaux et des établissements à régime restrictif (ERR).
La DST peut également se voir confier une mission d'expertise judiciaire consistant en l'analyse de supports informatiques lors des enquêtes judiciaires autres que dans le domaine du piratage informatique.

Enfin, la sécurité informatique est assurée au sein de la DST par le Bureau de sécurité des systèmes d'information. Celui-ci est chargé de l'application de la politique de SSI définie à la DST. En concertation avec les équipes réseaux, systèmes et développement applicatifs, il met en place les outils et procédures nécessaires pour s'assurer de la disponibilité, de la confidentialité et de l'intégrité des systèmes d'information.

– **L'OCLCTIC** : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.
En matière de lutte contre la cybercriminalité, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), structure nationale à vocation interministérielle et opérationnelle, a été créé en 2000 au sein de la Direction de la police judiciaire (DCPJ).
L'OCLCTIC est principalement chargé :
• d'animer et coordonner la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions liés aux TIC ;
• de procéder, à la demande de l'autorité judiciaire, à tous actes d'enquêtes et travaux techniques d'investigation ;
• de centraliser et diffuser l'information sur les infractions technologiques à l'ensemble des services répressifs (DCPJ, Douanes, Gendarmerie).

Le centre national de signalement sur Internet, composé à parité de gendarmes et de policiers, destiné au recueil et au traitement des signalements portant sur des messages et comportements inacceptables sur Internet, est placé au sein de l'OCLCTIC.

• **Le ministère de l'Économie, des Finances et de l'Industrie**

Comme pour les autres domaines technologiques, le Minefi contribue au financement de l'innovation en matière de SSI dans les entreprises par divers mécanismes d'aide, en particulier le crédit impôt recherche, et au travers d'OSEO-ANVAR dont il a la tutelle.

– **La DGE** (Direction générale des entreprises)
L'action en matière de SSI du service des technologies et de la société de l'information (STSI) de la direction générale des entreprises (DGE) est double : il assure le suivi d'une partie de la réglementation en SSI, notamment sur l'accréditation des acteurs liés à la signature électronique et dans le cadre de sa mission de subvention à la R&D collaborative finance des actions de soutien à la R&D en matière de SSI de toutes les actions du ministère : clusters EUREKA qui rassemblent des partenaires européens dans le domaine des télécommunications, du logiciel et des composants, pôles de compétitivité (en Île-de-France, en Provence Alpes Côte d'Azur et en Basse Normandie) et le programme spécifique Oppidum. Mis en place en 1998, le programme Oppidum dédié à la sécurité a permis le développement de solutions commerciales accompagnant la libéralisation de la cryptologie et la mise en place de la signature électronique. Même si la crise des technologies de l'information a ralenti la valorisation commerciale de certains projets, des avancées importantes ont été obtenues notamment en matière de signature électronique (mise en place de télé procédures et du schéma de qualification des prestataires), de protection

des réseaux d'entreprise (firewall, administration de réseaux privés virtuels, système d'infrastructure de gestion de clés en logiciel libre installé dans la plupart des ministères) et de sécurité des cartes à puce.

– **Pour ce qui est d'Oppidum** : le dernier appel à proposition en 2004, doté d'un budget limité à 4 millions d'euros, a rencontré un vif succès puisque 45 dossiers ont été déposés pour un total de 22 millions d'euros environ.

– **L'ADAE** :

L'Agence pour le développement de l'administration électronique, créée par le décret du 21 février 2003, publié au JO du 22 février, un service interministériel rattaché au ministre chargé du Budget et de la réforme de l'État.

L'agence pour le développement de l'administration électronique favorise le développement de systèmes d'information et de communication permettant de moderniser le fonctionnement de l'administration et de mieux répondre aux besoins du public.

Dans ce domaine :

• Elle contribue à la promotion et à la coordination des initiatives, assure leur suivi et procède à leur évaluation et apporte son appui aux administrations pour l'identification des besoins, la connaissance de l'offre et la conception des projets.

• Elle propose au Premier ministre les mesures tendant à la dématérialisation des procédures administratives, à l'interopérabilité des systèmes d'information, ainsi qu'au développement de standards et de référentiels communs.

• Elle assure, pour le compte du Premier ministre, la maîtrise d'ouvrage des services opérationnels d'interconnexion et de partage des ressources, notamment en matière de transport, de gestion des noms de domaine, de messagerie, d'annuaire, d'accès à des applications informatiques et de registres des ressources numériques.

Parmi ses missions, le volet sécurité regroupe toutes les activités nécessaires à la mise en place, en liaison avec la DCSSI, de l'infrastructure de confiance avec les outils, les référentiels, les guides méthodologiques (FEROS) et l'expertise (EBIOS).

La coordination des autorités certifiantes et l'élaboration des référentiels sont menées avec la DCSSI. La définition d'une carte à puce générique est conduite en lien avec les partenaires européens.

Dans le cadre de cette mission, l'ADAE développe des projets tels que la « **carte agent** », offrant des services de chiffrement et de signature, dont l'appel d'offres, en vue de son déploiement à destination des ministères, est prévu en novembre 2006. L'ADAE travaille à la mise en place **d'une offre de services de confiance mutualisés** (émission de certificats, validation, gestion de la preuve...), dont la mise en production est prévue en 2006.

Cette description des tâches montre la **difficulté à appréhender les responsabilités respectives de l'ADAE et de la DCSSI** en matière de sécurité des systèmes d'information.

• **La CNIL : Commission nationale informatique et libertés**

En matière de sécurité des systèmes d'information, la CNIL, autorité indépendante qui a pour mission essentielle de protéger la vie privée et les libertés individuelles ou publiques, s'intéresse essentiellement à **la confidentialité des données**.

La loi du le 6 août 2004 donne à la CNIL **une mission de labellisation de produits et de procédures.** Même si la réflexion engagée sur la problématique complexe du label ne permet pas encore de définir aujourd'hui la portée et le contenu de ce dernier, il semble probable que les aspects relatifs à la sécurité (sous l'angle de la confidentialité des données personnelles) seront essentiels. Quelle distinction peut-on faire entre un produit labellisé par la CNIL ou certifié par la DCSSI ? Quelles sont les ressources techniques dont dispose la CNIL pour accomplir cette mission ?

Cette même loi permet, mais n'oblige pas, aux entreprises de se doter d'un **correspondant informatique et liberté**. Là encore, il est difficile aujourd'hui d'évaluer l'attrait (et donc le succès futur) de cette possibilité, ni même le profil de ces correspondants. Cependant, il est admis que ces derniers devront posséder une excellente connaissance des problématiques de sécurité. Ainsi, nous pouvons légitimement attendre de ces correspondants une meilleure diffusion de cette culture de la sécurité informatique au sein des entreprises qui se doteront d'un correspondant.

La CNIL et la DCSSI ont commencé à travailler ensemble de manière quasi-informelle. Mais si la CNIL a, selon les termes de la loi, un pouvoir d'imposer que la DCSSI n'a pas, la DCSSI, en revanche, dispose, du fait de ses origines, de compétences techniques incontestables. Dans le cadre des expérimentations menées suite au rapport Babusiaux (transmission d'information de santé vers les assureurs complémentaires) le système de transmission sécurisée envisagé par la FNMF (fédération nationale de la mutualité française) a été audité par la DCSSI à la demande de la CNIL. Il devrait en être de même pour le dispositif transitoire envisagé par AXA (avant les déploiements de Sésame Vitale 1.40 chez les pharmaciens). Cette non-formulation peut-être très préjudiciable au bon fonctionnement de l'État.

Les conséquences de la multiplication des acteurs publics

La multiplication des acteurs publics dont les missions se chevauchent et les textes fondateurs peu précis, donne une impression générale de confusion et d'éparpillement des moyens et des hommes. C'est notamment le cas en matière de labellisation où l'ADAE, la CNIL et la DCSSI interviennent à un degré variable de coordination. Dans cette nébuleuse, l'acteur public dédié, le SGDN et plus précisément la DCSSI, souffre d'un manque d'autorité et parfois de crédibilité auprès des publics concernés. Ces deux facteurs : l'éparpillement des moyens et le manque d'autorité du SGDN nuisent à l'efficacité de l'État dans la définition et la mise en œuvre de la politique globale de SSI, cela d'autant plus que chaque ministère est responsable de son propre système d'information.

Comment s'étonner dès lors, que l'avis d'un haut fonctionnaire de Défense ne soit pas suivi d'effet, ou qu'une note du SGDN sur un appareil PDA reste lettre morte ? Quelle crédibilité apporter à la labellisation de produit par la DCSSI dans son secteur alors que la CNIL le fait dans le respect de ses prérogatives ? Quand l'ADAE conduit des missions parallèles qui sembleraient devoir ressortir de la compétence de la DCSSI ?

Chaque ministère est responsable de la sécurité de son propre système d'information : de fortes disparités dans l'organisation

Chaque ministère est libre d'appliquer les mesures de sécurité qui lui semblent pertinentes et adaptées à ses besoins. Cette liberté est cependant encadrée par des instructions générales interministérielles qui précisent la responsabilité des ministres, par exemple :

« La sécurité des systèmes d'information relève de la responsabilité de chaque ministre, pour le département dont il a la charge.
À ce titre, chaque ministre prend, dans les conditions fixées par le Premier ministre et sous son contrôle, des dispositions en vue de :
– développer à tous les échelons le souci de la sécurité ;
– apprécier en permanence le niveau de sécurité des installations ;
– recenser les besoins en matière de protection des systèmes d'information et veiller à ce qu'ils soient satisfaits.
Dans les départements autres que celui de la Défense, ces attributions sont exercées par les Hauts fonctionnaires de défense. »

• **Organigramme type proposé** :

Les directives IGI 900 et 901, proposent un modèle d'organisation :

– **Le haut fonctionnaire de défense (HFD)**
Dans chaque département ministériel, à l'exception de celui de la défense, le ministre est assisté pour l'exercice de ses responsabilités de défense par un ou, exceptionnellement, plusieurs hauts fonctionnaires de défense.
Le haut fonctionnaire de défense est responsable de l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information. Il contrôle en particulier les programmes d'équipement de son département. Il fait appel aux compétences du service central de la sécurité des systèmes d'information pour la spécification et l'homologation des produits et des installations.

– Le fonctionnaire de sécurité des systèmes d'information (FSSI)
Dans les départements ministériels qui utilisent des systèmes d'information justifiant une protection ou qui assurent la tutelle d'organismes ou d'entreprises utilisant de tels systèmes, le ministre désigne un fonctionnaire de sécurité des systèmes d'information (FSSI), placé sous l'autorité du haut fonctionnaire de défense. Lorsque la charge de travail n'est pas suffisante, le ministre peut charger le haut fonctionnaire de défense d'assurer lui-même les fonctions de FSSI.

Une équipe de sécurité des systèmes d'information, à la disposition du haut fonctionnaire de défense et du fonctionnaire de sécurité des systèmes d'information, peut être constituée si les besoins du département ministériel l'exigent.

– L'autorité qualifiée (AQSSI)

Les autorités qualifiées sont les autorités responsables de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'État, ainsi que dans des établissements publics et dans des organismes et entreprises ayant conclu avec l'administration des marchés ou des contrats. Leur responsabilité ne peut pas se déléguer.

– L'agent de sécurité des systèmes d'information (ASSI)

À tous les niveaux, les autorités hiérarchiques sont personnellement responsables de l'application des mesures, définies par les autorités qualifiées, destinées à assurer la sécurité des systèmes d'information. Elles peuvent, à cet effet, se faire assister par un ou plusieurs agents de sécurité des systèmes d'information (ASSI), chargés de la gestion et du suivi des ACSSI se trouvant sur le ou les sites où s'exercent leurs responsabilités, notamment lorsque la gestion et le suivi de ces articles nécessitent une comptabilité individuelle.

Les disparités dans la mise en œuvre de ce dispositif, ainsi que des difficultés à mobiliser les ressources nécessaires – en particulier des ressources humaines compétentes et dédiées –, et l'absence de pouvoir réel de ces acteurs de la SSI, rendent cette organisation inopérante. Il est fréquent de constater que les services informatiques ne suivent pas les fortes recommandations des HFD lors de choix de solutions pour des applications sensibles, sous couvert d'une stricte application du code des marchés publics.

Des ressources humaines insuffisantes

Le plan de renforcement de la SSI (**PRSSI**) approuvé, le 10 mars 2004, par le Premier ministre, faisait déjà état d'un « manque de spécialistes compétents en sécurité des systèmes d'information au sein des différentes administrations particulièrement alarmant ».

En effet, la pénurie de personnel formé, associé au manque de perspectives de carrière au sein de l'Administration et au niveau de rémunération proposé, n'encouragent pas les candidatures. Face aux difficultés de recrutement de personnels, les ministères sont contraints soit à privilégier la spécialisation interne [1], soit à recourir à l'externalisation [2].

1. Le centre de formation de la DCSSI (CFSSI) dispense gratuitement des formations en SSI. Cependant, un déficit de notoriété de l'offre du CFSSI et l'organisation du travail au sein des différents services, limitent le recours à cette opportunité.
2. Parfois retenue par certains ministères, le recours à l'externalisation doit être conditionné à un encadrement plus strict.

Ce constat ne doit pas occulter le fait que certains ministères aient mieux intégré la problématique SSI et s'appuient sur des équipes compétentes et motivées.

Approche technique des ministères : des faiblesses et un manque de cohérence

Les ministères s'équipent de manière autonome. L'hétérogénéité des matériels et logiciels utilisés, rend difficile une approche globale de la sécurité des systèmes d'information des administrations, par exemple :

– pour ce qui est de **l'architecture de sécurité**, si on peut regretter que la DCSSI n'ait pas un rôle plus directif dans ses missions de conseil, on constate cependant que des progrès ont été accomplis pour faire face à la menace externe. En revanche, la menace interne est insuffisamment prise en considération, en particulier lorsque des ministères disposent d'organes ou de services sous tutelle, le niveau de sécurité n'est pas toujours maintenu et garanti [1] ;

– pour ce qui est de **l'administration et de l'exploitation** qui reposent avant tout sur des méthodes et sur le personnel, le manque d'effectif formé et des faiblesses de méthodologies peuvent par exemple conduire à une gestion aléatoire des mises à jour de produits, ouvrant des vulnérabilités sur les systèmes ;

– de plus, aucune politique **« produits »** globale n'existe dans le domaine de la SSI, et notamment en matière de logiciels libres. C'est pourquoi, la solution consistant à « mettre en place une organisation conjointe de développement de produits de sécurité », présentée par le PRSSI, est à recommander.

Comparaison de la mise en œuvre de la SSI de cinq ministères auditionnés

Une analyse comparative de l'organisation, du budget consacré, de l'existence de schémas directeurs opérationnels, de la classification des données sensibles et de la mise en place de charte utilisateurs, des ministères de l'Intérieur, de la Défense, de l'Éducation nationale, des Affaires étrangères et de la Santé, révèle une hétérogénéité pour chacun de ces domaines :

• en terme d'organisation, il n'y a pas de séparation systématique de la fonction Sécurité des Systèmes d'information et de la Direction des services informatiques, comme il est préférable de le faire, et comme le font la quasi-totalité des acteurs privés auditionnés ;

1. Source : auditions

• corollairement à cette indifférenciation, il n'existe aucun chiffre précis du budget consacré à la SSI par ministère ;
• des schémas directeurs existent, la plupart sont en cours d'implémentation ;
• la classification des données sensibles (hors *confidentiel – défense* et – *secret défense*) ne semble pas obéir à une règle uniforme entre tous les ministères ;
• il n'existe pas, par ministère, une liste des logiciels associés aux applications traitant de ces données sensibles, démontrant une carence de l'attention portée aux solutions de confiance pour ce type d'application ;
• les chartes utilisateurs existent parfois, en cours d'élaboration pour certaines ou de mise en place pour d'autres ; en tout état de cause, il n'y a pas de règle précise concernant le descriptif précis de ces chartes, la manière de les appliquer, qui doit les signer, et à quel type de document les apposer.

Tout laisse à penser que cette analyse comparative de cinq ministères, est *a priori* généralisable à l'ensemble des ministères.

Les infrastructures vitales comportent une dimension de sécurité des systèmes d'information

L'État a la responsabilité, en relation avec les représentants des secteurs stratégiques économiques, de la protection des infrastructures vitales.

Les secteurs d'activités d'importance vitale sont les activités ayant trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense et à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables, ou peuvent causer un danger grave pour la population.

En France, le pilotage général de la protection des infrastructures vitales est confié au Secrétariat général de la Défense nationale, avec un rôle particulier pour le COSSI (centre opérationnel en SSI qui englobe le CERTA). La politique de protection comprend des inspections pratiquées régulièrement sur un ensemble de points et réseaux sensibles répartis sur le territoire, des plans de vigilance et d'intervention qui sont déclenchés lorsque les menaces augmentent significativement, et des exercices impliquant tout ou partie de l'appareil d'État et des infrastructures critiques.

De plus en plus, ces activités nationales s'élargissent à des actions coordonnées au plan international (Table top exercice impliquant

les pays du G8 en mai 2005) et européen avec notamment la préparation d'un Programme européen de protection des infrastructures critiques (EPCIP).

Un nouveau dispositif, en cours d'élaboration, formalisera la liste des secteurs, des opérateurs et des points d'importance vitale. Un des objectifs de ce nouveau dispositif est d'arriver à un nombre de points d'importance vitale sensiblement inférieur à celui des actuelles installations et points sensibles, afin de mieux les protéger.

Comment sont organisés nos principaux partenaires étrangers ?

Les ressources humaines des agences homologues de la DCSSI, peuvent être considérées comme un bon indicateur de la priorité politique accordée à ces questions : environ 3000 personnes à la *Division Information Assurance de la NSA* aux États-Unis, 450 *au Bundesamt für Sicherheit in der Infromationstechnik* (BSI) en Allemagne et 450 au *Communications Electronics Security Group* (CESG) au Royaume-Uni, contre à peine 110 à la DCSSI. Disposant de plus de moyens que la DCSSI, ces agences développent un véritable partenariat privé-public centré sur les produits de sécurité.

De manière générale, la conception et l'organisation anglo-saxonne de la sécurité des systèmes d'information se caractérisent par une approche unifiée des aspects défensifs et offensifs.

Les États-Unis : une doctrine forte, *l'Information dominance*

• Une agence offensive et défensive : la *National security agency* (NSA)

L'E*xecutive order* 12 333 du 4 décembre 1981 décrit les principales responsabilités de la NSA (*National security agency* créée le 4 novembre 1952). : ***« The ability to understand the secret communications of our foreign adversaries while protecting our own communications, a capability in which the United States leads the world, gives our nation a unique advantage ».*** Tout est dit en quelques mots sur le pouvoir que revêtent la maîtrise et la protection de son information pour un État.

La NSA a une double mission : protéger les systèmes d'information des États-Unis et obtenir des renseignements à partir d'interceptions et des écoutes d'autres pays. **La NSA est à la fois une agence de cryptologie et une agence de renseignement.** Elle emploie 3500 personnes et son budget n'est pas connu.

L'Information Assurance a pour missions de **:**
– fournir des solutions, des produits et des services ;
– de mener des opérations de protection des systèmes d'information ;
– d'assurer la protection des infrastructures critiques au profit des intérêts de la sécurité nationale des États-Unis. L'*Information Assurance Directorate* (IAD), est l'homologue de la DCSSI du SGDN.

La NSA mène des travaux sur l'instauration de mécanismes d'alerte face aux menaces sur les systèmes d'information et sur le renforcement de la protection des infrastructures vitales fondé sur la mise en œuvre d'un partenariat étroit avec l'industrie.

Le Directeur de la NSA est un général de corps d'armée.

Après les attentats du 11 septembre 2001, qui ont ébranlé l'image de marque de la NSA, la cybersécurité est devenue un enjeu de sécurité nationale fondé sur la définition de la stratégie nationale de sécurisation du cyberspace (*National Strategy to Secure Cyberspace*) du Critical Infrastructure Protection Board.

L'USA PATRIOT ACT, promulgué en octobre 2001, invite à la mise en œuvre d'actions nécessaires à la protection des infrastructures critiques, actions développées sous la responsabilité de partenariats public-privé. L'Office of Homeland Security (OHS) est établi par l'executive order 13 228 et est chargé de coordonner les efforts de protection des infrastructures critiques.

Prise en compte de la menace : veille, alerte, réponse : la création du Department of Homeland Security par regroupement d'agences auparavant dispersées est un premier pas. Les responsabilités du DHS en matière de sécurité du cyberespace concernent la direction *Information Analysis and Infrastructure Protection and Directorate* (IAIP) chargée de :
– développer un plan national de sécurisation des infrastructures critiques ;
– mettre en place un dispositif de réponses aux attaques sur la sécurité les systèmes d'information critiques ;
– assurer une assistance technique au secteur privé et aux administrations dans le cadre d'incidents sur les systèmes d'information critiques et coordonner la diffusion d'informations d'alerte et de protection ;
– encourager la recherche dans ces domaines techniques.

L'IAIP s'articule autour du National Infrastructure Protection Center (NIPC) qui couvre l'ensemble des menaces sur les infrastructures critiques et de la National Cyber Security division (NCSD) dont les missions sont l'identification des risques et l'aide à la réduction des vulnérabilités des systèmes d'information gouvernementaux et le développement de l'information sur la cybersécurité de l'ensemble de la société (universités, consommateurs, entreprises et communauté internationale) En mars 2003, le CERT Fédéral du FBI (FedCIRC) a été rattaché au DHS. Il a vocation à traiter prioritairement les administrations civiles.

Royaume-Uni : un partenariat public-privé très développé

En 2003, le Royaume-Uni s'est doté d'une stratégie nationale en matière de sécurité de l'information qui met l'accent sur le partenariat avec le secteur privé et comporte un volet plus particulièrement orienté sur l'information des entreprises et des usagers afin de faire régner l'ordre dans le cyberespace. Le Gouvernement a créé le Central Sponsor Information Assurance (CSIA).

Le *Communications and Electronic Security Group* (CESG) placé sous l'autorité du *Communication Government Head Quarter,* chargé de la protection des systèmes d'information de l'État, est l'homologue de la DCSSI. Au Royaume Uni, le NISCC [1], rattaché au Home Office, s'appuie sur l'UNIRAS (CSIRT gouvernemental) pour fournir aux opérateurs des infrastructures critiques des avis techniques, des informations sur les menaces, les vulnérabilités et les niveaux d'alerte. Il s'appuie aussi sur des WARP [2], chargé de recueillir des alertes et de signaler des incidents (mais sans capacité d'intervention) et des ISAC [3], qui diffusent des informations d'alerte et d'incident au sein d'une communauté donnée d'utilisateurs, généralement sur une base commerciale.

Un partenariat public-privé très développé : en 1999, le Royaume-Uni a créé, à l'initiative de plusieurs administrations, le National Infrastructure Security Co-ordination Centre (NISCC) qui englobe des missions plus larges liées à la gestion des risques telles que la protection des infrastructures critiques ou le partenariat avec l'industrie.

Le partenariat entre le secteur public et le secteur privé sur l'analyse des vulnérabilités des infrastructures vitales est érigé en système bien défini et s'organise autour de groupes composés de 30 personnes chargés de mettre en place l'échange d'informations. Le NISCC a mis en place des groupes pour 4 secteurs prioritaires : les finances, la sécurité des réseaux, les services externalisés des ministères et les systèmes de supervision de contrôles industriels (SCADA – *Supervisory Control and Data Acquisition*). Les secteurs des compagnies aériennes, des opérateurs d'Internet et des distributeurs feront l'objet du même plan d'action. Par ailleurs, le NISCC a formalisé avec les éditeurs de produits un protocole d'accord sur le partage d'informations sur les vulnérabilités articulé autour de neuf principes, dont l'objectif principal est de garantir la confidentialité absolue des informations transmises par le NISCC.

Le ministère de l'Économie et de l'Industrie poursuit sa procédure de tests fonctionnels des produits de sécurité, nommée GIPSI [4] et a émis deux premiers certificats (le niveau d'exigence est moins élevé que pour *les certificats critères communs*). Au CESG, les travaux se poursuivent sur le passeport électronique (délivrance des clés et évaluation du dispositif)

1. National Infrastructure Security Co-ordination Centre.
2. Warning, Advice and Reporting Point.
3. Information Sharing and Analysis Center.
4. General Information Assurance Products and Services Initiative – www.gipsi.gov.uk

pour une délivrance des premiers passeports à l'automne 2006. Par ailleurs, un nouveau programme de recherche (IADP [1]) a été mis en place afin d'optimiser les efforts dans le domaine SSI, en partenariat avec l'industrie.

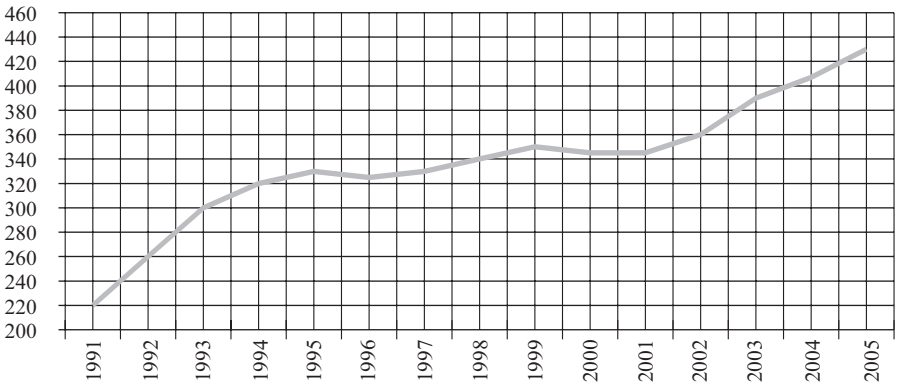
Allemagne : une politique produit forte très tournée vers les utilisateurs

L'Allemagne a adopté en juillet dernier, un plan national pour la protection des infrastructures d'information (NPSI) [2] qui comporte trois objectifs principaux :
– la prévention afin de protéger convenablement les infrastructures ;
– la préparation afin de répondre efficacement en cas d'incidents de sécurité informatique ;
– le maintien et le renforcement des compétences allemandes dans le domaine SSI.

Ce plan doit être maintenant décliné sous la forme de plans d'actions plus détaillés permettant sa mise en place dans le secteur public et dans le secteur privé qui est très concerné car il détient une grande partie des réseaux de communication.

La mise en œuvre de ce plan s'appuiera notamment sur le BSI, rattaché au ministère de l'Intérieur, qui est **responsable de la SSI en Allemagne**, homologue de la DCSSI. Il compte un effectif de **430 personnes** (contre 100 à la DCSSI) en croissance régulière depuis 2001.

Évolution du nombre de salariés du BSI



Les objectifs du BSI sont de sécuriser les systèmes d'information allemands.

Pour les atteindre, le BSI assure, auprès des utilisateurs quels qu'ils soient (administration, entreprises, citoyens) et des fabricants de technologies de l'information les missions suivantes :

1. Information Assurance Development Programme.
2. http://www.bmi.bund.de/nn_148134/Internet/Content/Nachrichten/Pressemitteilungen/2005/08/Information__Infrastructure__en.html .

– **Informer le pays :**

· en sensibilisant le public aux enjeux de la SSI par exemple par une information trimestrielle sur leur site Web et la production de CD-rom conçus pour les citoyens. L'industrie supporte cette initiative du BSI et fournit gratuitement des démonstrateurs ;

· en participant à des campagnes de sensibilisation des PME en 2004 (Sécurité de l'Internet pour les PME) ;

· le BSI réalise également des analyses de tendance et des futurs risques qui pèsent sur les systèmes d'information.

– **Fournir des conseils et des supports techniques dans le cadre d'un partenariat avec le privé très fort :**

· ainsi le BSI a créé un **standard** professionnel en 1993, une *IT Baseline Protection* (les bases de la protection d'un système d'information) remise à jour constamment qui est devenu un standard pour l'industrie. C'est un ensemble de bonnes pratiques qui permettent de sécuriser un système (CD-ROM ou 3 classeurs papier). Au départ, des grandes entreprises allemandes (SIEMENS, DAIMLER, VW, des banques...) se sont associées à cette initiative. La *baseline protection* est utilisée par le gouvernement et par les entreprises ;

· il assure du conseil et un support technique en sécurité des SI vers les agences gouvernementales par exemple l'initiative 2005 BundOnline ou la justice et la police ;

· il réalise des tests d'intrusion et apporte l'expertise sur la protection contre les bogues et les émissions radios. Ainsi, le BSI a une équipe spécialisée qui réalise des tests d'intrusion pour les ministères et les entreprises des secteurs sensibles ;

· la protection des infrastructures critiques est confiée au BSI qui a entrepris un travail d'identification de ces infrastructures, grâce à des exercices impliquant l'administration (ministères de l'Intérieur, de la Défense, des Transports, des Télécommunications) et des industriels. Dans ce cadre, il entretient des relations avec d'autres pays comme les États-Unis, la Suisse, la Suède et la Finlande ;

· le BSI conseille également les Länder sur le plan technique.

– **Analyser les risques, évaluer et tester :**

· le BSI assure la certification des produits et services de SSI (38 en 2004) ainsi que l'attribution de licences pour des applications classifiées ;

· il a une action particulière sur les procédures biométriques et des applications mobiles ;

· il conduit une analyse permanente de la sécurité Internet et de ses évolutions. Par exemple le BSI a une équipe spécialisée sur le projet de l'alliance TCG (Trusted Computing Group – cf. infra § 3.1) qui a des relations avec TCG mais qui recherche aussi des alternatives.

– **Développer des produits et des technologies SSI :**

Le BSI évalue et développe des équipements cryptographiques ainsi que des outils de sécurité et de modèles de sécurité formelle. Ainsi, le BSI participe à des projets à forte implication technologique : la carte santé (18 millions de cartes) la CNI-e avec 80 millions de cartes (carte d'identité) ou encore le passeport biométrique.

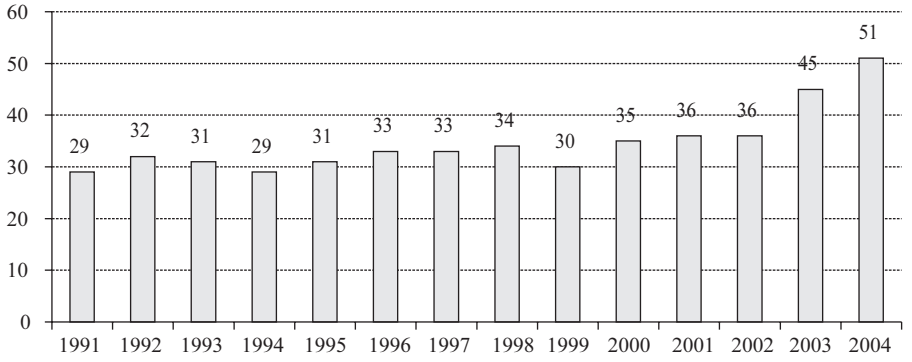
– **Assurer des fonctions opérationnelles :**

· assurer la fonction de CERT allemand (Computer Emergency Response Team) ;
· coordination technique du réseau d'information Berlin-Bonn ;
· administration de la PKI du gouvernement ;
· production de clés pour les équipements cryptographiques.

– **Jouer un rôle actif dans la normalisation et la standardisation :**

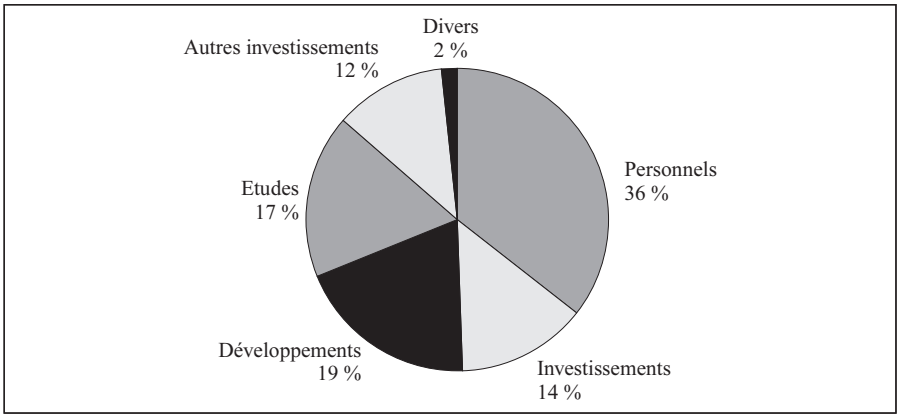
Le BSI joue un rôle actif dans les comités nationaux et internationaux de normalisation et de standardisation relatifs à la SSI.
Pour assurer l'ensemble de ces missions, le BSI dispose d'un budget significatif de **51 millions d'euros** en augmentation régulière depuis 2002.

Budget en millions d'euros du BSI



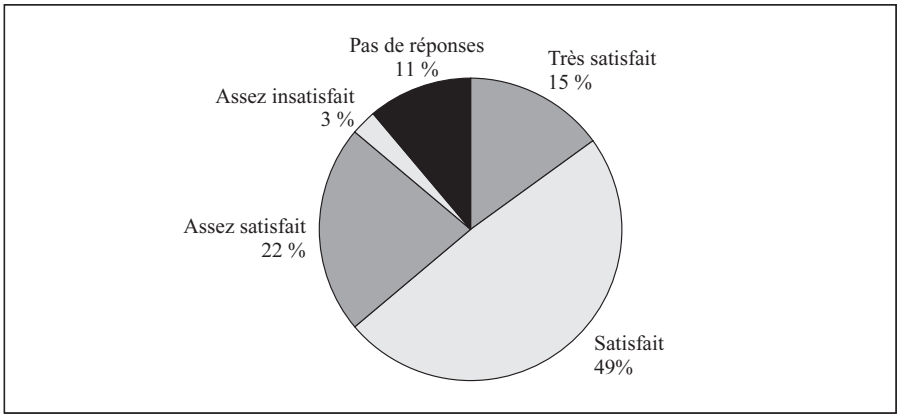
La répartition de ce budget, montre une action forte sur les développements, 10 M€, soit 19 % du budget et les études pour 9 M€ soit 17 % du budget que l'on ne retrouve pas en France.

Répartition des dépenses du BSI en 2004



Enfin, l'enquête de satisfaction réalisée par TNS-Emnid auprès de 500 experts de SSI afin de juger la qualité de cette politique volontariste du BSI, indique que 86 % des sondés sont satisfaits de son travail. La réputation très forte du BSI en Allemagne est une réalité.

Taux de satisfaction de l'action du BSI



La Suède, dont nous n'exposons pas ici l'organisation, mérite une attention particulière car le gouvernement met en place des mesures visant à renforcer la SSI

Un projet de loi a été présenté à l'été 2005 afin de mieux sécuriser les fonctions critiques de l'infrastructure Internet.

La commission parlementaire sur la sécurité de l'information a publié son rapport final en septembre dernier et prône la mise en place d'une nouvelle politique de sécurité de l'information en Suède ainsi qu'une réorganisation des services compétents en matière de SSI. Il est ainsi proposé de s'appuyer sur les compétences existantes en matière de renseignement électronique pour renforcer les capacités dans le domaine SSI et partager ainsi les responsabilités entre deux agences : la SEMA [1] pour les aspects organisationnels et l'IST [2] (appelé à remplacer le FRA [3]) pour les aspects techniques. Un projet de loi pourrait être présenté prochainement pour mettre en place l'ensemble de ces propositions.

Deux pays méritent une attention particulière. L'un témoigne de la montée en puissance rapide et efficace de l'Asie, **la Corée du Sud,** et l'autre la complémentarité entre la SSI et le ministère de la Défense, **Israël.**

1. Swedish Emergency Management Agency.
2. Institute for Signals Intelligence and Technical Infosec.
3. National Defence Radio Establishment.

Corée du Sud : une montée en puissance rapide des structures de lutte contre la menace informatique

À la suite de la journée noire du 25 janvier 2003 au cours de laquelle les réseaux d'information et l'économie coréenne ont été paralysés pendant plusieurs heures à cause d'un virus, le ministère de l'Information et de la Communication sud-coréen a créé une nouvelle organisation rassemblant les procureurs, la police et les services de renseignement en vue de prévenir l'attaque des infrastructures et des systèmes d'information et les perturbations qui en résultent. Le 20 juin 2003, le président sud-coréen Roh Moo-Hyeon a ordonné au National Intelligence Service (NIS) que des mesures soient prises pour faire face à ce type de situation. **Le National Security Council (NSC)**, structure de la présidence sud-coréenne, est chargé de définir la politique de lutte contre la criminalité informatique, de la mettre en pratique et d'assurer la coordination entre les différentes agences.

Le National Intelligence Service (NIS), agence nationale de renseignement placée sous les ordres de l'instance présidentielle, a décidé la création en décembre **2003 du National Cyber Security Center (NCSC) devenu opérationnel en février 2004**. Ce centre a pour mission d'intégrer les capacités et de regrouper les expertises des différents services et forces de sécurité, nécessaires et disponibles pour prévenir et lutter contre la criminalité informatique, principalement contre les sites officiels du pays. De fait, le NCSC traite de cyberterrorisme en général, sachant qu'il n'est pas fait de réelle différence entre la criminalité informatique et le terrorisme. Son directeur est issu du secteur privé. Le NCSC dispose de capacités offensives mais déclare ne pas se livrer à ce type d'activité. Auparavant, au mois de juillet 2002, le 6e Bureau (domestic affairs) s'était vu adjoindre le Cyber Crime Group dont le personnel pourrait rejoindre le NCSC.

Israël : le rôle prépondérant du ministère de la Défense

Israël dispose de compétences scientifiques et technologiques de haut niveau en particulier en ce qui concerne les technologies de pointe ayant des applications sur le marché de la sécurité des systèmes d'information fondés sur une politique très volontariste des autorités en terme de soutien à la formation et la recherche scientifique universitaire, le rôle du ministère de la Défense étant prépondérant. Compte tenu des évolutions rapides des technologies d'information et de communication et des menaces qu'elles engendrent intrinsèquement ou dans le cadre d'une utilisation malveillante, l'État hébreu s'est attaché à mettre sur pied une législation adaptée pour lutter contre la menace informatique, à mettre en place une politique globale de sensibilisation des acteurs susceptibles d'être la cible d'attaques et à renforcer son soutien financier en direction des sociétés qui développent des technologies de sécurité (firewall, cryptographie, biométrie, etc.)

Les autorités israéliennes, qui ont pourtant dans le passé montré leur clémence envers les pirates informatiques nationaux (cas du *hacker* Ehud Tenenbaum alias Analyzer par exemple), travaillent au renforcement de l'arsenal juridique du pays en matière de lutte contre la cybercriminalité.

Les sociétés israéliennes développent des capacités en matière de tests d'intrusion. Ainsi, Beyond Security a mené, au cours du premier trimestre 2004, un exercice de pénétration de sites Internet d'organisations sensibles. Cet exercice, qui a visé notamment la bourse du commerce de Tel-Aviv, la compagnie nationale de l'eau, la police israélienne, des municipalités ou encore un vendeur de livres par Internet, était limité à des actions de défiguration de sites Internet (modifications du contenu mis en ligne).

Cadre multilatéral : Union européenne, OCDE, ONU, G8, les réseaux de veille et d'alerte

L'émergence de la problématique de la protection des infrastructures vitales (ou critiques), dans un cadre multilatéral est récente. Elle résulte de la prise de conscience que les nouvelles menaces, attaques, virus, peuvent avoir des incidences directes et graves sur le fonctionnement des réseaux de l'État, des services publics et des entreprises, non seulement dans un cadre national mais également international.

• Activités européennes

La Commission européenne a publié en juin dernier une communication sur un nouveau programme dans le domaine de la société de l'information, faisant suite au programme e-Europe 2005 : « i2010 – Une société de l'information pour la croissance et l'emploi ». Dans son volet consacré à la mise en place d'un espace européen unique de l'information, la Commission annonce la publication d'une stratégie pour une société de l'information sûre, au cours de l'année 2006. Cette stratégie traitera entre autres de la sensibilisation en SSI, de la réaction rapide aux attaques et défaillances des systèmes, des moyens d'identification et d'authentification électroniques.

• Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

L'importance croissante accordée dans l'Union européenne aux questions de sécurité et la nécessité d'améliorer le partage de l'information et la coopération entre les initiatives nationales en la matière ont amené le Conseil et le Parlement de l'Union européenne à approuver, au début de 2004, la création d'une agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) [1]. Son principal objectif est de promouvoir le développement d'une culture de la sécurité des réseaux et de l'information au sein de l'Union européenne.

ENISA a vocation à être un centre d'expertise capable de « *prêter son assistance à la Commission et aux États membres, et de coopérer de ce fait*

1. Règlement 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'ENISA : European Networks and Information Security Agency.

avec le secteur des entreprises, en vue de les aider à satisfaire aux exigences en matière de sécurité des réseaux et de l'information, [...] garantissant ainsi le bon fonctionnement du marché intérieur ». Elle doit en particulier « *renforcer la coopération entre les différents acteurs dans le domaine de la sécurité des réseaux et de l'information, [...] en créant des réseaux de contacts à l'usage des organismes communautaires, des organismes du secteur public désignés par les États membres, des organismes du secteur privé et des organisations de consommateurs* ». L'une de ses premières tâches est d'établir un catalogue de compétences à l'échelle de l'Union européenne pour toutes les professions et tous les acteurs concernés par la sécurité des systèmes d'information. Outre ses fonctions de sensibilisation parmi les acteurs et « *la promotion des échanges des meilleures pratiques actuelles, y compris les méthodes d'alerte des utilisateurs* », l'ENISA doit « *fournir à la Commission des conseils sur la recherche en matière de sécurité des réseaux et de l'information* » et « *suivre l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information* ». D'autre part, son domaine de compétence ne s'applique nullement à des activités liées « *à la sécurité publique, à la défense, à la sécurité de l'État [...] ou aux activités de l'État dans le domaine du droit pénal* ». Il n'inclut pas d'activités opérationnelles ou de participation directe à la lutte contre la criminalité informatique. Enfin, l'ENISA devrait lancer une analyse à moyen ou long terme sur les risques actuels et émergents, améliorant ainsi la compréhension des questions de sécurité des réseaux et de l'information, mais elle n'est pas censée agir comme un CERT dans le règlement des incidents au jour le jour.
Le directeur de l'agence est un Italien, M. Pirotti, qui vient du secteur privé.

- **ONU**

Les Nations unies ont perçu très tôt les nouveaux enjeux, liés à la sécurité des systèmes d'information, dans leurs différentes composantes : juridiques, économiques et de sécurité nationale. Ainsi, depuis 1998, l'Assemblée générale a adopté plusieurs résolutions relevant de la 1ère commission sur les conséquences de l'utilisation des technologies de l'information et des communications (TIC) [1], de la deuxième commission sur le développement d'une culture globale de la cybersécurité [2] et de la troisième commission sur la lutte contre l'utilisation criminelle des technologies de l'information [3]. Ces résolutions ont permis entre autres d'élever au niveau international des travaux menés par des organisations plus régionales telles que l'OCDE, le G8 ou le Conseil de l'Europe. Elles ont également mis en place un groupe d'experts gouvernementaux chargé d'examiner les menaces potentielles et existantes dans le domaine de la sécurité de l'information et les mesures possibles de coopération à mettre en place afin de mieux les contrer. En raison de fortes oppositions entre les États-Unis et la Russie sur la prise en compte de l'utilisation des TIC à des

1. Résolutions nº 53/70 of 4 décembre 1998, 54/49 du 1er décembre 1999, 55/28 du 20 novembre 2000, 56/19 du 29 novembre 2001, 57/53 du 22 novembre 2002, 58/32 du 8 décembre 2003 et 59/61 du 3 décembre 2004.
2. Résolutions nº 57/239 du 20 décembre 2002 et 58/199 du 23 décembre 2003.
3. Résolutions nº 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001.

fins militaires, ces travaux n'ont pas abouti à ce jour mais pourraient donner lieu à moyen ou long terme à une nouvelle convention régissant l'utilisation des TIC aux dépens de la sécurité nationale et internationale et complétant le droit international dans ce domaine.

• **SMSI (Sommet mondial sur la société de l'information)**

L'UIT [1] et l'assemblée générale des Nations Unies ont décidé d'organiser un sommet mondial sur la société de l'information. La première phase du sommet, tenue à Genève du 10 au 12 décembre 2003, a permis l'adoption d'une déclaration de principes et d'un plan d'action, dont une section est dédiée à la sécurité de l'information et des réseaux. La deuxième phase du sommet, a eu lieu du 16 au 18 novembre 2005, et a consacré ses travaux au problème épineux de la gouvernance de l'Internet ; elle a notamment examiné la possibilité d'une internationalisation de la gestion des ressources de l'Internet.

• **OCDE**

Le groupe de travail sur la sécurité de l'information et la protection de la vie privée (WPISP [2]), qui dépend du comité PIIC (Comité de la politique de l'information, de l'informatique et des communications), se réunit deux fois par an à Paris au siège de l'OCDE. Il réunit des experts des 30 États membres de l'OCDE ainsi que des représentants du secteur privé et de la société civile. Il favorise le rapprochement des politiques publiques dans ce domaine par l'échange d'information et la promotion de bonnes pratiques. L'OCDE a émis en juillet 2002 des lignes directrices sur la sécurité des systèmes d'information et des réseaux [3] qui ont donné naissance à un nouveau concept : la promotion de la culture de la sécurité. Depuis cette date, le WPISP s'efforce de mieux comprendre les stratégies nationales mises en place pour répondre à ces lignes directrices et de cerner les nouveaux enjeux dans ce domaine, liés à l'évolution des technologies.

• **G8**

Sous l'impulsion de la présidence française du G8 en 2003, le thème de la protection des infrastructures critiques d'information, considéré jusqu'alors comme un sujet sensible, enjeu de la souveraineté nationale, a fait l'objet de travaux dans un cadre multilatéral. En mars 2003, une conférence ad hoc, co-parrainée par la France et les États-Unis, rassemblait pour la première fois des experts gouvernementaux et des grands opérateurs responsables des infrastructures d'information. L'adoption de 11 principes directeurs lors de la réunion ministérielle Justice-Affaires intérieures le 5 mai 2003 marquait cette première étape dans l'émergence d'une culture de sécurité face aux menaces informatiques. Les 11 Principes directeurs encouragent les pays du G8 à mieux protéger leurs infrastructures vitales en favorisant notamment la coordination internationale, la promotion d'un véritable partenariat entre le secteur public et privé ; le renforcement de la coopération bi et multilatérale ; la mise en œuvre des « bonnes pratiques » dans le domaine de l'alerte et de la veille informatique (CERT) ; la

1. Union internationale des télécommunications.
2. Working party in information security and privacy.
3. www.oecd.org/sti/cultureofsecurity .

conduite d'exercices communs pour tester les capacités de réactions en cas d'incidents ; la sensibilisation des autres pays à ces questions.
En mai dernier, le G8 a organisé un « Table Top Exercice », premier exercice sur les infrastructures critiques d'information impliquant les Administrations et l'industrie. Cet exercice a permis d'identifier des points de contacts au sein des CERTs, des services de police. La DCSSI, l'OCLCTIC ainsi que des représentants d'EDF et de RTE y ont participé.

Coopération internationale entre les CERTs

La mise en place de dispositifs d'alerte tels que les CERTs (Computer Emergency Response Teams) afin de pouvoir faire face à des attaques de virus ou à toutes sortes de nouvelles vulnérabilités nécessite de nombreux échanges entre les équipes aux niveaux national, régional et international. Pour la France, ces échanges ont lieu à l'échelle internationale au sein du FIRST [1] et à l'échelle européenne au sein de la TF-CSIRT [2] qui contribue également à la formation des nouvelles équipes. Enfin, la coopération étroite entre les CERTs gouvernementaux de six pays européens est très fructueuse.

La constitution de réseaux dans le domaine de la veille et de l'alerte est une nouvelle étape de la coopération internationale. Ainsi, la constitution actuelle du réseau IWWN (*International Watch and Warning Networks*) qui rassemble 15 pays, (États-Unis, Canada, Australie, Nouvelle Zélande, Royaume-Uni, Japon, Finlande, France, Allemagne, Hongrie, Italie, Pays-Bas, Norvège, Suède, Suisse) témoigne de l'objectif prioritaire pour les États d'une coopération renforcée en matière de cyber-sécurité. Les CERTs constitueront la colonne vertébrale de ce réseau pour lequel des outils de mise en œuvre sont identifiés (infrastructures de communication reposant sur un portail unique et un dispositif de secours).

Le monde de l'entreprise au cœur de la menace et de la problématique SSI

Le déplacement des enjeux et des risques vers l'économique

• Gérer le paradoxe de l'ouverture et de la protection

Le système d'information de l'entreprise est désormais déployé dans un contexte d'entreprise étendue permettant un travail en réseau avec ses clients ou usagers, ses fournisseurs, ses donneurs d'ordre, ses partenaires ou les représentants de l'administration. Ces échanges génèrent des vulnérabilités

1. Forum of Incident Response and Security Teams.
2. Task Force to promote the collaboration between Computer Security Incident Response Teams.

pour les systèmes d'information de l'entreprise vis-à-vis d'attaques potentielles contre lesquelles elle doit se protéger.
En outre, la généralisation des outils nomades (téléphones mobiles, PDA, ordinateurs portables...) et le passage au tout numérique gomment la frontière entre espace professionnel et espace privé, accentuent très significativement les risques.

• De nombreux sinistres identifiés dans les entreprises

Dans l'étude Clusif 2003 [1] qui met en évidence les principaux sinistres chez les grandes et moyennes entreprises on notera que :
– **41 %** des sondés déclarent avoir subi un sinistre dont 76 % n'ont procédé à aucune évaluation de l'impact financier ;
– les facteurs déclenchant se répartissent comme suit : infection par virus (35 %), panne interne (18 %), vol (15 %), perte de services essentiels (10 %), erreurs d'utilisation (8 %), évènement naturel (3 %).

Il est à noter que la menace stratégique, par exemple d'espionnage industriel, n'apparaît jamais dans les enquêtes, sans doute pour des questions de confidentialité et d'image.

• Des incidences économiques considérables

Les incidents dus à une défaillance de la SSI peuvent affecter l'ensemble des activités et du patrimoine de l'entreprise et peuvent conduire à :
– des perturbations ou des interruptions des processus clés de production de l'entreprise ;
– des pertes de parts de marchés (vol de technologies, de bases clients/fournisseurs...) ;
– des pertes financières directes :
• coûts d'immobilisation des installations de production ;
• coût du temps passé à la restauration des systèmes ;
• coûts techniques de remplacement de matériels ou de logiciels... ;
– une perte d'image et/ou de confiance des clients, partenaires et employés ;
– des actions contentieuses ou de mise en responsabilité liées à la fraude informatique ;
– une remise en cause des assurances de perte d'activité.

De manière moins visible mais plus lourde de conséquences, les actions d'espionnage industriel relayées parfois par des moyens étatiques vont se traduire pour les entreprises françaises par une perte de substance ou de compétitivité et au final par des incidences négatives sur l'emploi. Un parallèle s'impose avec les dommages causés par la contrefaçon qui représente un coût en France évalué à 6 milliards d'euros et le nombre d'emplois perdus à 30 000 par an [2].

1. Enquête intersectorielle auprès de 608 entreprises et 111 collectivités publiques (de 10 à 199 salariés : 54 %, 200 à 499 : 27 % ; 500 à 999 : 12 % ; + de 1000 : 7 %).
2. Source : Minefi.

• **Des conséquences financières et sur l'emploi sous-évaluées**

D'après une étude de l'institut américain en sécurité informatique CSI [1], menée en 2004 en partenariat avec le FBI (« Federal Bureau of Investigation »), une société perdrait **en moyenne** 204 000 dollars par an consécutivement aux incidents de sécurité informatique. Le « US CERT » américain quant à lui évalue à 506 670 dollars par an les conséquences financières des incidents de sécurité en entreprise.

La fiabilité de ces chiffres est très relative. D'une part, de nombreux responsables sécurité des systèmes d'information (28 % des participants) ne connaissaient pas le nombre d'attaques réussies survenues dans leur entreprise. D'autre part, même concrétisées, les conséquences de ces incidents et leurs coûts demeurent difficiles à évaluer.

Ainsi lors de l'étude sécurité 2005 du CERT, 62 % des personnes interrogées n'ont pu chiffrer précisément la perte annuelle engendrée par les incidents de sécurité informatique.

S'agissant des pertes d'emplois, il n'y a pas de données statistiques précises qui permettent d'avoir une vision précise du phénomène.

• **Des protections insuffisantes, en particulier dans les PME** (Étude Clusif 2003) :

– 10 % des entreprises n'avaient pas d'antivirus ;
– 64 % avaient une fréquence de mise à jour des antivirus insuffisante (une fois par semaine ou moins) ;
– 51 % seulement des répondants avaient installé des correctifs pour leur système d'exploitation ;
– 54 % des entreprises de plus de 1000 personnes avaient un plan de continuité, contre 16 % des PME de 10 à 199 personnes ;
– 44 % seulement des PME de 10 à 199 personnes disposaient d'un pare-feu contre plus de 90 % pour les plus grandes entreprises.

Or, plus de 70 % des entreprises, sont fortement dépendantes des systèmes d'information pour leur activité économique.

Ces premiers éléments chiffrés montrent bien une **perception** des menaces qui s'exercent sur les systèmes d'information dans les entreprises qui reste malheureusement **encore insuffisante** sur de nombreux points.

Un référentiel SSI partagé, des enjeux et des réponses spécifiques

• **L'impératif d'une approche globale, systémique et préventive**

La sécurité est certes liée à la fiabilité du système d'information, mais au-delà des équipements et des équipes en charge de leur sécurisation, elle implique pour les dirigeants de ces entreprises la mise en œuvre d'une

1. CSI/FBI Computer Crime and Security Survey - 2005 – Enquête auprès de 700 entreprises et organisations publiques américaines.

réflexion globale sur la maîtrise de ces risques impliquant l'ensemble de ses personnels ainsi que ses partenaires sur le périmètre de ses activités. Le déploiement de solutions de sécurité (produits ou services) et des procédures associées doit s'inscrire dans une démarche préventive, les investissements nécessaires pour couvrir raisonnablement et efficacement les menaces potentielles étant en général sans commune mesure avec les conséquences d'une attaque majeure qui pourrait se traduire par des pertes économiques ou d'image considérables voire à une perte d'indépendance ou à une cessation d'activité.

• Vers un référentiel commun de bonnes pratiques

Les pouvoirs publics, des cabinets de conseil spécialisés en SSI, des SSII, des éditeurs de logiciels, des fournisseurs de matériels de sécurité, des organisations patronales, notamment le Medef [1], et des organismes privés et publics divers ont formalisé des recommandations convergentes pour une démarche de sécurisation des grandes entreprises et des PME/PMI :
– bâtir une politique de sécurité ;
– connaître les législations en vigueur, les jurisprudences et les usages en vigueur dans chaque pays où les activités s'exercent ;
– alerter et activer les services compétents ;
– mettre en œuvre des moyens appropriés à la confidentialité des données ;
– sensibiliser et mobiliser les personnels par une charte d'utilisation, des campagnes régulières de formation et de sensibilisation ;
– mettre en œuvre un plan de sauvegarde ;
– gérer et maintenir les politiques de sécurité.

• À chaque entreprise sa propre démarche d'implémentation

Si les entreprises et les organisations sont toutes menacées, elles ne sont pas exposées au même niveau de risque. Il y a en effet des jeux de facteurs aggravants tels que :
– la taille et la complexité des activités ;
– le déploiement mondial des implantations et des systèmes d'information ;
– la nature des activités (nucléaire, défense, agro-alimentaire, réseaux d'infrastructures...) qui peuvent créer une attractivité en tant que cibles privilégiées pour des pirates, des terroristes, des concurrents ou des États ;
– la culture ou l'expérience en matière de sécurité et de protection acquises par l'entreprise et l'organisation.

Elles doivent donc adopter leur démarche à leur situation particulière.

1. Medef : Guide de sensibilisation à la sécurisation du systèmes d'information et du patrimoine informationnel de l'entreprise – mai 2005.

Mais des freins et un manque de maturité s'opposent encore à la mise en œuvre d'une politique SSI efficace dans les entreprises selon leur taille et expérience

Selon une étude récente de Ernst&Young [1], les obstacles principaux à la mise en œuvre d'une sécurité efficace des SSI sont les suivants :

Principaux obstacles à la mise en œuvre d'une SSI efficace	Monde	France
Faible prise de conscience des utilisateurs	45 %	**51 %**
Rythme des évolutions informatiques	31 %	**51 %**
Limites ou contraintes budgétaires	42 %	49 %
Absence d'un processus formel de gestion de la SSI	31 %	**45 %**
Engagement et sensibilisation insuffisant ou inexistant des cadres dirigeants	30 %	**43 %**
Communication inefficace avec les utilisateurs	27 %	**40 %**
Problème de cohérence entre les besoins en SSI et les objectifs métiers	26 %	**37 %**
Difficulté à justifier l'importance de la SSI	35 %	35 %

Source : Étude Ernst & Young – 2005

Cette même enquête souligne aussi les préoccupations majeures des grandes et moyennes entreprises et met en évidence l'attitude particulière des entreprises françaises dans de nombreux domaines par rapport à leurs homologues étrangères :

• **Un manque d'implication des directions générales**

La perception de l'importance de la sécurité par les directions générales reste faible. 90 % des responsables de la SSI (DSI ou RSSI) considèrent que la SSI est directement liée à l'atteinte des objectifs généraux de l'entreprise et seuls 20 % considèrent que la SSI est réellement une priorité de leur direction générale.

• **Une prise en compte insuffisante des facteurs humains**

Seulement 49 % des entreprises françaises ont conscience des risques de complicité interne, contre 60 % au niveau mondial. Or, 35 % des incidents ayant provoqué un arrêt du système d'information, ont pour origine la faute d'un salarié ou d'un ex-salarié. Dès lors, toute démarche efficace en matière de SSI doit s'accompagner d'un volet ressources humaines (sensibilisation, procédures, audits et contrôles).

Seulement 20 % des entreprises françaises assurent à leurs salariés une formation régulière sur la sécurité et la maîtrise des risques, contre 47 % des entreprises dans le monde.

1. La sécurité des systèmes d'information dans les entreprises françaises en 2004, vision comparée de la France et du monde, Ernst&Young, décembre 2004, Etude réalisée auprès de 1230 entreprises dans le monde dont 50 en France.

• **Des freins organisationnels**

Peu d'entreprises, même parmi les plus importantes, ont une approche de sécurité globale dont la SSI serait un volet parmi d'autres.

Dans l'étude Ernst&Young déjà citée, si au plan mondial, 85 % des responsables de la SSI jugent l'organisation de cette dernière efficace par rapport aux besoins des métiers, ils ne sont que 65 % à avoir cette opinion au plan français et à peine **un quart** des responsables métiers sont capables d'apprécier la valeur ajoutée de la SSI à leurs activités.

Contrairement à leurs homologues étrangers, les RSSI français portent une attention accrue sur les aspects technologiques et organisationnels qui l'emporte sur l'efficacité opérationnelle.

• **L'intégration de la SSI dans le modèle culturel de l'entreprise demeure une exception**

Très peu d'entreprises ont intégré dans leur modèle culturel et dans leurs processus opérationnels la SSI comme une priorité stratégique, une fonction vitale pouvant s'imposer dans la prévention, la réaction ou le temps de crise à toutes autres considérations économiques, commerciales ou financières majeures.

Le RSSI d'un grand groupe manufacturier [1] est ainsi rattaché directement au PDG. Il anime et contrôle une structure transversale « sécurité » qui croise et s'impose à la responsabilité SSI de chaque grande unité opérationnelle (cette structure matricielle est doublée d'une structure d'audit indépendante qui couvre également le domaine SSI). Il a tout pouvoir d'arrêter un dispositif opérationnel s'il juge que la politique de sécurité n'est pas respectée, même si cette décision est susceptible de générer des pertes financières significatives.

Il faut noter également la faible collaboration entre RSSI et audits internes (en France 40 % des RSSI avouent n'avoir aucune coopération avec l'audit interne et seuls 29 % déclarent plus d'une coopération par an).

• **L'identification des données sensibles est insuffisante**

Certaines entreprises, par leurs activités notamment liées à la Défense nationale, ont une pratique des données classifiées ou des données sensibles [2]. D'autres entreprises se sont appuyées sur ces méthodologies afin d'identifier, de classifier et de protéger de manière spécifique certaines informations sensibles.

Une réflexion préalable sur la nature des données sensibles de l'entreprise au regard des menaces qui s'exercent sur elle est indispensable. Or, dans la même étude, seuls **51 %** des répondants français (contre 71 % au niveau mondial), ont répertorié les informations sensibles ou confidentielles. Comment bien protéger quelque chose que l'on n'a pas identifié ?

• **Le retour sur investissement en matière de sécurité informatique est difficile à justifier**

Si pour de nombreux acteurs audités elle n'est pas essentielle et surtout n'a pas nécessairement de sens, la question du retour sur investissement se pose. Cependant, les pertes financières consécutives à des attaques informatiques étant souvent difficiles à cerner, peut-on et doit-on promettre aux directions

1. Source : auditions.
2. Source : auditions.

générales un retour sur investissement concernant les dépenses en sécurité informatique ?
D'après une étude du Clusif réalisée en 2004, 21,4 % des responsables en sécurité des P.M.E. de 200 à 499 salariés estiment que cette justification est effectivement nécessaire, mais dans les entreprises de plus de 2 000 salariés, ils ne sont plus que 7,5 %. Plus les dirigeants sont informés de leur responsabilité civile ou pénale, moins ils exigent de justifier une dépense en sécurité informatique par un rendement particulier. Ainsi, pour plus de 26 % des responsables sécurité, la première justification des investissements en sécurité est désormais de se conformer aux réglementations. Ce taux atteint 37,5 % dans les grandes entreprises.
L'étude CSI/FBI 2005, précise en outre que seules 25 % des entreprises prennent une assurance extérieure contre les risques de menaces informatiques. La menace reste sous-estimée.

• **Le budget SSI souvent insuffisant**

Les responsables SSI considèrent que l'un des principaux obstacles à leur mission est la limitation des budgets notamment dans les PME/PMI (29,7 % contre 21,8 % dans les grandes entreprises).

Selon l'étude CSI/FBI 2005 : 27 % des sondés dépensent plus de 6 % de leur budget informatique en SSI, près d'un quart de 3 à 5 %, autant de 1 à 3 % et 25 % moins de 1 % ou ne savent pas. Les grandes entreprises françaises sensibilisées dépensent quant à elles en moyenne 6 % de leur budget informatique en SSI [1]. La motivation à investir dans la SSI varie de manière considérable selon la taille de l'entreprise.

Des modèles organisationnels diversifiés pour parer aux menaces et risques informatiques

Quelques exemples d'organisations [2]

Les organisations mises en place par les entreprises, en particulier les plus grandes, méritent l'attention.

Quelques points clés se dégagent :

– **Gouvernance** : présence de comités des systèmes d'information qui rendent compte devant le comité exécutif des groupes. L'opérationnel est assuré par des directions générales des systèmes d'information qui assurent la coordination et la maîtrise d'œuvre des systèmes d'information dans le groupe.

– **Politiques de sécurité** : en complément d'une politique de sécurité générale, qui intègre des règles, des instructions et des recommandations, mise en œuvre de politiques complémentaires SSI dédiées :
· en cas de crises ;

1. Source : auditions.
2. Source : auditions.

· pour les filiales ;
· pour les réseaux sans fil ;
· pour les fournisseurs ;
· pour les personnels (internes, administrateurs systèmes, missionnaires, expatriés...).

– **Budgets** : des budgets SSI correspondant à 6 % du budget informatique.

– **Organisation** :
· la présence de RSSI rattaché à une direction en charge de la sécurité des systèmes d'information au niveau groupe et des RSSI par branches ou filiales ;
· un suivi régulier des plans d'actions validés par la Direction Générale ;
· des cellules de veille et de crise activées en 24 heures, 7 jours /7 ;
· une externalisation croissante d'un certain nombre de fonctions mais pas d'externalisation globale ;
· la réalisation en interne ou sous-traitée de tests d'intrusion ;
· la réalisation d'audits sur les différentes entités des groupes.

– **Personnels** :
· des formations/sensibilisations pour **tous** les personnels ;
· la **signature de chartes** (cf. annexe XI pour des exemples) d'utilisation des systèmes d'information par tous les salariés. Celles-ci peuvent être annexées au contrat de travail ou faire partie du règlement intérieur des entreprises.

– **Aspects techniques** :
· existence de solutions redondantes pour les systèmes critiques et des évolutions en cours pour disposer de solutions de secours général ;
· sécurisation des postes individuels et des nomades ;
· sécurisation de l'accès aux réseaux privés des entreprises et à Internet ;
· la sécurisation des données sensibles devient une priorité conduisant à l'utilisation croissante du chiffrement de tous les flux échangés pour l'accès aux données techniques, financières... stockées dans des banques de données ;
· renforcement croissant des contrôles d'accès (sécurisation de l'authentification, gestion et contrôle des habilitations, authentification forte...) ;
· logique de hiérarchisation : l'accès aux systèmes d'information est possible de l'intérieur ou de l'extérieur selon des droits affectés à la personne, à sa fonction et au niveau de sécurité de son poste au moment de la connexion ;
· sécurisation en cours des données et des accès des partenaires ;
· approches spécifiques pour les dirigeants.

– **Moyens spécifiques** :
· l'utilisation de cartes à puces pour les salariés dans leur accès au système d'information se généralise ;
· la fonction PKI (Public Key Infrastructure) s'implante de manière croissante dans les organisations.

Une montée en puissance de l'infogérance de sécurité

La définition d'une politique SSI, sa mise en œuvre et sa maintenance peuvent être assurées par des ressources internes, par une sous-traitance à un prestataire de services informatiques ou par l'utilisation des services mutualisés à distance par des MSSP [1] (tests de vulnérabilité, cartographie des flux applicatifs, gestion des moyens de protection, gestion des identifications/authentifications...).

Même si les RSSI, à une large majorité, ne confieraient pas l'ensemble de l'administration de la SSI à un prestataire unique comme le montre l'enquête CSO d'avril 2005 [2] dans laquelle la sécurité est gérée en interne à 82,4 %, la montée en puissance de l'infogérance en France se confirme. En effet, selon l'enquête IDC Sécurité 2005 [3], en moyenne 60 % des sondés font appel à des prestataires externes pour intégrer les solutions de sécurité et 43 % pour définir la politique de sécurité. Enfin, 39 % des sondés confient certaines activités de leur politique de sécurité à une société d'infogérance, parmi lesquels 26 % externalisent l'ensemble de l'administration de la sécurité de leur système d'information.

Selon un sondage LOGICACM [4] les motifs d'externalisation sont liés principalement à la réduction des coûts (89 %) et l'accès à de nouvelles technologies (60 %) et d'après le Syntec [5], la croissance de l'activité d'infogérance informatique, qui intègre également de la SSI, sur 2005 a été de plus de 10 % et devrait se poursuivre sur 2 006.

On peut cependant noter que certaines entreprises expérimentent des modèles hybrides, par exemple BNP Paribas qui a créé une *joint venture* avec IBM pour gérer une partie de son activité informatique mais qui a gardé en interne la maîtrise de la sécurité, la relation avec les métiers et la gestion des applications [6].

L'inventaire et l'élaboration de la politique de sécurité imposent généralement l'intervention de consultants externes qui doivent s'inscrire dans une relation de partenaires de confiance car ils seront amenés à identifier les cibles potentielles ou les failles des systèmes d'information. Ainsi, les RSSI souhaitent à une large majorité que la certification des prestataires soit obligatoire.

Cette demande est en outre en phase avec la mesure F4 du PRSSI visant à qualifier des prestataires privés en sécurité des systèmes d'information, qui propose :

1. Managed Security Service Provider.
2. CSO Entreprise & Sécurité de l'Information – Enquête auprès de 144 entreprises de plus de 200 salariés.
3. Enquête IDC Sécurité 2005 -103 entretiens auprès d'un panel de grandes entreprises et administrations en France composées à 45 % de plus de 2000 salariés et 55 % de 1000 à 1999 salariés – novembre 2005.
4. Source : l'Agefi.
5. Source : Syntec et 01 Informatique.
6. Source : l'Agefi.

– de procéder à un inventaire des processus de qualification des métiers de la SSI en concertation entre le secteur privé et public et sous l'égide de l'AFNOR ;
– de définir les procédures de qualification des prestataires ;
– de faire en sorte que cette qualification soit requise pour la passation de marchés publics.

Ainsi, le besoin de disposer d'un corpus réglementaire encadrant ces activités est nécessaire pour réellement rassurer les entreprises et notamment les PME sur la qualité des prestations en particulier s'agissant de la confidentialité et des compétences mises en œuvre. À cet effet, les récents travaux conduits par l'AFNOR, le CIGREF et le SYNTEC sur ce thème sont à signaler.

La SSI n'est pas suffisamment opérationnelle dans les entreprises françaises

• Une capacité insuffisante à répondre à un risque d'accident grave

Il n'y a que 30 % des entreprises françaises du panel de l'enquête Ernst & Young qui estiment pouvoir faire face à un risque d'incident grave et pouvoir assurer leur continuité d'activité (47 % pour le reste du panel mondial). Si beaucoup d'entreprises ont mis en place une organisation SSI et des plans de continuité, il est cependant très inquiétant de constater que plus d'un tiers des entreprises, françaises ou mondiales, reconnaissent ne pas tester leur plan de continuité de l'activité (31 %), leur plan de secours informatique (21 %) et/ou leur plan d'intervention d'urgence suite à un incident (30 %).

• Le cadre juridique de la SSI est mal maîtrisé et les moyens juridiques à l'international doivent être renforcés

Les nombreuses dispositions législatives et réglementaires qui s'appliquent à la SSI procèdent de trois grandes préoccupations majeures dont certaines peuvent parfois être antinomiques :
– les atteintes aux droits de la personne ;
– les atteintes aux systèmes d'information ou l'usage délictueux de l'informatique ;
– les menaces spécifiques sur les activités liées à la Défense et à certaines activités sensibles.

Les contraintes réglementaires sont nombreuses et exigeantes : art. 226-16 à 24 (traitement des données à caractère personnel) et art. 323-1 et suivants (renforcés par la Loi du 21 juin 2004 pour la confiance dans l'économie numérique : atteinte aux systèmes de traitement automatisée des données) du code pénal, CNIL, Loi Sarbannes-Oxley, Loi de Sécurité Financière, groupement Visa...

Par exemple la loi Sarbannes-Oxley, votée par le Congrès en juillet 2002, suite aux affaires Enron et Worldcom, implique que les Présidents des entreprises cotées des États-Unis certifient leurs comptes auprès

de la Security and Exchange Commission (SEC), l'organisme de régulation des marchés financiers US. Cette loi est guidée par 3 grands principes : l'exactitude et l'accessibilité des informations, la responsabilité des gestionnaires et l'indépendance des vérificateurs/auditeurs.

Selon l'étude CSI/FBI 2005, cette loi a eu comme conséquences pour près de 50 % des entreprises d'augmenter le niveau d'intérêt pour la sécurité des informations.

En outre, à l'instar des dirigeants d'entreprises, la responsabilité civile et pénale des DSI et RSSI est aussi de plus en plus invoquée devant les tribunaux qui peuvent infliger des peines de prison.

Si le dispositif législatif et réglementaire qui encadre la SSI sur le périmètre du territoire national est globalement satisfaisant, un effort significatif doit être engagé pour le porter de manière pédagogique à la connaissance des entreprises. En effet, la conformité à la réglementation constitue un levier significatif de progrès pour convaincre les dirigeants de mettre en œuvre des plans d'action SSI.

Cependant, il existe une disproportion de jugement chez les magistrats, pour qui une intrusion physique au sein d'un établissement bancaire sera considérée comme plus grave qu'une intrusion par mode informatique, alors que les préjudices financiers conséquences de ce dernier peuvent être plus significatifs [1].

Enfin la France ne dispose pas, comme par exemple les États-Unis, des moyens juridiques permettant des poursuites efficaces contre des attaques exercées à partir de territoires étrangers notamment contre de grandes entreprises.

Les besoins des entreprises : des outils et des architectures certifiés, des produits clés d'origine nationale ou européenne et une industrialisation de la maintenance

• Le besoin impératif d'outils et d'architectures certifiés

En matière de produits, les entreprises expriment une forte demande de produits certifiés tels que :
– techniques et protocoles cryptographiques (chiffrement de messages, signature électronique, sécurité des transactions commerciales...) ;
– fabrication de réseaux virtuels privés ;
– pare-feu matériel et/ou logiciel ;
– systèmes de détection d'intrusion et de surveillance réseaux, systèmes antivirus ;
– filtrage de contenus, antispams... ;
– tatouage électronique ;
– cartes à puces et infrastructures associées ;
– identification biométrique...

1. Source : auditions.

Cette attente n'impose pas pour autant que l'ensemble des éléments de la SSI soit produit par une filière française et certifiée par une autorité étatique française.

Le **premier niveau d'exigence** pour l'ensemble des entreprises concerne la qualité des produits du marché destinés à faire face à des menaces génériques (spams, virus, tentatives d'intrusion « standards »...). Le souhait des RSSI est de disposer de produits labellisés par une autorité (publique ou privée, nationale ou internationale) qui a pu vérifier qu'ils étaient globalement bien construits et répondaient aux fonctionnalités avancées par le fournisseur.

Le **deuxième niveau d'exigence** couvre le cercle des grandes entreprises internationales et des PME/PMI sensibles. Dans ce dernier cas, le souhait des RSSI est de pouvoir disposer, à défaut d'une offre complète, de briques conçues par des entreprises françaises ou européennes permettant, associées à des architectures de systèmes spécifiques SSI, d'accéder à une sécurité plus efficace et certifiée par une entité digne de confiance, la DCSSI.

Le **troisième niveau** est de pouvoir disposer à moyen terme :
– d'outils permettant d'identifier clairement la personne à l'origine d'un fichier donné ;
– d'outils offrant en temps réel une protection complète d'un réseau ;
– d'outils permettant un suivi et un contrôle efficace du niveau de sécurité du réseau ;
– de moteurs de recherche indépendants des solutions anglo-saxonnes type Google ou Yahoo.

• La nécessité d'industrialiser la maintenance de la SSI et la diffusion des correctifs logiciels

La maintenance au fil de l'eau 24 heures/24 et 7 jours /7 et la garantie de déploiement des mises à jour sur l'ensemble du parc dans des délais généralement de l'ordre de l'heure ou de la demi-heure constituent un enjeu majeur pour la majorité des responsables de SSI des grandes entreprises.
Cela exige des solutions techniques fiables et certifiées, un processus régulier de déploiement des correctifs de sécurité et une équipe de supervision en alerte permanente prête à intervenir à l'arrivée de nouvelles failles de sécurité des systèmes d'exploitation et à réagir aux déploiements de nouvelles menaces.

Les entreprises attendent de l'État des services de support efficaces et accessibles

• L'identification du bon interlocuteur

Les entreprises qui ne disposent pas d'expertises internes ou de connaissances précises de l'organisation de l'État ont des difficultés à identifier rapidement le bon interlocuteur [1] parmi les nombreux services de l'État.

1. Source : auditions.

Elles souhaiteraient pouvoir disposer d'un guichet unique permettant :
– d'accéder aisément à des expertises pour qualifier rapidement la menace à laquelle elles sont confrontées et de disposer de plans d'action ou de moyens méthodologiques ou techniques susceptibles de la contrer, d'identifier ses auteurs et de rassembler les preuves du délit pour la justice et les assurances ;
– de les assister dans les dépôts de plaintes auprès des services les plus compétents en fonction de l'infraction (financière, espionnage, mœurs, terrorisme...).

Du point de vue des entreprises, plus d'une vingtaine d'organismes ou programmes dédiés SSI ont été mis en place par l'État ou par des initiatives privées suscitant de facto une grande perplexité lorsque des problèmes apparaissent.

Cette organisation génère un chevauchement des compétences et une absence d'optimisation des ressources qui rend la coordination des actions défensives ou d'investigations extrêmement complexes et se traduit généralement par un manque d'efficacité et de réactivité alors que les attaques se font plus précises, rapides et violentes.

• **Les entreprises françaises sont confrontées à des contraintes particulières dans leurs activités internationales**
Les grands groupes français déployés à l'international conjuguent par nature toutes les contraintes :
– d'une organisation complexe ;
– d'une organisation s'exerçant dans des environnements variés, parfois hostiles ou pouvant coopérer avec des concurrents ;
– de cadres législatifs ou réglementaires à l'étranger insuffisamment connus et mal maîtrisés.

Les entreprises intervenant à l'international souhaitent disposer d'un support efficace des services de l'État pour les accompagner face aux risques spécifiques de l'international : veille, alertes, informations sur les menaces, conseils (juridiques, procédures, méthodologie, outils et solutions, architecture, informations des personnels), capitalisation d'expérience, identification de prestataires de confiance, appui auprès des autorités locales (étrangères et françaises), gestion de crise via le Quai d'Orsay (évacuation des expatriés, etc.)...

En outre, l'interdiction ou la limitation du chiffrement dans certains États devient problématique pour la politique de sécurité de grands groupes [1].

1. Source : auditions.

Les problématiques spécifiques des PME face à la SSI

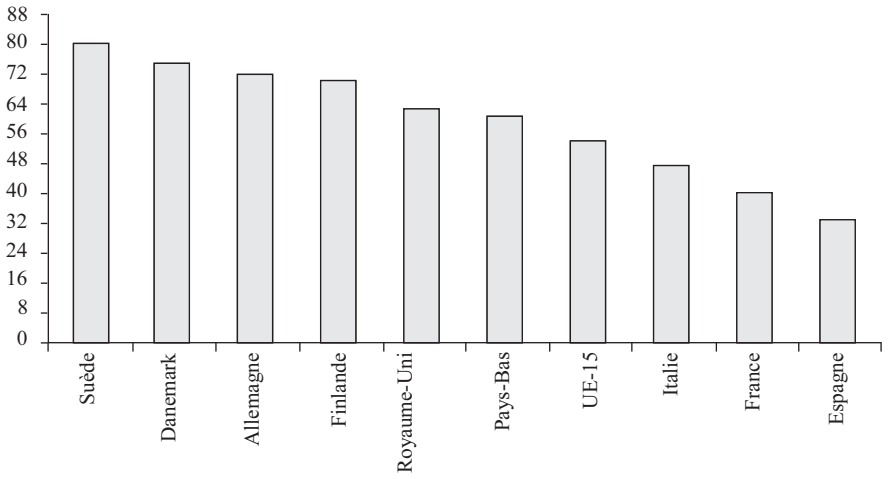
Un retard des PME dans l'usage des TIC explique en partie leur manque de maturité face à la SSI

Ce retard des PME françaises et de la France en général, dans l'usage des TIC, qui a été présenté au § 1.5.3 est également attesté par les éléments chiffrés ci-après issus de l'étude de la mission pour l'économie numérique 2004 [1], relatifs à la proportion des entreprises disposant d'un site sur Internet fin 2002. La France, l'Italie et l'Espagne affichent des taux d'équipements nettement inférieurs aux autres pays.

• **Les PME françaises sont elles-mêmes de taille plus réduites.**

Les entreprises françaises sont, en moyenne, plus petites que les entreprises européennes, qui sont elles-mêmes plus petites que les entreprises américaines. L'appétence des entreprises pour les investissements TIC va croissant avec leur taille compte tenu des coûts financiers pour de tels investissements.

Proportion des entreprises disposant d'un site sur la Toile en pourcentage des entreprises



Source : Eurostat – enquêtes TIC 2002-2003 – publication 2004

Ces données sont confirmées par cette même étude de la Mission pour l'Économie Numérique, selon laquelle la proportion des entreprises françaises disposant d'un site Internet est de 65 % pour une taille supérieure à 250 salariés et **de 38 %** pour les **PME de 10 à 250 salariés.**

1. Mission pour l'économie numérique – tableau de bord du commerce électronique de décembre 2004 – 6e édition – Services des études et des statistiques industrielles (SESSI) – Ministère délégué à l'Industrie.

• **Le tissu industriel est encore très manufacturier**

La part manufacturière est plus importante qu'aux États-Unis alors que ce sont les industries de services qui sont les plus consommatrices de TIC : cette seconde explication du retard des PME françaises est confirmée par la Mission Économie Numérique.

Une absence de moyens et de compétences suffisants expose les PME

De tailles plus réduites et disposant de moins de moyens que les PME de pays concurrents, les PME françaises sont confrontées à :
– une difficulté pour investir dans les TIC et la SSI, qui risque de les exclure des chaînes de fournisseurs ;
– une quasi-impossibilité de s'appuyer sur des compétences fortes en SSI et plus généralement en TIC.

• **Conséquences du développement de la logique d'entreprise étendue**

Le concept d'entreprise étendue, que l'on peut définir comme un ensemble d'entreprises indépendantes du point de vue capitalistique mais qui travaillent pour des clients communs, un marché spécifique ou pour un produit identifiant un marché (automobiles...), prend une ampleur qu'il convient de ne pas négliger. L'entreprise étendue est désormais considérée comme un levier de performance dont **les technologies de l'information sont une composante essentielle** avec en particulier les technologies EDI, le trio Internet/intranet/extranet, datawarehouse [1], workflow [2]...

Compte tenu de l'importance des TIC dans cette nouvelle organisation, le traitement de la problématique SSI devient primordial. Selon une étude réalisée par l'éditeur Novell [3] auprès de 80 décideurs informatiques sur la zone EMEA (Europe, Moyen-Orient et Afrique), le premier critère des entreprises pour choisir un outil de collaboration en temps réel est **la sécurité (69 %),** loin devant la conformité à la réglementation (13 %) et l'interopérabilité (13 %).

La tendance sera donc de voir **les grands groupes imposer progressivement des impératifs de sécurité à l'ensemble de leur chaîne de fournisseurs.** Un rapprochement doit être opéré avec le processus qui a conduit à la mise en œuvre d'une politique « qualité ». Rappelons que l'action de l'État en matière de politique « qualité », à travers les DRIRE (MINEFI), a consisté notamment à prendre en charge une partie significative des dépenses engagées par les entreprises pour la mise en conformité aux normes ISO 9000 et la formation du personnel. Cette politique avait réellement permis à de nombreuses PME de progresser en matière de qualité, mais également de soutenir l'activité des sociétés de conseil sur ces thématiques. Une politique similaire pourrait être envisagée en matière de certification de sécurité.

1. Stockage de données.
2. Outils informatiques de gestion de flux de travail des entreprises qui permet d'optimiser leurs processus métiers clés.
3. Source : *Le Monde Informatique*.

Ainsi, l'AFNOR [1] constate un intérêt croissant porté à la politique de sécurité induit par la norme ISO 17799 (issue de la norme BS 7799).

• **Le développement de l'infogérance de sécurité**

Les tendances du marché et surtout les positionnements pris par de nombreux acteurs informatiques le démontrent, **les PME apparaissent comme un futur marché en croissance en matière d'infogérance et de services de sécurité informatique** afin de compenser leurs déficiences internes qui les obligent à externaliser cette fonction.

Ainsi des opérateurs industriels, filiales de groupes étrangers asiatiques, sont en train de préparer des offres orientées sur les entreprises disposant de 50 à 500 postes principalement des PME, laissant les entreprises de plus de 1 000 postes aux SSII [2]. Les PME confiant à des tiers le cœur de leur société, sont dans une situation de faiblesse par rapport à l'offre de sociétés de services bien plus importantes.

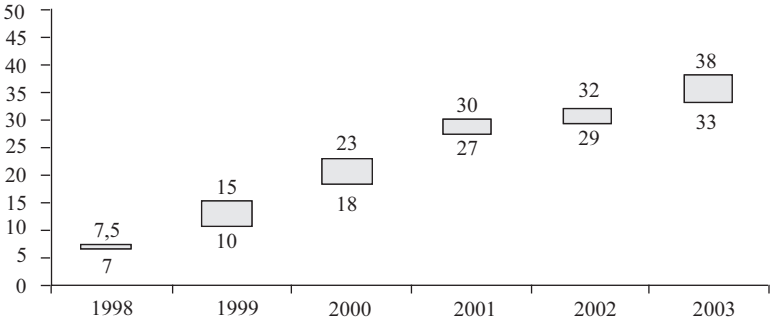
Une sensibilisation des citoyens insuffisante et une protection faible de leurs ordinateurs personnels

L'augmentation régulière du nombre d'internautes français, 24 millions en juin 2004 en hausse de 10 % par rapport à 2003, et le développement du commerce électronique, 38 % environ des internautes ont effectué des achats en ligne en France en 2003, doivent s'accompagner d'une meilleure sensibilisation des citoyens en matière de sécurité des systèmes d'information.

En effet, malgré la perception des menaces, le sentiment d'évoluer dans un univers libre, où l'on fait ce que l'on veut, prédomine. À l'exception de l'antivirus, pas toujours mis à jour, **la maturité des usagers n'est pas suffisante** pour faire face aux menaces qui pèsent sur ses équipements individuels. Pourtant ces menaces peuvent porter atteinte à la protection de la vie privée. Elles demeurent également un frein au développement des nouveaux usages des TIC (commerce électronique, e-administration...) qui nécessitent une confiance des citoyens dans l'outil qu'ils mettent en œuvre.

1. Source : auditions.
2. Source : *01 Informatique*.

Internautes ayant effectué des achats en ligne en France
en % des internautes – estimations en valeurs minimum et maximum



Source : Ipsos Corporate, GfK, Benchmark Group, Jupiter MMXI, NielsenNetRatings

Rappelons également qu'une chaîne de sécurité repose sur son maillon le plus faible. **L'ordinateur personnel du citoyen peut notamment être utilisé comme une passerelle pour des attaques sur des systèmes plus importants** (ordinateurs « zombis »). Il est donc particulièrement nécessaire d'améliorer la sensibilisation du citoyen en matière de SSI.

La campagne lancée récemment pour prévenir les internautes de ne jamais divulguer de données personnelles, en particulier sur les « Chats », va dans le sens d'une meilleure prise de conscience des risques. Il est à noter également la première semaine nationale de la sécurité informatique du 3 au 10 juin 2005 [1]. Ce type d'action est à amplifier.

Conclusion partielle, une prise de conscience insuffisante et des organisations non-matures

La France accuse un retard préoccupant face aux impératifs de sécurité des systèmes d'information, tant au niveau de l'État qu'au niveau des entreprises, quelques grands groupes mis à part.

Malgré les prémices d'une prise de conscience de la nécessité de se doter d'une politique en SSI, la situation de l'État apparaît encore fragile. Une sensibilisation insuffisante, une confusion des responsabilités, **le manque d'autorité des responsables de la SSI dans les administrations**, le sous-effectif en personnels dédiés, et l'absence de politique d'achat globale, multiplient les vulnérabilités. Les entreprises, surtout les grandes, semblent mieux sensibilisées mais hésitent peut-être à investir

1. Source : Délégation aux usages de l'Internet.

dans ce domaine n'étant pas pleinement conscientes des conséquences économiques d'une atteinte à l'intégrité de leurs systèmes.

Pourtant la sécurité des systèmes d'information est un enjeu national à caractère stratégique, politique et économique.

Dans une logique de souveraineté, la France et l'Europe peuvent-elles aujourd'hui se doter des moyens d'assurer de manière autonome la protection de leurs infrastructures et de leurs systèmes ?

Chapitre III

Une base industrielle et technologique spécialisée en SSI autonome pour répondre aux enjeux économiques et de souveraineté

Conduire la France à un **niveau de sécurité et d'autonomie** acceptable face aux menaces qui s'exercent contre les systèmes d'information français, privés ou publics, nécessite d'agir sur l'offre nationale et européenne.

La plupart des segments du marché SSI sont couverts par une offre étrangère. Aussi, pour atteindre une autonomie nécessaire à l'indépendance de notre pays, la mise en œuvre d'une politique spécifique pérenne est indispensable. Il importera de favoriser **l'existence et le développement d'un tissu industriel et technologique de confiance**, **autonome et spécialisé** sur certains points critiques des systèmes d'information, d'une taille minimale mais suffisante pour être viable, compétitif et créateur d'emplois, composé non seulement de centres de recherche, de grandes entreprises mais **également de PME.**

Le secteur des TIC, dont fait partie la SSI, peut se caractériser de manière synthétique par :
– son caractère totalement mondialisé avec des fournisseurs performants et des utilisateurs répartis à travers le monde ;
– une vitesse très rapide des évolutions technologiques et des usages ;
– une complexité croissante conséquence d'une explosion des usages qui orientent les marchés, avec la prolifération des terminaux et produits de toutes sortes.

Pour pouvoir survivre et éventuellement se développer dans cet environnement économique spécifique, la taille et les financements ne sont pas suffisants ; **la qualité, l'adaptabilité, la réactivité et la créativité sont indispensables.** Ainsi, au côté des grands groupes, la présence de PME innovantes performantes est une **condition nécessaire** à l'atteinte des objectifs recherchés en matière de SSI.

Un marché de la SSI en forte croissance mais dont les volumes sont limités

Le marché en matière de produits, logiciels et services en sécurité des systèmes d'information est intrinsèquement difficile à délimiter tant techniquement que financièrement. Quelques exemples illustrent cette difficulté :
– la réalisation d'un système d'information est susceptible d'inclure des prestations pour la sécurité de ce système qui ne sont pas identifiées ;
– les systèmes d'exploitation sont rarement inclus par les études de marché dans les logiciels de sécurité. Pourtant un système d'exploitation évolué inclut pourtant toujours de nombreux mécanismes de sécurité et ces mécanismes sont souvent le socle de la SSI ;
– les prochaines générations de microprocesseurs doivent intégrer de nombreuses fonctions de sécurité – chiffrement, vérification de l'intégrité et l'authenticité de codes exécutables, vérification de DRM [1]. Ils ne sont pas habituellement inclus dans le marché de la SSI ;
– certains logiciels permettant la virtualisation de matériels ne sont devenus des logiciels de sécurité que depuis que leur utilisation est envisagée pour réaliser des fonctionnements multiniveaux.

Le marché de la sécurité des systèmes d'information concerne les seuls matériels, produits logiciels et services principalement destinés à la protection de la confidentialité, de l'intégrité, de la disponibilité ou l'authenticité d'information ou d'un système d'information.

La segmentation du marché de la SSI

Cette segmentation s'appuie sur une analyse de trois critères principaux : les besoins à satisfaire qui recouvrent les aspects « produits », les clients, et les technologies mises en œuvre.

• **Des besoins multiples à satisfaire**

Selon une étude Ernst&Young [2] réalisée auprès de 1 230 entreprises, grandes et moyennes, dans 51 pays dont 50 en France, l'origine des besoins et donc **de la demande** apparaît multiple : exigence commerciale de continuité de service, obligations légales ou réglementaires, préoccupations d'image et protection du patrimoine de l'entreprise par rapport aux concurrents. Les besoins d'un État relèvent d'exigences de souveraineté et de sécurité des biens et des personnes.

1. Digital Right Management (gestion des droits numériques) : protection des contenus vidéos et audios, notamment soumis à des droits d'auteur, diffusés sur Internet.
2. La sécurité des systèmes d'information dans les entreprises françaises en 2004, vision comparée de la France et du monde ; Ernst&Young, décembre 2004.

Pour répondre à ces besoins, les attentes concernent des **produits logiciels** (antivirus, pare-feux...), des **matériels** (cartes à puces, systèmes biométriques...) et **des services** (architectures sécurisées, infogérance de sécurité...).

• **Des clients aux exigences diversifiées**

La demande en sécurité des systèmes d'information vient du secteur institutionnel et gouvernemental, des entreprises et du grand public.
Le secteur institutionnel et gouvernemental se distingue par des exigences réglementaires voire légales, la nécessité pour certains ministères de prendre en compte la menace stratégique, des conditions de contractualisation complexes et lentes et des budgets contraints.
Les entreprises se distinguent par une sensibilité à la sécurité et des moyens extrêmement variables, des politiques d'achat sous contraintes de prix et de pérennité, de standardisation des produits achetés, et des exigences réglementaires de source nationale ou européenne (notamment les banques).
Le grand public se distingue par un système d'information souvent limité à une ou à quelques machines, un niveau technique très variable et une connaissance de la sécurité souvent limitée aux virus et aux spams.

• **Les technologies de sécurité**

Elles sont le fondement du développement des produits et conditionnent ainsi directement la qualité de la SSI.

Les technologies essentielles de la sécurité des systèmes d'information sont par exemple :
– *les systèmes d'exploitation ;*
– *la conception d'architectures de sécurité, l'ingénierie logicielle sûre, la preuve logicielle, la preuve de protocoles et les méthodes d'évaluation associées ;*
– *la cryptographie, pour fournir des mécanismes de confidentialité, intégrité, preuve et authentification ;*
– *les dispositifs électroniques de protection de secrets (cartes à puces...) ;*
– *les méthodes applicatives de filtrage (antispam, antivirus...), de modélisation du comportement et de détection d'intention (intrusions...) ;*
– *le matériel avec des composants et circuits intégrés sécurisés.*

Il existe une gamme de produits et technologies pour répondre aux différents besoins de sécurité. Ils ne constituent pas des alternatives, mais doivent être utilisés de façon combinée pour assurer la protection requise. Les technologies de base sont :
– *identification/authentification par mot de passe (à usage unique ou pas), biométrie, carte à puce ou clé USB, combinaison de ces technologies ;*
– *signature électronique ;*
– *chiffrement ;*
– *effacement sûr.*

Ces solutions sont mises en œuvre dans différents types de produits de sécurité :
– *sécurité des réseaux : VPN (Virtual Private Networks, en français Réseaux Privés Virtuels), matériel/logiciel de chiffrement de liaison (standardisé ou non) ;*

– sécurité du poste de travail : Firewall logiciels et/ou matériels, antispam, antivirus, Contrôle parental ;
– sécurité des contenus : logiciel de chiffrement de fichier (standardisé ou non), Digital Right Management (DRM) pour le multimédia ;
– contrôle d'accès : cartes à puce et terminal associé, capteur biométrique ;
– Trusted Platform Module (TPM).

En complément des produits, il est nécessaire de prendre en compte les services de sécurité qui accompagnent la mise en œuvre de ces produits. Aux services traditionnels (gestion des clés et autres services de certification) se sont ajoutés des services plus commerciaux (conseil, audit, exploitation de la sécurité des réseaux). Comme dans le reste des TIC, ils constituent une activité en croissance plus forte que celle des équipements et plus difficilement délocalisable :
– infrastructure de gestion de clés (IGC) ;
– services de certification électronique (horodatage...) ;
– processus d'évaluation et de certification ;
– single Sign On et Fédération d'identité ;
– conseil en SSI (audit, recommandation, formation) ;
– management et surveillance des réseaux.

Parmi ces technologies et produits certains sont critiques pour la garantie d'un haut niveau de sécurité et devraient être de source française ou européenne, par exemple : des composants cryptologiques, des systèmes d'exploitation multi-niveaux, des processeurs de confiance, des dispositifs de gestion de clés, les PKI...

En outre, il conviendrait d'initier des études complémentaires visant à élargir les possibilités offertes par les logiciels libres (par exemple les systèmes d'exploitation).

Le marché de la sécurité est en forte croissance

Selon l'enquête IDC Sécurité 2005 [1], les dépenses informatiques globales sur le marché professionnel en **France** devraient atteindre en 2005, 41 009 M€, en croissance de 3,5 %.

Les dépenses de sécurité informatique, des entreprises et des administrations atteindraient 1 113 M€, en hausse de 17,4 % (contre 15,4 % de hausse entre 2003 et 2004). Parmi ces dépenses de sécurité informatiques en 2005 :
– les services représentent 612 M€ (55 %) en hausse de 15,5 % ;
– les logiciels représentent 405 M€ (36,4 %) en hausse de 16,4 % ;

1. Enquête IDC Sécurité 2005 -103 entretiens auprès d'un panel de grandes entreprises et administrations en France composées à 45 % de plus de 2000 salariés et 55 % de 1000 à 1999 salariés – novembre 2005.

– les appliances (boîtiers physiques intégrant de une à plusieurs fonctionnalités : pare-feu/VPN, antivirus, antispam, prévention et détection d'intrusion... (Cf. Annexe XII pour les définitions) représentent 96 M€ (8,6 %) en hausse de 37,1 %.

Un taux de croissance moyen de 17,2 % est attendu pour le marché de la SSI sur la période 2005-2009 pour atteindre 2 100 M€ (administrations et entreprises) :
– pour les services, le taux de croissance annuel devrait atteindre 19 % en 2009 ;
– pour les logiciels, il est prévu une baisse du taux de croissance à partir de 2007 qui ne serait plus que de 12,3 % en 2009.

En Europe, les marchés des produits logiciels de sécurité les plus attractifs en 2003 étaient :
– le Royaume-Uni avec 600 M$ de CA en croissance de plus de 20 % ;
– l'Allemagne avec 560 M$ en croissance de plus de 20 % ;
– la France avec 353 M$ en croissance d'environ 5 %.

La faible croissance du marché français pourrait s'expliquer par un retard dans l'usage des TIC et d'une prise de conscience tardive des enjeux de la SSI.

Concernant les matériels, la croissance est réelle sur certains produits :
– les cartes à puce, dont le taux de croissance en volume [1] attendu sur 2005 est de 18 % avec 1 727 millions d'unité après une croissance de 12 % en 2004 ;
– les systèmes biométriques, qui devraient représenter environ 1 M$ au niveau mondial en 2007.

Caractéristiques de quelques marchés logiciels et matériels de SSI

Des données complémentaires sont fournies en annexe XII sur les différents logiciels et matériels de SSi : antivirus, coupe-feu, détection d'intrusion, administration sûre, authentification renforcée, VPN, sécurité messagerie, chiffrement de fichiers, mémoires de masse et téléphone chiffrant.

1. Source : *Les Echos* / Eurosmart.

Selon IDC 2005 [1]

Segment	Croissance du marché/an (2004-2009)	Marché national (M€) en 2004	Principaux acteurs	Présence française	Produit logiciel libre public	Criticité des produits
Logiciels : Antivirus, Antispam et Spyware (segment SCM [2])	16 %	157	Symantec, Network Associates (MC Afee), Trend, Sophos...	Non	Oui, ClamAV	Non
Pare – feux/VPN (appliances)	2 %	47	Check Point, Cisco...	PME	Oui, netfilter, IP filter	Oui
Pare-feux (logiciels)	5 %	44				Oui
Prévention et détection d'intrusion (appliances)	22 %	11	Symantec et Internet Security Services (50 % du marché à 2)	PME	Oui, Snort	Oui
Administration sûre (3A) [3]	13 %	88	IBM, Computer Associates, Verisign...	GE [4] et PME		Oui

[1] Enquête IDC Sécurité 2005 -103 entretiens auprès d'un panel de grandes entreprises et administrations en France composées à 45 % de plus de 2000 salariés et 55 % de 1000 à 1999 salariés – novembre 2005
[2] Secure Content Management – Cf. annexe 12
[3] 3A pour Authentification, Autorisation et Administration – ou management des identités et de l'accès – Cf. annexe 12
[4] GE : Grande Entreprise

Une offre nationale en situation de faiblesse sur la partie produits logiciels

En France, les fournisseurs de produits ou services en SSI sont :
– de grands groupes, certains liés au marché de l'armement : Thalès, Safran, EADS, Bull, France Télécom ;
– des SSII ;
– des industriels du marché de la carte à puce ;
– une centaine de petites et moyennes entreprises, souvent à forte valeur technologique.

Au niveau européen, les autres fournisseurs se trouvent principalement au Royaume-Uni et en Allemagne.

Le classement IDC 2003 [1], selon le chiffre d'affaires réalisé en Europe en 2003, uniquement dans le domaine des logiciels liés à la SSI, montre que les leaders sont américains avec Symantec (405 M$ de CA et 16 % de parts de marché), Computer Associates (EU [2]), Check point (Israël-

1. IDC 2003, Western European security software forecast and competitive vendors shares, 2003-2008.
2. EU : États-Unis.

EU), Network Associates (EU), IBM (EU), Trend micro (EU), Sophos (RU [1]), Verisign (EU), Panda (EU), Microsoft (EU).

Cette situation globale de faiblesse européenne dans le domaine des logiciels par rapport à l'offre américaine est un fait établi qui évoluera difficilement dans les années à venir et qui impose de facto de concentrer l'effort public et privé sur des segments clés en matière de sécurité permettant d'atteindre un niveau d'autonomie acceptable.

Concernant les matériels, par exemple les systèmes biométriques et cartes à puces, la France dispose encore d'atouts à faire valoir au niveau mondial qu'il convient d'accompagner de manière volontariste.

Les marchés de la carte à puce en 2005

	Télécoms	Banque/ Finance	TV	Gouvernement/Santé	Transport	Sécurité
Volumes en millions d'unités	1 220	330	65	60	25	15
% de croissance	+ 16 %	+ 18 %	+ 18 %	+ 33 %	+ 67 %	+ 25 %

Source : *Les Echos* / Eurosmart

D'un volume relativement faible, les marchés gouvernementaux (cartes d'identité, cartes vitales) et de la sécurité (application d'authentification forte, accès aux systèmes d'information) affichent des taux de croissance importants. Les programmes à venir de passeports et de cartes d'identité qui devraient générer un marché de plusieurs centaines de millions d'unités seront un moteur de la croissance de ce secteur. En outre, le développement des cartes sans contacts, déjà utilisées pour les péages d'autoroutes, devrait être significatif dans les années à venir avec, par exemple, des applications de paiement sans contact avec un téléphone mobile. Selon Gartner Dataquest, ce marché devrait atteindre 500 millions d'unités en 2008.

L'industrie française, qui fait partie des leaders mondiaux, doit profiter de ces opportunités de croissance.

Caractéristiques de quelques segments du marché des services de sécurité informatique

Selon l'étude IDC Sécurité 2005, le marché des services de sécurité devrait passer de 612 M€ à 1 195 M€ en 2009, soit un taux de croissance moyenne de 18,2 % par an sur la période 2004-2009.

1. Royaume-Uni.

Segment	Croissance du marché/an (2004-2009)	Marché national (M€) en 2004	Marché national (M€) en 2009	Présence française	Criticité
Gestion de la sécurité – infogérance	18,8 %	113	267	GE et PME	Oui
Conseil en sécurité	17,8 %	152	345	GE et PME	Oui
Implémentation	17 %	211	463	GE et PME	Non
Formation	16,7 %	55	119	GE et PME	Non

Parmi ces différents segments du marché des services de sécurité, le conseil et l'infogérance méritent des précisions complémentaires compte tenu de leur criticité.

Le conseil en sécurité d'un système d'information est directement lié à son architecture. Les principales sociétés en informatique ont donc développé une activité forte en conception d'architecture de sécurité et quelques PME se sont spécialisées dans le conseil en sécurité des systèmes d'information.

• **Infogérance de la sécurité**

Les services infogérés dans ce domaine se sont développés, en particulier aux États-Unis, car ils permettent de mutualiser l'expertise, de valoriser des centres de recherche et de veille permanentes, afin d'offrir une capacité d'analyse et de réaction 24 heures sur 24, 7 jours sur 7. Les niveaux de service sont différenciés, depuis un simple support aux équipes internes jusqu'au management global de la sécurité.

Le développement de ces services est cependant freiné par l'absence de critères objectifs de confiance indispensables puisque l'infogérance de sécurité ouvre à des tiers l'accès au cœur des entreprises.

Le développement de cette activité, qui contribuerait largement à améliorer la protection des entreprises et des organisations en la confiant à des professionnels compétents, passe donc par une labellisation des sociétés de confiance.

• **L'exemple de la montée en puissance des opérateurs d'Infrastructures à clés publiques (ICP)**

Les ICP sont l'ensemble des moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer avec des systèmes cryptographiques asymétriques (cf. Annexe III – glossaire pour les définitions) un environnement sécurisé aux échanges.

Certaines entreprises ou organisations choisissent de se doter de leur propre infrastructure ICP (en anglais PKI [1]) et de l'exploiter en interne. Mais beaucoup préfèrent recourir à des services externes délivrés par des sociétés spécialisées. Ainsi sont apparus des Opérateurs de Services de Confiance qui opèrent une ICP multiclients et peuvent fournir une multitude de services associés : gestion du cycle de vie des certificats, horodatage, coffre-fort électronique, personnalisation de cartes à puces pour porter les certificats. Des offres nationales de qualité existent.

1. Public Key Infrastructure ; on utilise en français la terminologie de IGC pour Infrastructure de Gestion de Clés.

Le développement de ce marché en croissance compte tenu du développement de la dématérialisation des échanges est cependant contraint par le coût et les processus à mettre en place.

Les conséquences des évolutions actuelles du marché de la SSI avec l'émergence de l'informatique dite « de confiance » : initiatives TCG et NGCSB

Les objectifs de ces initiatives

L'initiative TCG (*Trusted Computing Group*). a été lancée en 2003 par AMD, Hewlett-Packard, IBM, Intel Corporation et Microsoft. Elle est la suite du projet TCPA (*Trusted Computer Platform Alliance*) lancé en 1999, mais aussi d'autres initiatives qui visaient généralement à contrôler l'utilisation des œuvres ou des logiciels et à limiter les copies illicites.

Elle a pour objectif d'améliorer la sécurité des ordinateurs via l'insertion dans chaque outil informatique d'un composant permettant d'offrir des services de cryptologie et d'avoir une assurance sur l'état logique de l'ordinateur, afin de pouvoir détecter tout changement de configuration ayant un impact potentiel sur la sécurité.

L'initiative Palladium, complémentaire de TCG, lancée par Microsoft en juillet 2002, est devenue *Next Generation Secure Computing Base* (NGSCB) en janvier 2003. Elle repose sur l'utilisation d'un composant sécurisé et a pour objectif de contrôler que les ordinateurs utilisent bien des « ressources de confiance » (trusted) : codes, périphériques disques durs... Ce composant vérifiera ainsi l'intégrité du logiciel de l'ordinateur, les autorisations de fonctionnement de périphériques ainsi que la légalité des opérations que réalisent ces ressources. En pratique, elles devront obtenir un certificat numérique délivré par Microsoft.

L'environnement de confiance crée par NGSCB vise à protéger Microsoft contre le piratage mais également à améliorer la sécurité des ordinateurs en particulier en offrant une meilleure résistance aux attaques de virus et de chevaux de Troie.

Enfin, en mai 2005, l'initiative TCG a été complétée par Trusted Network Connect (TNC). Cette dernière initiative a pour objet d'étendre la confiance que peut apporter TCG sur un poste à un **réseau.** Pour ce faire, la plupart des protocoles de sécurité classiques – SSL, TLS, SSH... – ont été complétés par une phase préliminaire destinée à établir une preuve réciproque d'intégrité et d'authenticité pour des ordinateurs entrant en communication.

Les menaces possibles

Pour certains, ces limitations d'usage sont justifiées par le développement du commerce électronique et la gestion sûre des droits de propriété intellectuelle des œuvres numériques. L'industrie des médias et des services la réclame. Mais en restreignant les droits de l'utilisateur,

NGSCB donne un droit de regard aux constructeurs de matériels et de logiciels, de l'usage fait des ordinateurs personnels. Il permet de contrôler l'accès des logiciels aux ressources matérielles.

Cette émergence d'une informatique de confiance conduirait un nombre très limité de sociétés à imposer leur modèle de sécurité à la planète, en autorisant ou non, par la délivrance de certificats numériques, des applications à s'exécuter sur des PC donnés. Il en résulterait une mise en cause de l'autonomie des individus et des organisations (restriction des droits d'un utilisateur sur sa propre machine).

Cela constitue une menace évidente à la souveraineté des États. Il est à noter que le BSI allemand dispose d'une équipe travaillant sur le sujet.

Synthèse sur l'offre et le marché de la SSI

L'analyse du marché SSI permet de dégager la synthèse suivante :

• Compte tenu du lien fort entre architecture de système et sécurité, tout segment du marché de la sécurité, dès qu'il est mature, a vocation à être intégré dans le marché des technologies de l'information. Les fonctions de sécurité qui ont du succès finissent par être offertes en standard dans les systèmes d'exploitation, surtout propriétaires. Rares sont les fonctions de sécurité qui connaissent pendant plusieurs années une persistance de leur demande. Cet état de fait contraint les pionniers du segment, souvent des PME, à une mobilité stratégique permanente pour ne pas disparaître. Elles doivent innover, développer des services autour des produits, ou accepter d'être absorbées par des éditeurs de logiciels ou des industriels.

• Le marché réagit en fonction de la menace dont les symptômes sont clairement apparents. La réalité des dégâts des virus explique le succès des logiciels antivirus. De même des actes de piraterie sur les systèmes d'information expliquent le succès des coupe-feux. À l'inverse, les menaces « sans douleur apparente » sont rarement prises en compte. la menace d'interception passive de communication, bien que réelle, est très rarement prise en compte. Tous les produits de chiffrement, logiciels ou matériels, dès lors qu'ils ne sont pas « offerts » avec un système d'exploitation, un équipement de télécommunications ou une autre fonction de sécurité ne constituent pas à ce jour un marché viable en dehors du secteur public et du secteur bancaire.

• Les tentatives de différencier les produits de meilleure sécurité, par l'évaluation, la certification ou la qualification, n'ont pas encore eu l'effet d'entraînement que l'on en attendait. L'évaluation ne constitue pas aujourd'hui un élément de choix primordial pour les acquéreurs de solutions de sécurité.

• Sans une intervention volontaire de l'État, par le biais principal de la commande publique, une offre strictement nationale ne pourra se développer en attendant que les segments du marché deviennent suffisamment importants.

Les principaux moteurs de cette transformation seront :
– la meilleure définition des objectifs et des politiques de sécurité ;
– la volonté de recourir à des produits de confiance ;
– l'acceptation de standards et normes de protection ;
– le recours aux services, type infogérance, pour confier la sécurité à des spécialistes habilités et compétents dans le cadre d'un marché réglementé.

La base industrielle et technologique nationale de SSI, notamment les PME-PMI : un effritement en cours qui risque d'être irréversible sans politique volontariste

Les grandes entreprises fournisseurs de produits et services de SSI sont dans un contexte peu favorable et n'ont pas la taille critique

En France, les grandes entreprises évoluent dans un marché de la sécurité des systèmes d'information dispersé, faible en volume et peu mature.

De plus, un niveau de sensibilisation inférieur devant nos partenaires européens et une certaine résignation face aux Américains, voire aux Asiatiques, suite à notre incapacité à fédérer une industrie informatique européenne font que les grands acteurs sont peu nombreux.

En fait, deux marchés – le monde de la finance, et plus spécifiquement les moyens de paiement et les réseaux interbancaires, et la défense nationale et la sécurité intérieure – ont favorisé l'éclosion de pôles industriels différents, les uns tournés vers le marché concurrentiel, les autres ancrés dans l'industrie de défense. Ce n'est que très récemment, avec la réduction de la croissance de ces marchés, que les industriels ont cherché à se diversifier.

Nos grandes entreprises doivent affronter la concurrence des entreprises anglo-saxonnes, mais le marché qui leur est accessible est réduit.

Le marché américain de la sécurité est marqué par une politique protectionniste forte sur le marché intérieur et un contrôle strict à l'exportation. Cette stratégie de domination technologique présente le double avantage de servir à la fois les intérêts des industriels et ceux de l'administration. Comment éviter en France que, sous couvert d'un appel à la concurrence imposé par le code des Marchés Publics, les équipes techniques de certaines administrations marquent leur indépendance en choisissant un produit de PKI ou une carte cryptographique américains quand des produits français équivalents existent ?

Une véritable politique d'achat des administrations pour consolider une industrie nationale serait nécessaire.

En outre, il n'existe pas actuellement assez d'incitation pour constituer une offre de confiance pilotée par de grandes entreprises ayant une capacité d'intégration de systèmes, et valorisant les produits innovants des PME. Le Pacte PME pourrait favoriser cette approche, sous réserve d'être accompagné par une politique d'achat des administrations, voire des grandes entreprises.

La France possède de grandes entreprises de services informatiques capables d'intervenir sur le domaine de la SSI. Pour des raisons évidentes attenantes à la préservation de leur « intégrité », il conviendrait d'attribuer un label de confiance sous certains critères.

• L'offre nationale et européenne éclatée : de nécessaires rapprochements

La dispersion des forces est patente aussi bien en France qu'au niveau européen. On retrouve ainsi des activités SSI dispersées dans plusieurs groupes qui n'ont pas individuellement la taille critique pour être réellement performantes au niveau mondial et qui sont isolées au sein de ces groupes. En outre, les grands industriels leaders privilégient désormais de plus en plus le métier d'intégrateur.

Si cette situation se poursuit, les risques d'effritement de la qualité et de la compétitivité de l'offre de ces groupes deviendront de plus en plus délicats à gérer pour l'État.

C'est pourquoi, des actions visant au rapprochement de ces activités, en s'inspirant de ce qui a été fait dans la Défense et l'Aéronautique, apparaissent nécessaires.

• Un financement public de la R&D dispersé et insuffisant devant les enjeux de la SSI

Différentes sources de financement existent, plus ou mois accessibles aux PME également : l'ANR (Agence nationale de la Recherche), l'A2I (Agence de l'innovation industrielle), le Minefi et l'Union européenne.

En ce qui concerne l'État :

– **ANR** : la sécurité est un des thèmes des RRIT (Réseaux de recherche et d'innovation en technologie) communs aux ministères de l'Industrie et de la Recherche, notamment ceux sur les télécommunications

(RNRT) et le logiciel (RNTL). Dans les appels à projets 2005 de l'ANR, la sécurité a été traitée dans le RNRT, mais fait également l'objet avec les mémoires de masse, d'une thématique additionnelle dotée de 10M€. Entre 5 et 10 projets devraient être retenus pour un montant de 4 à 8 M€. Entre l'ensemble des dispositifs du ministère de la Recherche, environ 23 M€ entre 2001 et 2004 ont été consacrés au thème SSI [1].

– **A2I** : l'Agence créée le 26 août 2005, est dotée d'un budget de 1 Md€ et contribuera au financement d'une dizaine de projets d'entreprises ou de laboratoires de recherche en technologie d'une durée de cinq à dix ans. Parmi ceux-ci il est souhaitable qu'un ou des projets soient orientés SSI.

• **MINEFI**

– **Oppidum** : le ministère de l'Industrie a mis en place en 1998 le programme Oppidum dédié à la sécurité. Les deux premiers appels à projets en 1998 et 2001, chacun doté d'un budget de 6 M€, ont permis le développement de solutions commerciales accompagnant la libéralisation de la cryptologie et la mise en place de la signature électronique. Même si la crise des technologies de l'information a ralenti la valorisation commerciale de certains projets, des avancées importantes ont été obtenues : en signature électronique, en protection des réseaux d'entreprise et en sécurité des cartes à puce. Le troisième appel à projets lancé en 2004, doté d'un budget de 4 millions d'euros, a rencontré un vif succès puisque 45 dossiers ont été déposés pour un total de 22 millions d'euros environ. 18 projets portant sur les cartes à puce, notamment sans contact, les outils biométriques, les produits de signature numérique, de sécurisation des PC et des produits de surveillance des réseaux, ont été labellisés.

– Des programmes de R&D dans le domaine des télécommunications (CELTIC), du logiciel (ITEA) ou des composants (MEDEA) peuvent aussi contenir des projets concernant plus ou moins la sécurité.

À titre indicatif, le montant des crédits alloués par le ministère de l'Industrie aux projets sur la sécurité dans la période 2001-2003 a été :

Programme en M€	2001	2002	2003	Total
Medea (composants)	2,7	3,7	4,2	10,7
Itea (logiciel)	4,9		2,9	7,8
RNRT (télécoms)	2,1	1,6	2,3	6
Oppidum (applications)	1,4	4,7	3,4	9,5
Total	**11,2**	**10**	**12,7**	**34**

De plus, il est à signaler qu'environ 20 thèses consacrées à la SSI sont soutenues chaque année.

Enfin, on peut noter la montée en puissance des pôles de compétitivité dont certains intègrent les questions de SSI notamment en Île-de-France (System@tic), en PACA (solutions de communications sécu-

1. Source : ministère de la Recherche.

risées) et Rhône-Alpes (Minatec) ou de transactions électroniques sécurisées en Basse-Normandie.

En ce qui concerne la Commission européenne :

Le 6e PCRD comporte des programmes dans le thème « technologies de la société de l'information » qui est doté d'un budget de 4 milliards d'euros environ [1]. De plus la Commission a lancé une action préparatoire, en vue du 7e PCRD, dotée d'un budget prévisionnel de 65 millions d'euros pour la période 2004-2006, concernant la recherche de sécurité :

– **6e PCRD** : la SSI est au cœur de différentes actions (environnement sécurisé, sûreté des réseaux électroniques pour les transports aériens et automobiles, management des risques...) pour un montant évalué à environ 140 millions d'euros sur la période [2] ;

– **action préparatoire** : couvrant les domaines de la sécurité globale (protection des frontières, bioterrorisme, SSI...), les projets SSI ont concerné par exemple les communications sécurisées ou la protection des infrastructures critiques. Les montants affectés à la SSI n'ont pas été précisés ;

– **7e PCRD** : le thème de la sécurité apparaît comme une priorité de ce plan qui dépendra cependant des résultats de l'action préparatoire sur les actions à lancer. Le budget envisagé est de 1 milliard d'euros.

La multiplicité de ces sources de financements et l'absence de coordination ne favorisent pas des actions concentrées sur les thèmes critiques de souveraineté nationale.

• Il existe des réflexions en cours chez des industriels et organismes de recherche qui méritent une attention de la part des pouvoirs publics

Des industriels et des centres de recherche français [3] ont engagé des réflexions sur la mise au point de produits de confiance, par exemple :

– aujourd'hui, la maîtrise de la partie logicielle des produits ne permet pas de garantir la sécurité si le hardware sur lequel elle s'exécute n'est pas maîtrisé. Il est donc nécessaire de lancer des programmes technologiques pour mettre au point des circuits intégrés sécurisés ;

– le lancement d'un projet **structurant** dans les usages et la gestion sécurisée de l'identité, avec comme enjeu l'intégration du citoyen et la préservation de ses droits (individu numérique).

L'implication de l'État dans de telles actions est nécessaire ; mais la volonté et les financements semblent encore incertains.

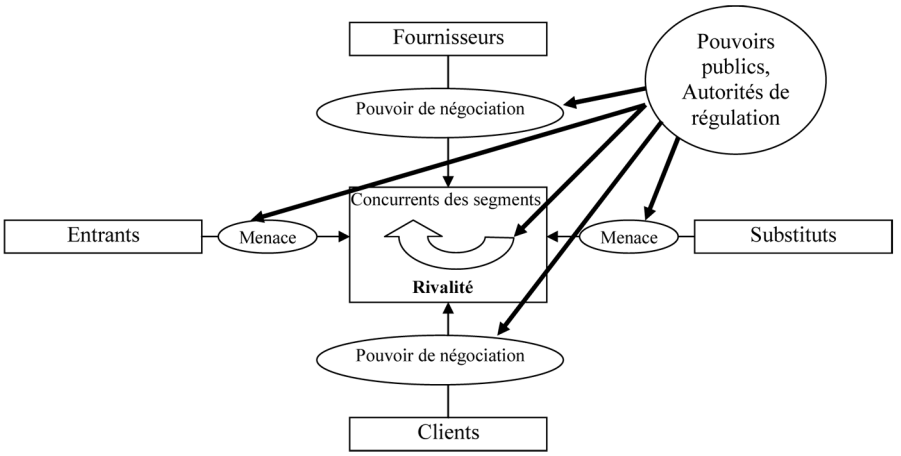
1. Source : Commission européenne.
2. Source : Commission européenne.
3. Source : auditions.

La situation des PME fournisseurs de produits et services SSI est très critique

Le développement des PME françaises et européennes innovantes, parmi lesquelles celles spécialisées dans la SSI, se heurte à de nombreuses difficultés qui ont fait l'objet de multiples rapports ces dernières années. Des propositions, certaines effectivement mises en œuvre par les pouvoirs publics, tendent à améliorer la situation mais demeurent insuffisantes s'agissant du secteur particulier de la SSI.

Un marché de la SSI particulièrement difficile pour les PME françaises

L'analyse des problématiques spécifiques des PME fournisseurs de produits et de services de SSI nécessite au préalable, d'apprécier l'intensité concurrentielle qui prévaut dans le secteur, car elle détermine le niveau de rentabilité moyen des entreprises et donc influence leurs stratégies.



L'État intervient comme client et comme autorité de régulation.

En se plaçant du point de vue de la PME, l'analyse synthétique de l'intensité concurrentielle qui prend en compte six forces donne les caractéristiques suivantes :

- **Pouvoir de négociation des fournisseurs**

Les PME prestataires de services en SSI, sont amenées parfois à intégrer des produits provenant d'acteurs de taille plus importante, en situation de quasi-monopole, ce qui les place en situation de faiblesse à l'achat. Ces entreprises se trouvent de facto fortement dépendantes. Le problème disparaît pour des PME qui développent des produits.
L'État doit favoriser l'existence et le développement d'offres alternatives pour contrebalancer ce déséquilibre en particulier par une politique incitative de financement de développement de produits et de technologies, et une politique d'achat appropriée.

• **Pouvoir de négociation des clients**

Les PME françaises sont en situation de faiblesse face à des clients importants tels que l'État et les grands comptes. Leur marge de négociation est assez limitée alors qu'il existe une concurrence internationale importante et que le critère « fournisseur de confiance » ne semble pas exister dans les politiques d'achat de ces clients.

Sans une prise de conscience des pouvoirs publics, mais également des grands donneurs d'ordres, suivie d'actes concrets et pérennes, en particulier une politique d'achat appropriée, l'offre européenne s'effritera progressivement.

• **Rivalité entre les concurrents**

La croissance du marché de 15 % en moyenne par an attise les ambitions de nombreux acteurs en place, attire de nouveaux concurrents et provoque aussi une concentration des différents segments. La petite taille des acteurs européens et européens ne les favorise pas.

Aussi, lorsque les marchés sont peu protégés par la puissance publique, il est difficile pour une PME de trouver la voie de la survie et du développement dans cet environnement très mondialisé, face à des leaders puissants.

Près de 900 [1] entreprises technologiques dans le monde interviennent dans la SSI, dont 70 % sont d'origine américaine. Leur chiffre d'affaires ne dépasse pas en général 30 M$. Le marché est donc surtout composé de nombreuses petites sociétés et de quelques grandes entreprises.

Dès lors, la concentration du secteur apparaît inéluctable et l'objectif des PME françaises, si elles veulent éviter la marginalisation ou le rachat, est d'accroître fortement leur chiffre d'affaires à hauteur de 30-50 M€, par exemple en se regroupant. À ce niveau d'activité, elles devraient pouvoir générer suffisamment de *cash flow* pour continuer à innover et financer leur R&D.

L'État peut jouer un rôle dans le regroupement européen, à l'image de ce qui est en cours dans l'industrie de défense.

• **Difficultés pour les nouveaux entrants**

Les barrières à l'entrée pour les PME **sont fortes** sur ce secteur en raison :

– de l'expérience forte des teneurs du marché ;

– des besoins importants en capitaux pour un secteur où les stratégies sont mondiales ;

– de l'accès compliqué aux circuits de distribution pour les PME ;

– des avantages spécifiques (brevets...) détenus par les leaders présents ;

– de l'insuffisance de l'appui par les pouvoirs publics de l'offre européenne**.**

Les pouvoirs publics, sans s'opposer naturellement aux nouveaux entrants, se doivent de contribuer activement au développement des acteurs existants. Ainsi, avoir une politique en matière de capital-risque, notamment d'amorçage, est sans doute essentiel, mais disposer sur le territoire de financement plus substantiel en capital développement l'est sans doute davantage et doit être encouragé et accompagné.

1. Source : auditions.

• **La menace des produits substituables**

Elle est soutenue sur ces secteurs compte tenu d'une évolution permanente des technologies consécutives à l'évolution des besoins. Par exemple, l'avancée de l'Ipv6 et de la post 3G aura des conséquences fortes sur le tissu national spécialisé dans les TIC et donc sur celui spécialisé en SSI.
Pour y répondre, un effort intense et continu de R&D est nécessaire, en particulier au sein des PME innovantes. Un effet de levier important par le financement public national et européen est naturellement indispensable et doit être accentué. Mais sans un accroissement significatif des financements privés, notamment des grands donneurs d'ordres, les montants consacrés seront insuffisants pour rester au meilleur niveau.

• **Le rôle des pouvoirs publics et des autorités de régulation**

Les pouvoirs publics et les autorités de régulation influent directement sur le marché. Ainsi, peuvent-ils faire jouer leur influence sur les pouvoirs de négociation des fournisseurs et des clients (réglementations en matière de délai de paiements, ou de sous-traitance obligatoire à des PME dans le cadre de contrats publics...), sur les menaces des nouveaux entrants (autorisations d'exercer notamment dans la SSI, existence de normes spécifiques...). L'Union européenne peut également intervenir, en particulier dans le financement de la R&D et en matière réglementaire (textes pro-PME, normalisation favorable à l'offre issue de l'Union européenne...) pour favoriser l'environnement de ces PME SSI.
L'État doit prendre conscience de son rôle moteur indispensable dans ce domaine particulier qu'est la SSI. Son rôle ne doit pas se limiter à une politique de financement et d'incitations fiscales.

Contraintes complémentaires issues de l'environnement

En complément des analyses précédentes, trois autres facteurs permettent de mieux comprendre la situation actuelle de faiblesse de l'offre nationale et européenne de SSI :

• **Marché européen fragmenté et souverainetés nationales**

Contrairement aux États-Unis qui dispose d'un marché de la SSI unique et important en volume, celui de l'Europe est fragmenté. Chaque pays, pour des questions de souveraineté, privilégie des solutions nationales, quand elles existent.
On observe que le marché accessible à une PME étant restreint, son potentiel de développement limité, ce qui la rend peu attractive pour des investisseurs.
Favoriser une offre européenne apte à vendre aux États et aux grands donneurs d'ordres européens sans barrières spécifiques doit être un objectif de l'État français en coopération avec ses partenaires européens les plus proches sur les questions de SSI.

• **Faiblesse des grandes entreprises européennes de SSI**

L'absence de leaders mondiaux sur le territoire national et européen entraîne un manque de stimulation pour toute la chaîne de fournisseurs et pour l'environnement de recherche. Ainsi, nos entreprises et nos laboratoires se trouvent-ils éloignés de ceux qui ont une vision claire de leurs marchés et

de ses évolutions à venir. Ils auront de ce fait un temps de retard par rapport à des PME et laboratoires installés à proximité des grands donneurs d'ordres américains.

• **Montée en puissance de l'Asie**

La croissance de l'Asie sur ces différents segments de marché est forte et s'appuie désormais sur sa propre expertise technique. La volonté de la Chine de verrouiller ses systèmes d'information privés et publics et de contrôler l'ensemble de la chaîne laisse augurer dans le futur la montée en puissance d'une offre indépendante asiatique qui cherchera à s'implanter en Europe, comme c'est le cas pour l'automobile.

Prises en tenaille entre les États-Unis et l'Asie, les PME européennes devront faire preuve d'une grande agilité et d'un appui sans failles de la puissance publique et de quelques donneurs d'ordres privés pour exister et se développer.

Les politiques d'achat de l'État et des grands donneurs d'ordres sont peu orientées sur les PME SSI et les fragilisent

• **Une politique d'achat public marquée par la complexité du processus et la culture des acheteurs**

Les pouvoirs publics interviennent sur ce marché en tant qu'acheteur important.

Or, à ce jour, la centralisation et la rationalisation des achats, un code des marchés publics plus adapté aux grandes entreprises qu'aux PME innovantes, la culture des acheteurs qui privilégient, pour des raisons de prudence et de prix immédiat les grandes entreprises installées dont la pérennité semble mieux assurée, a pour conséquence une politique d'achat de l'État, qui ne favorise pas le chiffre d'affaires des PME innovantes sur ce secteur, ce qui n'est pas le cas d'autres pays.

Le gouvernement a certes pris quelques mesures :

– action auprès des partenaires européens pour une renégociation du traité OMC et de la législation européenne ;

– installation d'un observatoire de la commande publique le 15 novembre 2005 ;

– lancement d'une concertation pour optimiser la passation des appels d'offres à des PME ;

– pacte PME proposé par le Comité Richelieu en association avec OSEO-Anvar, dont l'objectif est de faciliter les relations entre les grands comptes et les PME innovantes.

Ces mesures ont naturellement le mérite d'exister et contribueront, peut-être, à une évolution culturelle indispensable chez les acheteurs et donc de la mise en place d'une politique d'achat plus adaptée aux PME innovantes, mais elles mettront du temps à produire leurs effets.

Les ministères devraient mener une politique d'achat en cohérence avec leurs axes stratégiques, notamment en matière de sécurité nationale. Il est intéressant de citer la politique d'acquisition du ministère de la

Défense, fondée sur un principe d'autonomie compétitive qui s'articule autour de deux objectifs complémentaires :
– garantir la meilleure efficacité économique des investissements réalisés pour satisfaire les besoins des forces armées ;
– assurer un accès aux capacités industrielles et technologiques qui conditionnent la satisfaction à long terme des besoins des forces armées.

En outre, du fait de la complexité croissante des produits informatiques et des services associés, leur conception et leur réalisation impliquent de multiples acteurs avec une part croissante de sous-traitance et d'externalisation. Pour l'acheteur public final, la sécurité du système installé s'avère de plus en plus complexe en l'absence d'une volonté forte de contrôler l'ensemble de la chaîne de fournisseurs de SSI de confiance.

Il est à noter à cet effet que le PRSSI [1] recommandait dans sa mesure I1 : « de garantir une diversité d'approvisionnement en produits de sécurité en stimulant le développement de produits industriels innovants et répondant à des besoins identifiés, en s'adressant à un tissu d'industriels de confiance notamment de PME. »

Ainsi, le ministère de la Défense a pris l'initiative de lancer en 2004 le développement d'un système d'exploitation durci et fiable. Ce projet, **Sinapse**, s'appuie sur des PME françaises du secteur de la SSI. Cette démarche pourrait inspirer d'autres développements.

Dès lors, une définition interministérielle de principes communs en matière d'acquisition de produits et services de SSI, sans remettre en cause l'autonomie décisionnelle de chaque ministère permettrait d'assurer à l'État une meilleure cohérence et une meilleure maîtrise de l'intégration de produits et services de SSI dans ses différents systèmes d'information, en phase avec ses objectifs régaliens.

À ce jour, la politique d'achat des ministères ne semble pas prendre suffisamment en considération les enjeux de l'existence d'une offre de confiance au niveau national et européen.

• Une politique d'achat des grandes entreprises qui manque de souplesse et ne favorise pas l'innovation

Les critères de sélection des grandes entreprises n'intègrent pas suffisamment le caractère innovant des PME, facteur d'innovation pour leurs propres produits, et les enjeux de sécurité que représente une offre européenne viable sur le long terme. La résistance des acheteurs à l'innovation semble réelle et presque de nature culturelle. À cela s'ajoutent les grandes entreprises qui cherchent à diminuer fortement le nombre de leurs interlocuteurs et à faire partager les risques de développement à leurs sous-traitants. Ces objectifs sont des freins de plus en plus importantes pour les PME.
À l'exception du **Pacte PME**, il n'y a pas de réelles dynamiques de la part des grands donneurs d'ordres. Une politique d'achat à des entreprises françaises ou européennes de confiance peut être effective sans nécessairement

1. Plan de Renforcement de la Sécurité des Systèmes d'Information de l'État (2004-2007) du 10 mars 2004.

entraîner un surcoût mais sous réserve d'une **volonté forte de changement** des grands donneurs d'ordres.

Les PME SSI françaises ne disposent pas des ressources suffisantes pour se développer

• **Le financement**

L'accès aux ressources financières est naturellement un point essentiel et recouvre : les fonds propres, les crédits bancaires, le financement de projet ou à l'exportation [1] et la transmission/cession [2].

Certes, les mesures gouvernementales ont été nombreuses ces dernières années :
– développement des FCPI [3] et d'Alternext ;
– incitation auprès des assureurs français à investir 6 G€ dans les PME ;
– politique en matière d'amorçage et d'incubation qui a le mérite d'exister même si, pour l'instant, les résultats ne sont pas toujours très positifs ;
– concours création d'entreprises du ministère de la Recherche, renforcement d'Oséo.

Mais des améliorations sont souhaitables, en particulier en matière de conditions de sortie vers les marchés cotés et de garanties par Oséo Sofaris qui restent insuffisantes. Cependant, un point plus critique est l'affectation effective de ces ressources aux PME innovantes notamment SSI.

En effet, la tendance du marché du capital d'investissement se caractérise par :
– une prédominance des opérations de LBO [4] ;
– une faiblesse structurelle des fonds de capital-risque à lever des fonds ;
– une orientation croissante des FCPI vers le marché coté.

En outre, pour les fonds d'amorçage, les difficultés de sortie sont croissantes en l'absence de fonds de capital développement prêts à prendre le relais et à payer le prix. Pour les participations à fort potentiel de développement, seuls les Anglo-Saxons sont en mesure de le faire.

De plus, le temps de maturation des technologies est souvent plus long que sur les autres secteurs des TIC, compte tenu d'un environnement normatif et réglementaire contraignant affectant la durée d'investissement qui peut être plus longue que la norme du marché.

1. Financement projet : difficile compte tenu de la pression des donneurs d'ordres pour partager le risque avec les sous-traitants. Un effet de levier serait nécessaire. Le financement de l'exportation : il n'existe pas à ce jour de réponse efficace en termes de cautions bancaires.
2. Nécessite une attention particulière afin de favoriser des solutions européennes permettant progressivement l'émergence de PME de plus grande taille, aptes à intervenir au niveau mondial.
3. Fonds Communs de Placement dans l'Innovation.
4. Leveraged By Out : opération d'acquisition d'une entreprises financée par un fort recours à l'endettement.

Enfin, les décrets récents relatifs au contrôle des investissements étrangers sur des secteurs sensibles, risquent de gêner les volontés de certains fonds qui peuvent voir dans cette réglementation une nouvelle contrainte forte à la sortie et ce, dans un contexte difficile. La situation aux États-Unis est différente : la taille du marché intérieur et les sources de financement disponibles leur permettent de se dispenser de financements étrangers.

Un marché restreint et plus contraignant en durée, une commande publique et privée insuffisamment orientée, une réglementation qui contrôle les investissements étrangers, un manque en capital développement et la difficulté d'aller en bourse en Europe continentale, rendent ce marché de la SSI peu attractif pour des investisseurs européens.

Des fonds d'investissement spécifiques adaptés aux profils de ces entreprises spécifiques, d'une durée de vie de 12 à 15 ans, seraient un complément nécessaire aux fonds de capital investissement actuels.

On peut noter l'existence en 2005 d'un dispositif de fonds d'investissement stratégiques sur l'initiative du Haut Responsable à l'Intelligence Économique orienté vers les PME sensibles françaises qui traduit la mise en place d'un système de suivi interministériel des secteurs stratégiques, par la mise en place de fonds dédiés aux entreprises relevant de ces secteurs, désormais opérationnel.

• **Un financement public et privé de la R&D insuffisant**

Les PME des secteurs technologiques et notamment des TIC, sont confrontées à une **évolution en ciseau** avec, d'une part, une très forte croissance des besoins de financement de la R&D et, d'autre part, un plafonnement des ressources traditionnelles que sont les financements gouvernementaux et des grandes entreprises européennes continentales.

En effet, pour être en mesure de suivre l'évolution technologique permanente de ces marchés, les entreprises doivent consacrer en moyenne jusqu'à 15 % de leur CA en R&D. Or, la **France et ses entreprises ne sont pas suffisamment actives dans le domaine des TIC** [1] :
– en 2003, le financement de la R&D en TIC était de 90 $ par habitant en France, contre 220-240 $ aux États-Unis ou au Japon ;
– la même année, l'effort de R&D global en TIC ramené au PIB était de 0,31 % en France, contre 0,65 % aux États-Unis et 0,76 % au Japon. Pour l'effort de R&D des entreprises, les ratios sont similaires ;
– l'effet de levier de la dépense publique en TIC sur les entreprises, c'est-à-dire le ratio entre la R&D exécutée par les entreprises et les fonds publics qui y sont consacrés, est très nettement inférieur en Europe (5,2) qu'aux États-Unis (7,1), la **France étant encore en retrait avec 4,3**, loin derrière des pays où le ratio se situe entre 10 et 12 (Canada, Corée, Finlande et Suède notamment).

1. Source : Futuris et Conseil Stratégique des Technologies de l'Information – Groupement Français de l'Industrie de l'Information octobre 2003.

Ainsi, le financement de la R&D par les grandes entreprises françaises et européennes étant proportionnellement plus faible que celui des entreprises concurrentes aux États-Unis ou en Asie, **la part sous-traitée à des PME notamment SSI n'en sera que plus limitée**.

Des mesures gouvernementales de nature générale ou sectorielle ont ainsi été prises :
– renforcement du crédit impôt recherche [1] ;
– augmentation des moyens financiers d'Oséo annoncée en juillet 2005 ;
– accès des PME aux projets financés par l'Agence de l'Innovation Industrielle (mais il n'y a pas de part réservée aux PME), ainsi qu'à ceux de la Commission (les PME n'ont pas toujours les moyens et le temps à consacrer aux réponses aux appels à projets) ;
– accès aux programmes de développement de la DGA (PEA [2]...) ;
– programmes sectoriels avec :
· oppidum (Minefi) ;
· abondement par la DCSSI ou la DGA d'avances remboursables accordées par Oséo Anvar à des projets les intéressant (SSI, technologies duales...) pour des montants trop faibles.

Cependant, l'ensemble n'est pas pour l'instant à la hauteur des moyens consacrés par les pays concurrents notamment aux États-Unis, en Allemagne et en Asie.

• **Des ressources humaines qualifiées insuffisantes**

Les PME françaises ne disposent pas toujours des compétences nécessaires pour attirer des investisseurs et rassurer les clients, alors qu'il s'agit d'un critère essentiel**. Aujourd'hui la question n'est pas tant de savoir si de bons projets sont développés ou non, en France, mais plutôt, si de bonnes équipes existent** pour les exécuter.
À l'exception d'Oseo Anvar qui propose un dispositif spécifique de prise en charge d'une partie des charges liées à l'emploi de chercheurs, il n'y a pas à ce jour de mesures particulières pour favoriser le recrutement de compétences par des PME, notamment en marketing des technologies [3], alors que les freins au recrutement sont déjà forts.
En outre, **le vieillissement général** des dirigeants en France entraînera des conséquences qui ne peuvent être ignorées. En l'absence de solutions facilitant les transmissions, les solutions de reprise par des fonds d'investissement s'imposeront. Aussi, progressivement, le capital des PME françaises sera-t-il de plus en plus maîtrisé par des fonds disposant des capitaux nécessaires, aujourd'hui principalement anglo-saxons.

• **Un environnement juridique et fiscal perfectible**

L'environnement français est peu attractif. Certaines mesures fiscales récentes vont toutefois dans le bon sens :
– évolutions favorables en matière d'ISF ;

1. Doublement de 5 à 10 % de la part en volume des dépenses de recherche prises en compte.
2. Programme d'Etudes Amont.
3. Source : auditions.

– création du statut de JEI (Jeune Entreprise Innovante) intégrant des exonérations de charges sociales et d'impôts (même si le rachat d'une JEI par une JEI a pu aboutir à des redressements fiscaux) [1] ;
– création du statut de SUIR (Société Unipersonnelle d'Investissement à Risque).

Quant à la simplification des processus administratifs pour faciliter l'accès des marchés publics aux PME, elle relève pour l'instant encore des intentions...

Les centres de recherche orientés sur la SSI insuffisamment présents

Quelques centres et instituts en France ont des activités orientées sur la SSI, en logiciels ou matériels, pour certains de grande réputation. Ils travaillent en collaboration principalement avec les grands industriels qui interviennent dans le domaine.

L'absence de grands leaders industriels en France, une insuffisance de fonds publics sur ce thème et des contraintes à publier ne favorise pas pour l'instant une action suffisamment forte pour être au niveau des meilleurs mondiaux.

Une coopération accrue avec des leaders de la SSI, notamment américains, serait souhaitable mais nécessiterait un examen sans doute approfondi, car, même si elle présente des facteurs de risque significatifs, elle permettrait dans le cadre de **partenariats équilibrés** de mettre les chercheurs français au contact des leaders de ces marchés.

La certification de produits et les normes de sécurité sont insuffisamment prises en compte en France : un frein au développement de l'offre nationale de SSI

Le développement de l'offre nationale fournisseur de produits de SSI se réalisera de manière plus efficace si, en parallèle d'une politique d'achat appropriée, les produits pourront être certifiés et qu'ils seront pris en compte en amont dans le cadre des processus qui aboutissent à la mise au point de normes.

1. Source : auditions.

La certification (cf. Annexe XIII)

Selon IDC Sécurité 2005 [1], la certification des technologies de sécurité aux Critères Communs est impérative pour choisir les fournisseurs de solutions de sécurité pour 21 % des sondés et prise en compte par 27 %.

Le processus de certification : des délais à optimiser

• Les motivations des entreprises qui font évaluer et certifier leurs produits

Elles sont au nombre de trois :

– **raisons marketing** : disposer d'un avantage concurrentiel avec le certificat ;

– **raisons sécuritaires** : cette motivation est généralement le fait de certains donneurs d'ordres. Ces derniers imposent l'évaluation et/ou la certification à leurs fournisseurs pour accepter d'acheter leurs produits ;

– **raisons réglementaires** : cette motivation est généralement le fait des États ou des communautés d'États. Les États-Unis imposent aux administrations l'achat de produits évalués et certifiés [2]. En France et dans les autres pays européens, les dispositifs permettant de réaliser des signatures électroniques sécurisées doivent être évalués et certifiés.

• Des délais d'évaluations jugés trop longs et des exigences parfois excessives

Ce délai va dépendre de plusieurs facteurs : la complexité du produit à évaluer, le niveau de confiance visé... Pour une carte à puce évaluée au niveau EAL4 (cf. annexe XI pour le descriptif des niveaux), une évaluation peut être réalisée en 6 mois. Pour des produits de sécurité informatiques évalués au niveau EAL2, une évaluation peut-être réalisée en 4 mois.

Les utilisateurs de la certification se plaignent souvent des durées trop importantes du processus d'évaluation/certification pouvant dépasser un an. En outre, dans certains cas, la certification intervient alors qu'une version suivante va être commercialisée. Même si dans certains cas, ces délais anormaux sont dus à la mise en évidence de vulnérabilités lors de l'évaluation, les délais actuels apparaissent trop longs pour être en phase avec les évolutions des marchés et une obsolescence plus rapide des produits.

S'agissant des exigences pour l'obtention de la certification, elles doivent être proportionnelles aux risques et ne pas faire l'objet de surenchères préjudiciables aux entreprises.

1. Enquête IDC Sécurité 2005 – marché professionnel -103 entretiens auprès d'un panel de grandes entreprises et administrations en France composées à 45 % de plus de 2000 salariés et 55 % de 1000 à 1999 salariés – novembre 2005.

2. La *National Information Assurance Acquisition Policy* promulguée en janvier 2000, impose qu'à partir du 1er juillet 2002 les agences américains n'achètent que des produits certifiés (critères communs pour le produits et FIPS 140 pour les modules cryptographiques).

• **Le coût des évaluations à la charge des entreprises est important pour les PME**

La certification délivrée par la DCSSI est gratuite. Par contre, l'évaluation réalisée par le centre d'évaluation (CESTI) est payante :

– carte à puce, niveau EAL4 : 120 000 à 150 000 € HT ;

– produit informatique (firewall...), niveau EAL2+ : 50 000 à 60 000 €.

Ces prix peuvent être plus ou moins élevés selon la nature exacte du produit à évaluer et selon le nombre de reprises d'évaluation. Ce coût de la certification d'une version d'un produit, puis des versions successives, est un obstacle pour les PME [1].

La reconnaissance mutuelle des certificats : un risque d'abandon de souveraineté

Un point fondamental pour les développeurs est que les systèmes de certification CC (Critères Communs) et ITSEC (critères européens pour évaluer la sécurité des produits techniques) bénéficient d'accords de reconnaissance mutuelle entre de nombreux États. Ainsi, le constructeur d'un produit peut faire valoir, sur le territoire national, un certificat délivré par l'homologue de la DCSSI à l'issue d'une évaluation de son produit menée à l'étranger, et réciproquement.

Les certificats CC et ITSEC sont reconnus à tous les niveaux en Europe. Les certificats CC sont reconnus jusqu'au niveau EAL4 avec les autres pays signataire de l'accord de reconnaissance mutuelle (CCRA). Une vingtaine de pays avaient signé ces accords en 2004 et de nouveaux pays sont candidats aujourd'hui.

Il existe néanmoins des limitations au déploiement de ces accords de reconnaissance mutuelle. En effet, il faut conserver une capacité régalienne de pouvoir agréer ou non un produit même si celui-ci a été certifié par un pays étranger membre des accords de reconnaissance mutuelle.

Dans le cas contraire, cela revient à accepter de confier à des organismes étrangers, non-contrôlables par des intérêts français, une partie significative de la politique de sécurité de l'État et des entreprises. En effet, même si l'importance de l'architecture sur la sécurité des systèmes d'information ne peut être négligée, la composante produit est incontournable.

C'est d'ailleurs ce qui se fait aux États-Unis : les analyses de vulnérabilités de haut niveau sont faites par un centre étatique (la NSA) et ils ne reconnaissent pas les évaluations au-delà d'un certain niveau de confiance.

1. Source : auditions.

Un positionnement actif de la France vis-à-vis de ses homologues en terme de certificats délivrés mais très orienté sur les cartes à puce

La France fait partie des pays fondateurs des critères et des accords de reconnaissance mutuelle (autres pays : États-Unis, Royaume-Uni, Allemagne, Pays-Bas, Canada).

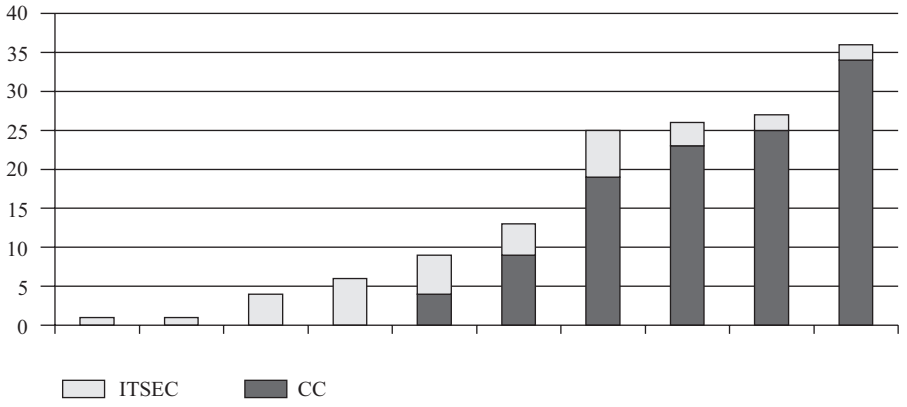
L'activité de certification française, mesurée en nombre de certificats, est assez soutenue comparée à celle d'autres pays mais l'effectif du centre de certification de la DCSSI semble trop limité devant la croissance des certificats délivrés :

Pays	Certificats 2004	Certificats 2005 (prévisionnel)	Nombre de CESTI	Effectif du Centre de Certification
France	36	45	5	6
Allemagne	38	40	13	20
Royaume-Uni	12	8 à fin octobre	5	
États-Unis (1)	27	35 à début octobre, **154 en cours**	10	30 en 2002
Canada	9	9 à début août.	3	4
Corée	20	16 à fin octobre	1	?

(1) Le grand nombre de certifications en cours aux États-Unis s'explique en partie par une politique volontariste du gouvernement fédéral

En 2004, 25 des 36 certificats délivrés concernaient les cartes à puces, 8, les profils de protection, et 3, les logiciels. Il est à signaler néanmoins, qu'il n'y a pas à ce jour de profil de certification concernant la biométrie [1].

Évolution du nombre de certificats en France



Mais une influence faible à l'international, préjudiciable aux intérêts nationaux.

1. Source : auditions.

Il est regrettable de constater qu'à part dans un cercle restreint d'initiés, la compétence et l'expérience particulière de la France (et en particulier de ses centres d'évaluation) sont peu connues et reconnues à l'étranger. La faible participation française [1] aux journées ICCC (*International Common Criteria Conference*) qui ont suivi le CCRA d'octobre 2005 au Japon ne contribue pas à améliorer cet état de fait.

On notera par exemple qu'à travers le BSI, les centres d'évaluation allemands se positionnent pour aider la formation de centres d'évaluation en Corée du Sud, à Singapour ou à Taiwan.

Depuis début 2005, le service de certification français de la DCSSI s'est réinvesti dans certaines instances internationales (Union européenne pour la sécurité des moyens de paiement, groupements professionnels tels que l'ISCI et Eurosmart) pour promouvoir son savoir-faire, ses méthodes et ses compétences. Toutefois, la taille modeste de son effectif empêche la France de prétendre se positionner sur tous les fronts et doit généralement suivre ce qui est préconisé par d'autres.

L'absence de Français au sein des instances en charge de faire évaluer les critères et les interprétations de ces critères est préjudiciable à la préservation de notre savoir-faire et ne nous permet pas d'éviter que des méthodes nous soient imposées par d'autres.

La qualification : une réponse à des besoins spécifiques de sécurité

Les administrations ou les entreprises souhaitent disposer de produits de sécurité dans lesquels elles peuvent avoir confiance et qui répondent à leurs besoins de sécurité. La certification offre un élément de réponse au premier point mais pas au second.

En effet, un produit est évalué selon sa cible de sécurité (sa spécification de besoin de sécurité). Or, cette cible est réalisée sous la responsabilité du développeur qui définit ce qu'il souhaite. Le processus de qualification créé par la DCSSI permet de s'assurer que les cibles de sécurité des produits (en terme notamment de périmètre et de profondeur de l'évaluation) répondent précisément aux besoins des administrations et des entreprises.

Pour l'État, la DCSSI et l'ADAE référencent la qualification dans le référentiel sécurité de l'administration électronique (Politique de référencement intersectorielle de sécurité, PRIS).

L'agrément : une réponse aux besoins spécifiques de l'État

L'agrément de produit est prononcé par la DCSSI lorsque le produit (notamment de chiffrement) est apte à traiter de l'information classifiée de défense.

1. En plus du représentant de la DCSSI, il y avait deux représentants de centres d'évaluation.

Le processus d'agrément est traité par le « bureau réglementation » de la sous-direction régulation de la DCSSI. Les évaluations sont réalisées par le CELAR. Il est de compétence national, et n'est pas soumis aux accords internationaux de reconnaissance mutuelle.

La normalisation

La normalisation : une source d'enjeux pour les standards des marchés

La normalisation est un outil d'ouverture des marchés, d'amélioration de la transparence, ainsi qu'un mode de preuve de conformité au service des économies mondiales. Elle facilite les choix stratégiques de l'entreprise. Elle favorise la protection des consommateurs et l'application de la réglementation.

Le terme de « normalisation » conserve souvent l'image de règles d'organisation imposées par l'extérieur qui brident la capacité d'adaptation des entreprises et leur réactivité à l'évolution de l'environnement. Elles sont donc souvent perçues comme contraignantes. Pourtant, les normes sont reconnues dans le monde des produits industriels où elles gouvernent les échanges entre partenaires, créent la confiance et font vivre les contrats.

La norme propose ainsi les conditions dans lesquelles une opération sera effectuée, un objet exécuté, un produit élaboré ou un service rendu et prend la forme d'un document de référence sur un sujet donné dont il reflète l'état de l'art, de la technique et du savoir-faire.

La reconnaissance des documents et profils de protection DCSSI : une amorce de coopération avec les instances de normalisation à dynamiser

À l'occasion d'un colloque à l'École militaire en 2002, la DCSSI avait acté le principe de donner à certains de ses documents, notamment des profils de protection, le statut de norme française pour une prise en compte systématique dans les appels d'offres publics, et surtout dans le but de les étendre au niveau européen voire international.

Après une première phase de préparation en groupe de travail, une série de documents ont été réalisés mais le projet de convention qui encadre cette action prévue en 2005 est toujours en discussion.

Une nouvelle impulsion à ce stade serait impérative pour donner ses chances à ce projet, et assurer en même temps la continuité du travail de la DCSSI avec AFNOR.

Les dissymétries transatlantiques : sources d'oppositions

La normalisation internationale est marquée par une double dissymétrie dans les relations entre Europe et États-Unis.

La plus évidente est celle qui résulte du système de vote : les pays européens disposent d'une trentaine de voix à l'ISO, contre une pour les États-Unis. Cet avantage ne résisterait pas à une politique systématique de concertation européenne et de vote de bloc. Les pays européens se sont donc abstenus de tout engagement en ce sens. Dans le domaine de la sécurité des systèmes d'information, le poids des pays européens a cependant été crucial dans l'adoption très rapide de normes comme l'ISO 17 799.

La seconde dissymétrie est plus profonde. En effet deux modèles s'affrontent :

– Dans l'approche des États-Unis, les normes sont établies par de multiples organisations aux statuts les plus variés, en concurrence et sans qu'aucune autorité soit missionnée pour apporter de la cohérence. Dans le seul secteur des technologies de l'information, plus de 300 entités américaines se déclarent organismes mondiaux de standardisation. L'organisme national des États-Unis, l'ANSI, a pour unique raison d'être, l'exigence de l'ISO d'avoir un membre unique par pays. Il ne bénéficie pas d'une reconnaissance forte des autorités fédérales ni des grands instituts américains comme l'IEEE [1].

– L'approche de l'Europe repose sur des processus menés par des organisations reconnues formellement par les pouvoirs publics nationaux et européens. L'institut européen de normalisation CEN a autorité pour harmoniser les normes en Europe et faire retirer les normes nationales divergentes. Cette approche vise à bénéficier notamment aux utilisateurs en garantissant la cohérence et l'interopérabilité. Cette organisation a été critiquée pour sa difficulté à répondre en temps réel aux besoins du marché et à l'évolution des technologies.

Le défi posé au modèle européen consiste à prouver qu'on peut combiner le bénéfice de la standardisation informelle, c'est-à-dire la rapidité dans la réponse au marché et aux technologies, avec les bénéfices de la co-régulation que sont l'interopérabilité et la coordination entre les exigences économiques et celles de la société.

L'influence de la France est insuffisante dans le processus d'adoption des normes de sécurité

• Le processus préalable à l'adoption des normes : des enjeux de pouvoir mais une présence insuffisante de représentants français

Le processus d'adoption des normes est très formel et la base des décisions est la recherche du consensus. Cependant, avant d'adopter des normes, un processus technique souvent informel se déroule dans des groupes de travail d'industriels et d'experts ou d'associations des secteurs considérés

1. Institut of Electrical and Electronics Engineers (USA).

dans lesquels la logique de lobby est très forte et où chacun défend ses intérêts pouvant aller jusqu'à s'opposer au processus de normalisation. Être absent de cette phase amont revient à ne pas pouvoir réellement peser sur les orientations prises par les futures normes.
Standarmedia [1] – un outil de veille collaborative, créé par l'AFNOR avec le soutien du ministère chargé de l'Industrie et avec des partenaires industriels – a identifié 63 instances actives en matière de sécurité, dont 38 complètement dédiées à la sécurité, l'authentification, la biométrie et les cartes à puce. 17 sont des groupes de travail consacrés à la sécurité au sein d'organisations généralistes comme OASIS [2] ou IETF [3] qui regroupent des industriels.
Les questions de sécurité se retrouvent également dans des thèmes voisins comme la traçabilité, notamment sous l'angle des étiquettes à radiofréquence (RFID).

• La montée en puissance de la Chine ou la force du marché : le cas de la sécurité des réseaux sans fil Wifi

Les systèmes de réseaux de données sans fil illustrent les difficultés rencontrées avec la Chine. Sa tentation de créer des standards divergents est imputée aux brevets occidentaux, jugés exorbitants, qui portent sur des technologies essentielles pour la mise en œuvre.
Les États-Unis ont établi une série de spécifications à travers l'organisme IEEE qui couvre les aspects de sécurité qui ont été proposés à l'ISO. Dans le même temps, la Chine a créé un autre standard – WAPI – pour la sécurité des réseaux Wifi, et le propose également à l'ISO qui doit donc prendre une décision sur le standard qui aura valeur de référence mondiale.
Cela apparaîtrait comme un mauvais signe pour le marché si deux standards étaient développés en parallèle, comme ce fut le cas sur la téléphonie mobile de seconde génération avec le CDMA et le GSM.
Cependant le marché intérieur chinois représentant à lui seul un potentiel énorme, l'ISO ne peut prendre une position excluant *a priori* l'un des deux standards. En cas de coupure en deux du marché, ce qui semble assez vraisemblable vu la situation à l'ISO [4] aujourd'hui, les perdants seraient probablement les Européens du fait d'un marché intérieur assez étroit qui les obligeraient à choisir l'une ou l'autre technologie, sans doute le Wifi IEEE.

• Le management de la sécurité des systèmes d'information, ISO 17 799 : la réussite d'une référence britannique

La première partie de la norme britannique BS7799 constituée de **recommandations** est devenue norme internationale sous le numéro ISO17799. La seconde, fixant des exigences, est restée quelques années dans les limbes, sous l'influence de grandes compagnies internationales opposées à la certification en général. La seule certification qui existe aujourd'hui est l'attestation de conformité à la norme britannique BS7799-2 qui n'a donc pas le caractère d'une norme internationale.

1. www.standarmedia.com
2. OASIS : Organisation for the Advancement of Structural Information Standards – localisation USA – différents thèmes traités dont PKI, biométrie et signature électronique.
3. IETF : Internet Engineering Task Force – localisation USA – groupe spécialisé dans l'architecture et le fonctionnement de l'Internet.
4. Source : auditions.

Selon cette source, plus de 1 700 certificats auraient été attribués dont plus de 1 000 à des entreprises japonaises, 200 au Royaume-Uni et, semble-t-il **un seul en France**.

Normes nationales et internationales de sécurité des systèmes d'information	**Exigences** **Peut faire l'objet d'une certification**	**Recommandations** **Non-certifiable – Peut faire l'objet d'une évaluation**
Situation jusqu'en 2005	BS 7799-2	BS 7799-1 ISO 17 799
Situation à partir de 2006	ISO 27 001	ISO 27 002

Recommandations

L'information constitue un **patrimoine essentiel** qu'il convient de protéger.

La protection de cette information est une condition essentielle à la préservation de nos entreprises et donc de l'emploi.

L'État, au moment où se généralise la dématérialisation des procédures, se doit également d'être exemplaire sur ce sujet. Il en va de la confiance des citoyens.

La logique qui soutient le projet de réorganisation du dispositif SSI de l'État s'inscrit dans la réflexion sur l'État stratège. « L'État stratège est un architecte de la compétitivité nationale et des nouveaux consensus sociaux induits par la mondialisation. Compte tenu de cette posture, il pilote des stratégies basées sur une meilleure cohérence des institutions publiques et destinées à produire leurs effets sur le système d'innovation et l'assimilation des mutations permanentes caractéristiques du monde contemporain. »

Les recommandations proposées correspondent à une double ambition :
– renforcer la posture stratégique de l'État en matière de TIC et de SSI ;
– assurer la mise en œuvre opérationnelle des politiques et des décisions de l'État en matière de SSI.

Pour répondre à ces deux enjeux : Six recommandations

La sécurité des systèmes d'information, sans laquelle la souveraineté nationale s'effrite, doit être considérée comme une **priorité nationale** par les plus hautes autorités de l'État.

Pour traduire cette priorité, le présent rapport préconise 6 axes stratégiques à mettre en œuvre et une proposition d'organisation.

Axe 1 : Sensibiliser et former à la sécurité des systèmes d'information

Des acteurs non-sensibilisés aux risques liés à l'usage des technologies de l'information et de la communication et non-formés aux bonnes pratiques représentent une source majeure de vulnérabilité des systèmes d'information. Quatre actions prioritaires sont à mettre en œuvre :

– **Sensibiliser** : organiser une grande campagne de communication s'inscrivant dans la durée à destination de tous, citoyens et entreprises :
· via les médias traditionnels, à l'image des campagnes menées sur la sécurité routière, à travers des spots de télévision, des insertions dans la presse écrite... ;
· par la fourniture de CD et de brochures gratuites (en s'inspirant par exemple d'initiatives récentes comme « l'Internet plus sûr, ça s'apprend »...) ;
· par l'organisation de journées nationales [1].

– **Communiquer** : mettre en place un portail Internet, véritable centre de ressources pour mettre à la disposition des utilisateurs, citoyens et entreprises, des informations d'actualité, des guides de bonnes pratiques, des contacts, des logiciels de tests gratuits, des alertes sur les menaces...

– **Former** : proposer au système éducatif, du primaire à l'enseignement supérieur (universités et grandes écoles) et au système de formation continu, des canevas de formation en SSI conçus en relation notamment avec le ministère de l'Éducation nationale et des organismes de formation spécialisés (CFSSI...), déclinables de la sensibilisation de 2 heures à la formation diplômante à l'image de ce qui se met en place pour l'intelligence économique.

– **Informer l'utilisateur d'outils personnels de communication** : à l'instar du port de la ceinture pour l'utilisation d'un véhicule automobile, imposer que la documentation utilisateur qui accompagne les produits personnels de communication (ordinateurs personnels, assistants personnels, téléphones, matériels et logiciels de communication utilisant notamment les technologies sensibles telles qu'Internet, Wifi...) mentionne les risques principaux encourus vis-à-vis de la protection des informations, les points de vigilance pour l'utilisateur et les recommandations types à mettre en œuvre (exemple : activer un pare-feu, protéger et changer régulièrement son mot de passe...).

Axe 2 : Responsabiliser les acteurs

Tous les acteurs qui interviennent dans les systèmes d'information (administration, fournisseurs de solutions de sécurité, fournisseurs

1. Voir les actions de la délégation aux usages de l'Internet et de la Finlande.

d'accès Internet, sociétés de services, opérateurs télécoms, utilisateurs) doivent être impliqués et responsabilisés.

En relation notamment avec les organisations professionnelles et syndicales ainsi que les ministères concernés, cela passera en particulier par :
– l'établissement obligatoire de chartes à l'usage des utilisateurs (en particulier lorsqu'ils se déplacent à l'étranger), annexées au contrat de travail des salariés, y compris de la fonction publique, ou aux règlements intérieurs des entreprises ;
– la labellisation des entreprises fournisseurs de produits ou services de SSI (infogérance de sécurité, fournisseurs de logiciels ou de matériels...) qui respectent un cahier des charges à établir.

Axe 3 : Renforcer la politique de développement de technologies et de produits de SSI et définir une politique d'achat public en cohérence

La sécurisation de l'administration et des entreprises sensibles impose de disposer de produits de sécurité maîtrisés, au moins pour des fonctions sensibles. L'offre disponible se révèle notoirement insuffisante. L'État doit concentrer des investissements sur les technologies et les produits de sécurité clés en misant sur quelques acteurs.

– Cette politique de développement de technologies et de produits de SSI doit contribuer ainsi :
• au maintien et au développement d'une industrie nationale et européenne spécialisée, autonome et compétitive capable de développer des produits de sécurité au rythme de l'évolution des besoins et des menaces ;
• à l'exportation auprès de clients soucieux de diversifier leurs fournisseurs ;
• à la création d'emplois à haute valeur ajoutée.

Pour ce faire, les actions suivantes seront à réaliser, notamment en relation avec les entreprises :
– identifier périodiquement les maillons des systèmes d'information qui exigent des produits qualifiés au sens de la DCSSI pour garantir la souveraineté de l'État et des entreprises ;
– établir et tenir à jour un catalogue des produits de sécurité nationaux qualifiés et des produits européens adaptés aux différents niveaux de sécurité à assurer ;
– enrichir ce catalogue par une politique volontariste de financements publics de R&D, nationale ou en coopération avec nos partenaires européens ;
– mobiliser les différents intervenants (ANR, A2I, fonds européens et les entreprises) pour accroître l'effort de recherche en SSI ;
– recentrer, mieux coordonner et intensifier les mécanismes d'aides au développement des PME innovantes dans la SSI ;
– inciter les grands groupes à faire confiance aux PME de SSI, à travers notamment le pacte PME ;

– renforcer la politique de certification et de qualification de produits et services de SSI par une augmentation des produits certifiés et qualifiés et une réduction des délais et des coûts de certification.
– accroître la présence et l'influence française dans les groupes de standardisation et les comités de normalisation ;
– renforcer les fonds d'investissement en capital développement.

– Le développement de technologies et de produits doit s'accompagner de la mise en œuvre d'une politique d'achat public de produits et services de SSI, en conformité avec les règles des marchés publics et les directives européennes, fondée sur le principe d'autonomie compétitive, qui s'articulerait autour de trois objectifs complémentaires :
• garantir la meilleure efficacité économique des investissements réalisés par les ministères pour satisfaire leurs besoins de sécurité ;
• assurer un accès à des capacités industrielles et technologiques qui conditionnent la satisfaction à long terme de ces besoins ;
• recourir à des acteurs de confiance.

Six actions devront être engagées :
– initier une action interministérielle visant à définir et à organiser une politique d'achat commune (définition des processus, des critères de choix...) ;
– former les acheteurs à l'achat de produits et services de SSI ;
– identifier et suivre la chaîne de fournisseurs intervenant sur la SSI : sous-traitants, laboratoires... ;
– inciter au regroupement de l'offre nationale puis européenne via la commande publique, pour faciliter une meilleure structuration du tissu industriel et permettre à des PME d'atteindre la taille critique ;
– faciliter l'accès des PME innovantes de SSI à la commande publique ;
– informer les fournisseurs des programmes à venir.

Axe 4 : Rendre accessible la SSI à toutes les entreprises

Le manque de maturité et une sensibilisation insuffisante de la plupart des entreprises françaises face aux risques qui pèsent sur leurs systèmes d'information, alors que les enjeux économiques notamment en terme d'emplois sont significatifs, nécessitent la mise en œuvre des actions suivantes :

– **inciter** les entreprises, en particulier les PME, à mettre en place, faire auditer et éventuellement certifier la sécurité de leurs systèmes d'information par des organismes habilités, comme cela avait été le cas pour la certification des systèmes qualité.

Pour ce faire, il est proposé la mise en place d'aides publiques, individuelles et collectives, visant à couvrir une partie des frais de conseils engagés auprès de prestataires dûment labellisés ;

– **créer** un centre d'aide et de conseil, guichet unique pour assister les entreprises ne disposant pas d'une expérience mature en SSI et les utilisateurs lorsqu'ils subissent des attaques informatiques ;

– **diffuser** aux PME sous une forme adaptée, les informations de veille, d'alerte et de réponse disponibles au niveau des CERT nationaux ;

– **initier et animer** des forums thématiques public – privé favorisant la circulation d'informations, les retours d'expériences, le partage des bonnes pratiques...

Axe 5 : Accroître la mobilisation des moyens judiciaires

La spécificité des contentieux liés aux systèmes d'information, la complexité et l'ampleur croissante des attaques devraient faire l'objet d'une reconnaissance plus forte qui pourrait se traduire :

– par des aménagements législatifs, notamment :
· une aggravation des peines prévues aux articles 323-1 et suivants du code Pénal, dans le prolongement de la loi du 21 juin 2004 pour la confiance dans l'économie numérique ;
· une évolution législative introduisant une exception au principe d'interdiction de la rétro-conception (art. L122-6-1 IV du code de la propriété intellectuelle) pour des motifs de sécurité.

– par une sensibilisation accrue des magistrats et des forces de sécurité (douanes, police et gendarmerie) en formation initiale et continue ;

– par la constitution d'un pôle judiciaire spécialisé et centralisé de compétence nationale ;

– par un renforcement des coopérations internationales visant à améliorer la réalisation des enquêtes judiciaires hors des frontières.

Axe 6 : Assurer la sécurité de l'État et des infrastructures vitales

La prise en compte des impératifs de SSI par les départements ministériels et les organismes sous tutelle a été jugée très inégale et globalement insatisfaisante. Les mesures suivantes devraient être mises en œuvre :

– mettre à jour les politiques de sécurité des systèmes d'information et les schémas directeurs de chaque ministère et les valider par une autorité centrale ;

– conseiller en amont les maîtrises d'ouvrage de l'État pour des projets sensibles et prescrire des dispositions pour la rédaction des consultations (par exemple cartes d'identité et dossier médical personnalisé) ;

– confier à une autorité centrale le rôle d'approuver formellement le lancement de ces projets sensibles après avoir précisé les critères de sensibilité dans des délais compatibles avec les besoins opérationnels ;

– identifier les éléments constitutifs des systèmes d'information qui doivent impérativement faire appel, pour leur réalisation, à des produits qualifiés ou à des prestataires labellisés ;

– faire contrôler par une autorité centrale l'application de ces prescriptions par des inspections sur site et des tests d'intrusion sans préavis ;

– pour disposer de spécialistes, mettre en place puis animer une filière SSI transverse dans laquelle la mobilité sera organisée, tant à l'intérieur de la fonction publique qu'au travers de passerelles avec les entreprises et les centres de recherche ;

– définir les profils de poste des responsables (HFD [1], FSSI, AQSSI...) intégrant des formations spécialisées et renforcer leur autorité et leur responsabilité au sein de leur ministère pour décliner à leur niveau la politique gouvernementale ; ils devront être indépendants des directions des systèmes d'information.

Pour ce qui est des opérateurs d'infrastructures vitales :
– valider la politique de sécurité par l'autorité centrale ;
– conduire des inspections et des tests d'intrusion.

Pour les entreprises sensibles, faire à la demande des audits et des tests d'intrusion.

* * *

Il est à noter que certaines recommandations du rapport rejoignent les mesures proposées dans le Plan de Renforcement de la Sécurité des Systèmes d'Information de l'État en 2004.

Ces recommandations ont été formulées à partir des éléments recueillis lors des nombreuses auditions qui ont été conduites.

Un impératif : Refondre l'organisation de la SSI de l'État

En complément aux six recommandations, afin d'amener notre pays à un niveau de sécurité et d'autonomie contrant les menaces, la nécessité s'impose :
– de renforcer l'action de l'État et de ses moyens humains et financiers en matière de SSI ;
– de rationaliser l'organisation des services de l'État ;
– d'accroître la cohérence des actions des différents acteurs.

1. Il est proposé d'intégrer plus fortement une composante sécurité dans les fonctions de HFD.

Le renforcement significatif des missions actuelles de la DCSSI qui en découlent, en particulier les plus opérationnelles, amène également à remettre en cause l'organisation mise en place en 1995.

Rappel du dispositif principal actuel :
– SGDN : veiller à la cohérence des actions gouvernementales en matière de SSI pour répondre aux objectifs définis par le Premier ministre ;
– DCSSI : assurer la sécurité des systèmes d'information de l'État et créer les conditions d'un environnement de confiance ;
– CISSI : assurer la concertation entre les départements ministériels ;
– ministère de la Défense : assurer la maîtrise d'œuvre des produits gouvernementaux de haute sécurité ;
– ministère de l'Économie, des Finances et de l'Industrie : assurer l'animation du développement des produits de sécurité non-gouvernementaux.

Cette organisation ne semble plus adaptée aux enjeux actuels.

Le nouveau dispositif présenté ne prend pas en compte les directions spécialisées comme la DST et la DGSE dont les missions sur la SSI **n'ont pas à être changées**.

Néanmoins, il s'agira de clarifier les rôles respectifs des nouvelles structures présentées ci-après avec notamment l'ADAE et la CNIL.

Pour ce qui est de la DGA, partie CELAR, sa spécificité, participer aux grands programmes industriels (porte-avions...), l'amène à être moins présente sur le secteur R&D en SSI. Les engagements budgétaires de ces dernières années l'ont montré. Aussi sera-t-il nécessaire de revoir son implication sur ce thème dans la future organisation.

Il est proposé :
– de recentrer le dispositif étatique sous l'autorité du Premier ministre afin de garantir la mise en œuvre des axes stratégiques et d'assurer la dimension interministérielle du dispositif (décider, arbitrer, sanctionner) ;
– de séparer les fonctions opérationnelles des fonctions d'autorité ;
– de mettre en place, à partir des fonctions opérationnelles de la DCSSI renforcées, une structure opérationnelle dédiée, centralisée et rattachée au Premier ministre ayant une culture de résultats pour assurer la mise en œuvre d'une partie importante des 6 axes.

Dans ce schéma, les fonctions d'autorité resteraient au sein du SGDN et comprendraient à titre d'exemple les missions suivantes :
– élaborer la politique nationale de SSI pour le compte et sous l'autorité du Premier ministre et ses évolutions futures ;
– valider les politiques de SSI de chaque ministère et des organismes sous tutelle ;
– évaluer les résultats de la structure opérationnelle ;
– assurer une veille stratégique sur l'évolution des risques, des menaces, de la réglementation... ;
– initier le renforcement de la dimension judiciaire et des actions interministérielles en matière de politique d'achat.

Les missions de la structure opérationnelle rattachée au Premier ministre pourraient être notamment les suivantes :

Informer, sensibiliser, communiquer, veiller

– l'information et les actions de sensibilisation et de formation de tous les publics (administrations, entreprises, monde académique, citoyens...) ;
– la veille technique et méthodologique : animation d'un réseau de veille SSI...
– la capitalisation et la diffusion des informations technologiques et méthodologiques (fiches techniques, guides, recommandations...) ;
– les échanges d'information entre les domaines SSI et IE ;
– la communication (portail, brochures, guides méthodologiques...) ;
– la promotion de la SSI (séminaires, colloques, prix...).

Conseiller, supporter, auditer, inspecter

– le conseil et le support aux organisations gouvernementales, aux établissements publics, aux grands réseaux d'infrastructure vitale et aux entreprises sensibles (au sens de l'IE) ;
– l'animation, le conseil, le support et le suivi de l'activité des HFD en ce qui concerne le volet SSI de leurs activités ;
– le support technique et méthodologique aux services de sécurité et de justice ;
– le premier niveau d'accueil PME/PMI (guichet unique d'aiguillage) ;
– la promotion de démarches méthodologiques, d'architectures solides et de plans de réaction en cas d'incident ;
– audits et inspections (organisation, continuité d'activité...) et tests d'intrusion.

Certifier, standardiser et normaliser

– la responsabilité des plans d'actions de standardisation et de normalisation avec un rôle actif dans les comités nationaux et internationaux ;
– la responsabilité de la certification et des actions de labellisation (fournisseurs, produits et services).

Alerter et réagir

– la gestion de crise SSI (supervision et coordination des services, ressources dédiées...) en liaison avec les cellules de crise étatiques (COSSI) ;
– la consolidation des différents réseaux d'alerte (CERTs) ;
– la supervision de dispositifs régionaux d'alerte PME/PMI à créer et qui pourraient être hébergés par exemple par les CRCI.

Mettre en œuvre la politique industrielle et d'achats publics

– la responsabilité des plans d'actions d'identification, d'évaluation et de développement des technologies et de produits sensibles (cryptologie, biométrie, clés publiques, carte à puces...) ;
– la responsabilité des plans d'action de renforcement (financement...) du tissu industriel et des laboratoires de recherche spécialisés en SSI (matériels et services) ;
– le suivi du respect des impératifs des politiques SSI dans la commande publique (sensibilisation des instances réglementaires à la démarche SSI).

Participer aux relations institutionnelles internationales SSI

– la gestion des partenariats et des coopérations institutionnelles internationales : coopération européenne, autres agences SSI à l'étranger, relations SSI avec les entités intervenant dans les domaines de la sécurité et de la défense (OCDE, OTAN...).

Assurer la gestion des ressources humaines

– la gestion de la filière de personnels spécialisés en SSI (FSSI, AQSSI, ASSI), avec notamment la définition des profils de postes ;
– la formation initiale et continue des personnels spécialisés.

Enfin, la structure opérationnelle constitue un centre d'expertises et de moyens au service des fonctions d'autorité.

Constituées autour des équipes de l'actuelle DCSSI (environ 110 personnes), les ressources de la structure opérationnelle seraient renforcées par des compléments de ressources pluridisciplinaires permanentes et des apports d'expertises ponctuelles externes publiques ou privées en fonction des programmes qu'elle sera amenée à conduire. À titre de référence, le BSI allemand disposait en 2004 d'un budget de 51 millions d'euros (dont 19 millions de budget d'études et de développement) et de 410 collaborateurs.

Afin de pouvoir :
– gérer une relation client/fournisseur basée sur la compétence et la qualité, les clients étant les administrations publiques, les collectivités territoriales, les entreprises, les réseaux d'infrastructures, les organismes de recherche et d'enseignement, et enfin les utilisateurs,
– attirer des compétences pointues dans des cadres de coopération et de rémunération souples,
– élaborer des contrats de partenariat dans des conditions analogues à ceux des entreprises privées ou publiques,

la structure opérationnelle pourrait bénéficier d'un statut de type EPIC.

Enfin, la structure opérationnelle serait, comme le BSI allemand :
– dotée de principe de gouvernance garantissant la confiance, l'implication des personnels, la transparence et la neutralité ;
– mesurée sur ses activités, notamment de support, de communication et de formation, selon des critères de performance et de qualité.

Annexes

Annexe I

Bibliographie

Sites Web

Français

Gouvernementaux

• www.certa.ssi.gouv.fr : site du centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA).
• www.adae.gouv.fr : site de l'agence de développement de l'administration électronique.
• cfssi@sgdn.pm.gouv.fr et www.formations.ssi.gouv.fr
• www.club.senat.fr : laboratoire d'idées du Sénat en amont des processus législatifs.
• www.internet.gouv.fr : site dédié à l'action de l'État et société de l'information.
• www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic : site de la Police nationale (OCLCTIC).
• www.legifrance.gouv.fr : service public de la diffusion du droit.
• www.ssi.gouv.fr : site gouvernemental d'information sur la SSI.
• www.telecom.gouv.fr : site de la direction générale de l'industrie, des technologies de l'information et des postes au ministère en charge de l'Économie, des Finances et de l'Industrie (DIGITIP).

Autres sites

• www.adit.fr : site de l'agence pour la diffusion de l'information technologique (ADIT).
• www.afnor.fr : site de l'association française de normalisation (AFNOR).
• www.clusif.asso.fr : site du club de la sécurité des systèmes d'information français (CSSIF), association qui s'est fixé l'analyse de la sinistralité dans le monde informatique.
• www.cnil.fr : site de la commission nationale de l'informatique et des libertés (CNIL).
• www.cigref.fr : site du club informatique des grandes entreprises françaises (CIGEF).
• www.fing.org : site de la fondation Internet nouvelle génération (FING).
• www.foruminternet.org : site du forum des droits sur Internet.
• www.idc.com ou www.idc.com/france/index.html : sites d'IDC, spécialiste du conseil dans le domaine des technologies de l'information.
• www.journaldunet.com : site du *Journal du Net*, journal en ligne comportant de nombreuses rubriques dédiées à la sécurité notamment sur Internet et à des témoignages d'entreprises et de prestataires.

• www.ladocumentationfrancaise.fr : site de la Documentation française.
• www.osir.org : site de l'observatoire de la sécurité des systèmes d'information et des réseaux (OSSIR).
• www.sg.cnrs.fr : site du Centre national de la recherche scientifique (CNRS) dédié à la sécurité et à la protection du patrimoine scientifique.
• www.urec.cnrs.fr : site de l'UREC/CNRS.

Étrangers

• www.bsi.bund.de : site du Bundesamt für Sicherheit der Informationstechnik du Gouvernement allemand.
• www.cert.org : site du Cert Coordination Center, organisation mondiale animant l'ensemble des CERT nationaux.
• www.cesg.gov.uk : site du Communications Electronics Security Group, the National Technical Authority for Information Assurance du Royaume-Uni.
• www.cse.dnd.ca : site du centre de la sécurité des télécommunications du Canada.
• www.dsd.gov.au : site du Defence Signals Directorate – Australian Government – Department of Defence.
• www.enisa.eu.int : site de l'European Network and Information Security Agency (ENISA).
• www.issaireland.org : site de l'Irish Information Security Organisation.
• www.nist.gov : site de l'agence américaine National Institute of Standards and Technology.
• www.nsa.gov : site de la National Security Agency/Central Security Service des États-Unis.
• www.raingod.com/angus/Computing/Internet/spam/index.html : site de spammers Live in Vain, association anglophone dédiée à la lutte contre les spams.
• www.securitystats.com : site anglophone créé en avril 2000 afin de disposer de statistiques mondiales sur la sécurité informatique.
• www.sophos.fr/virusinfo/analyses/w32sassera.html
• http://Webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase site de l'OCDE dédié à la sécurité des systèmes d'information.
• www.xesic.com : certification, normes.

Bibliographie

• *01 Informatique -01 DSI*.
• *Cybersecurity Curricula in European Universities*, Gabriel Clairet, Observatoire des sciences et des techniques – Fondazione Rosselli, janvier 2003.
• *Politique de sécurité des systèmes d'information et sinistralité en France*, enquête intersectorielle, Clusif, 2003.
• Plan « Safer Internet Plus », Commission européenne, 2005.
• *Computer Crime and Security Survey*, CSI/FBI, 2005.
• *Dynamique de la relation entre direction générale et direction des systèmes d'information dans les grandes entreprises françaises*, Livre blanc CIGREF/MacKinsey&Company, novembre 2002.

• *Dynamique des relations autour des systèmes d'information dans les équipes de direction des grandes entreprises françaises*, Livre blanc CIGREF/MacKinsey&Company, septembre 2004.
• *Futuris et conseil stratégique des technologies de l'information*, Groupement français de l'industrie de l'information, octobre 2003.
• *Guide de l'archivage électronique sécurisé*, juillet 2000.
• *Guide de sensibilisation à la sécurisation des systèmes d'information et du patrimoine informationnel de l'entreprise*, Medef, mai 2005.
• Direction de l'innovation et de la recherche, Medef, mai 2005.
• *Guide de la sécurité des systèmes d'information à l'usage des directeurs*, CNRS, 2e trimestre 1999.
• *Western European security software forecast and competitive vendors shares*, *2003-2008*, IDC, 2003.
• *Marché français de la sécurité des systèmes d'information (entreprises) – état de l'offre et de la demande*, IDC, 2005.
• *Intelligence économique et stratégique. Les systèmes d'information au cœur de la démarche*, CIREF, mars 2003.
• *Intelligence économique appliquée à la direction des systèmes d'information*, CIGREF, mars 2005.
• *Intelligence juridique et systèmes d'information*, CIGREF, septembre 2004.
• *Intimité et sécurité, les clefs de la confiance dans l'économie numérique*, club Sénat.fr, juin 2004.
• L'agence économique et financière (AGEFI).
• *La sécurité à l'heure d'Internet*, Rapport du CIGREF, octobre 2000.
• *La sécurité des systèmes d'information dans les entreprises françaises en 2004, vision comparée de la France et du monde*, Ernst&Young, décembre 2004.
• *Le Monde Informatique*.
• *L'État stratège – les organes, les outils et les pratiques au sein de la sphère publique : de la gestion à la gouvernance*, CEPS, octobre 2005.
• *Les priorités des responsables sécurité en 2005*, Cahier thématique, CSO, avril 2005.
• *Les Échos*.
• *Internet Secutiy System (ISS) sur la sécurité des systèmes d'information*, Livre blanc, IDC France, avril 2005.
• *Mission pour l'économie numérique – tableau de bord du commerce électronique de décembre 2004*, 6e édition, Services des études et des statistiques industrielles (SESSI), Ministère délégué à l'Industrie.
• *Plan de renforcement de la sécurité des systèmes d'information de l'État (2004-2007)*, 10 mars 2004.
• *Politique industrielle : les outils d'une nouvelle stratégie*, Bernard Carayon – Député, Assemblée nationale, mai 2005.
• Politique de référencement intersectorielle de sécurité (PRIS) – ADAE et SGDN-DCSSI – version 2.0 du 1er juin 2005.
• *Pour une stratégie de sécurité économique nationale*, Bernard Carayon – Député, Assemblée nationale, juin 2004.
• *Pour un management stratégique des cyber-risques*, Hervé Schauer, Livre blanc des assises de la sécurité, octobre 2004.
• *Quelle sécurité après le 11 mars ?*, SERENDIP, septembre 2004.

• *Rapport sur la sécurité des réseaux*, Club Sénat.fr, 2005.
• *Internet Security Threat Report*, société Symantec, septembre 2006.
• Thierry Dassault, « Les espaces de confiance » *in Défense Nationale*, nº 11, novembre 2005.
• *Sécurité des réseaux et de l'information : proposition pour une approche politique européenne*, Communication de la commission au Conseil, au Parlement européen, au comité économique et social et au comité des régions, 2001.
• *Sécurité des systèmes d'information. Quelle politique globale de gestion des risques ?*, CIGREF, septembre 2002.
• Veille *stratégique. Organiser la veille sur les nouvelles technologies de l'information*, CIGREF, septembre 1998.
• *Synthèse des besoins de sécurité et analyse des risques*, Étude OPPIDA pour le compte du Minefi/DIGITIP, septembre 2002.

Annexe II

Liste des entretiens

Premier ministre

Secrétariat général de la Défense nationale
Monsieur Francis Delon, *secrétaire général*
Monsieur Alain Juillet, *haut responsable chargé de l'Intelligence économique*

Direction centrale de la sécurité des systèmes d'information
Monsieur Henri Serres, *vice-président du CGTI, ancien directeur*
Monsieur Patrick Pailloux, *directeur*
Monsieur le général de division Jean Novacq, *directeur adjoint*

Sous-direction scientifique et technique
Monsieur Florent Chabaud, *sous-directeur*

Centre de certification
Monsieur Pascal Chour

Ministère de l'Intérieur et de l'Aménagement du territoire

Direction de la Défense et de la Sécurité civile
HFD/FSD/FSSI
Monsieur Alain Waquet, *préfet, haut fonctionnaire de Défense adjoint*
Monsieur Stéphane Guillerm, *conseiller technique auprès du HFD adjoint, fonctionnaire de sécurité des systèmes d'information adjoint*

Direction des systèmes d'information et de communication
Secrétariat général
Monsieur Jean-Claude Jeanneret, *ingénieur général des télécommunications, directeur adjoint*
Monsieur Reynald Bouy, *ingénieur en chef des télécommunications, sous-directeur de l'Ingénierie, de l'Équipement et de l'Exploitation*

Direction centrale de la Police judiciaire
Monsieur Christian Aghroum, *commissaire principal, chef du service interministériel d'assistance technique*
Madame Marie Lajus, *commissaire principal, adjointe au chef de l'OCLCTIC*

Direction de la surveillance du territoire
Monsieur Pierre de Bousquet de Florian, *préfet, directeur*

Sous-direction des services techniques et des moyens informatiques
Monsieur Michel Guerin, *contrôleur général, sous-directeur*
Monsieur Stéphane Tijardovic, *commissaire divisionnaire, chef de division*

Ministère de la Défense

État-major des Armées
Monsieur Le général d'armée Henri Bentegeat, *chef d'État-major*

Direction générale de la sécurité extérieure
Monsieur Pierre Brochand, *directeur*
Monsieur le général Mathian, *directeur technique*

Gendarmerie nationale

Direction générale de la Gendarmerie nationale
Monsieur le général Christian Brachet, *sous-directeur des télécommunications et informatique*

Ministère des Affaires étrangères

Cabinet du ministre
Monsieur Frédéric Dore, *directeur adjoint*
Monsieur Philippe Guelluy, *ambassadeur de France en Chine*
Monsieur Jean-Paul Dumont, *haut fonctionnaire de Défense*

Service des systèmes d'information et de communication
Monsieur Francis Étienne, *chef du service*
Monsieur Jean Cueugniet, *sous-directeur, adjoint au chef de service*

Direction technique
Monsieur Denys Tillet

Ministère de l'Économie, des Finances et de l'Industrie

Monsieur Didier Lallemand, *haut fonctionnaire de Défense*

Direction des Affaires juridiques
Monsieur Jérôme Grand d'Esnon, *directeur*

Ministère délégué au Budget et à la Réforme de l'État

Agence pour le développement de l'administration électronique (ADAE)
Monsieur Jacques Sauret, *directeur*

Ministère délégué à l'Industrie
Monsieur François Loos, *ministre délégué*
Monsieur Arnaud Lucaussy, *conseiller technique*

Service des technologies et de la société de l'information
Sous-direction réseaux, multimédia et communication en ligne
Madame Mireille Campana, *ingénieur général des télécommunications, sous-directrice*

Ministère des Transports, de l'Équipement, du Tourisme et de la Mer

Monsieur Serge Philibeau, *HFD/FSSI, chef de la mission SSI*

Ministère de la Santé et des Solidarités

Monsieur Gérard Dumont, *haut fonctionnaire de Défense*

Ministère délégué à la Recherche et à l'Enseignement supérieur

Direction de l'Enseignement supérieur
Monsieur Jean-Marc Monteil, *directeur*
Madame Isabelle Morel, *FSSI*

Délégation aux usages de l'Internet
Monsieur Benoît Sillard

Autorités administratives

AMF
Direction gestion interne et ressources humaines
Madame Florence Roussel, *secrétaire générale adjointe*

Service des systèmes d'information
Monsieur François Paysant, *chef du service*

CNIL
Monsieur Christophe Pallez, *secrétaire général*

Direction de l'expertise informatique et des contrôles
Monsieur Jean-Luc Bernard, *expert informaticien*

Forum des droits sur Internet
Madame Isabelle Falque-Pierrotin, *présidente*

Grandes entreprises

Aéroports de Paris
Direction de la Sûreté
Monsieur Jean-Louis Blanchou, *préfet, directeur*

Direction de l'informatique et télécommunications
Monsieur Jean Verdier, *directeur*
Monsieur Guy-Pierre Rodriguez, *responsable pôle infrastructures et architectures techniques*

Direction de la Stratégie
Monsieur Jean-Pierre Roche, *manager des risques*
Monsieur Jacques Demeuzoy, *responsable sécurité systèmes informatiques*

Air France

Direction générale des systèmes d'information

Monsieur Jean-Christophe Lalanne, *directeur stratégie, architecture, technologie, sécurité*

Monsieur Bruno Chambrelent, *responsable de la sécurité des systèmes d'information*

AFNOR

Monsieur Pascal Poupet, *chef du département transports, énergies et communications*

AXA

Monsieur Pascal Buffard, *directeur AXA France services*

AXALTO

Monsieur Laurent Vieille, *VP Business développement*

Monsieur Philippe Bouchet, *responsable sécurité*

Monsieur Pierre François, *business manager governement*

Banque de France

Monsieur George Peiffer, *adjoint au secrétaire général, directeur de l'organisation informatique*

Direction de la prévention des risques

Monsieur Jean-Pierre Delmas, *responsable de la sécurité de l'information*

CDC

Monsieur Jean-Jacques Delaporte, *directeur général informatique*

Monsieur Serge Bergamelli, *responsable du département des équipements numériques des territoires et du programme FAST*

CISCO

Monsieur Alain Fiocco, *directeur Europe stratégie technologique*

Monsieur Olivier Esper, *responsable affaires publiques*

Crédit Agricole

Monsieur Robert Zeitouni, *responsable du pôle sécurité et continuité d'activité*

EADS

Monsieur J.P. Quemard, *directeur de la sécurité DCS/EADS*

Monsieur I. Lahoud, *directeur scientifique CCR/EADS*

Monsieur Jean-Pierre Philippe, *secrétaire général marketing/international/stratégie*

EDF

Madame Dominique Spinosi, *directrice de la sécurité*

Monsieur Renaud de Barbuat, *directeur des systèmes d'information*

France Télécom

Monsieur Philippe Duluc, *directeur de la sécurité, direction de la sécurité de l'information*

Groupement des cartes bancaires

Monsieur Yves Randoux, *administrateur*

IBM
Monsieur Jean Grevet, *IGS/Responsable sécurité et Risk management*

KEYNECTIS
Monsieur Thierry Dassault, *président*
Monsieur Pascal Colin, *directeur général*

La Poste
Direction de la qualité et de la sécurité du groupe
Service de la sûreté du groupe
Monsieur Eric Le Grand, *directeur sécurité du groupe*
Monsieur Hervé Molina, *superviseur de l'audit informatique*

Michelin
Monsieur Jean-Pierre Vuillerme, *directeur des services environnement et prévention du groupe*

Microsoft
Monsieur Bernard Ourghanlian, *directeur technique et sécurité*
Monsieur Stéphane Senacq, *responsable affaires publiques et relations institutionnelles*

OSEO BDPME
Monsieur Xavier de Broca, *directeur de l'organisation et des systèmes d'information*

FIEEC
Monsieur Pierre Gattaz, *vice-président, président de Radiall*

RIM
Monsieur Don Morrison, directeur général des opérations de RIM
Monsieur Pierre Bury, directeur des relations avec le secteur public en Europe
Madame Valérie Wang, *ingénieur*

Sagem Défense Sécurité
Groupe Safran
Division sécurité
Monsieur Jean-Paul Jainsky, *directeur général adjoint, directeur de la division sécurité*

Département systèmes d'information et de commandement aéroterrestre
Division optronique et systèmes aéroterrestres
Monsieur Laurent Dupas, *directeur*
Monsieur le général Patrice Sartre, *conseiller militaire Terre*

SNCF
Direction des finances, des achats et des systèmes d'information et de télécommunication
Monsieur Michel Baudy, *directeur des systèmes d'information et télécommunication*

Suez
Monsieur Jean-Michel Binard, *directeur des systèmes d'information*
Monsieur Henry Masson, *directeur central risques, organisation et services centraux*
Monsieur Régis Poincelet, *directeur département sécurité groupe*

Thales
Monsieur Dominique Vernay, *directeur de la recherche*
Monsieur Jacques Bidaut, *direction sécurité groupe, sécurité des systèmes d'information*
Monsieur Marko Erman, *directeur de la recherche et de la technologie, système terre et interarmées*
Monsieur Jacques Delphis, *directeur des relations extérieures et institutionnelles*

Total
Monsieur Philippe Chalon, *directeur des systèmes d'information et télécommunication*
Monsieur Christophe Cevasco, *chargé des relations avec le Parlement et les élus*

PME

Arkoon
Monsieur Thierry Rouquet, *président*

Ercom
Monsieur Jean Lacroix, *président*

Everbee Networks
Monsieur Patrick de Roquemaurel, *président*

Ideal X
Monsieur Olivier Guilbert, *président-directeur général*

NETASQ
Monsieur Jean-Pierre Tomaszek, *directeur général*

LSTI
Madame Armelle Trotin, *présidente*

OPPIDA
Monsieur Olivier Mary, *directeur technique*

SISTECH
Monsieur Roger Simon, *président-directeur général*
Monsieur Jérôme Chappe, *directeur général*

Fonds d'investissement

ACE Management
Monsieur Thierry Letailleur, *managing partner*

Alven Capital
Monsieur Charles Letourneur, *partner*

Ventech
Monsieur Eric Huet, *general partner*

Iris Capital
Monsieur Pierre de Fouquet, *managing partner*

Écoles/instituts

École Polytechnique
Monsieur Maurice Robin, *directeur de la recherche*

ENST Bretagne
Monsieur Gilles Martineau, *directeur d'études, délégué du directeur, responsable du campus ENST Bretagne à Rennes*

EPITECH
Monsieur Sébastien Benoît, *professeur, responsable Intranet/site Web EPITECH*

INRIA
Monsieur Claude Kirchner, *directeur de recherche, responsable du projet Prothéo*
Monsieur Laurent Kott, *executive advisor INRIA Transfert*

INT
Monsieur Jean-Louis Ermine, *professeur, directeur du département des systèmes d'information*

SUPELEC
Monsieur Alain Bravo, *directeur général*

Associations/organisations professionnelles

Comité richelieu
Monsieur Buselli, *président*
Monsieur Emmanuel Leprince, *délégué général*

CIGREF
Monsieur Jean-François Pepin, *délégué général*
Monsieur Ludovic Étienne, *chargé de mission*
Monsieur Stéphane Rouhier, *chargé de mission*
Madame Sophie Bouteiller, *chargée de mission*
Monsieur Janick Taillandier, RATP, *département ses systèmes d'information et de télécommunication, directeur du département*
Monsieur François Blanc, VALEO, *directeur des systèmes d'information*
Monsieur Zbigniew Kotur, NEXANS, *responsable de la sécurité*

CLUSIF
Monsieur Pascal Lointier, *délégué général*

FEDERATION SYNTEC
Monsieur Bruno Carrias, *délégué général*

MEDEF

Madame Catherine Gabay, *directrice innovation, recherche, nouvelles technologies*

Droit

Monsieur David Benichou, *magistrat*
Monsieur Jean-Louis Bruguière, *magistrat*
Monsieur Alain Bensoussan, *avocat à la Cour*

Étranger

Responsables/BSI

Glossaire

Technique (source DCSSI)

Agent de sécurité : Il a pour mission d'appliquer les mesures de sécurité aux documents classifiés *très secret* et d'en assurer la gestion. Il est désigné par le chef de l'organisme où est implantée l'antenne ; ses missions ne doivent pas être confondues avec celles qui sont dévolues à l'agent de sécurité dans une entreprise titulaire d'un marché classé de Défense qui est désigné par le responsable de l'entreprise après agrément de l'Administration ayant contracté le marché.

Agrément : Reconnaissance formelle que le produit ou système évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies.

Agrément d'un laboratoire : Reconnaissance formelle qu'un laboratoire possède la compétence pour effectuer des évaluations d'un produit ou d'un système par rapport à des critères d'évaluation définis.

Analyse cryptologique : Étude des moyens de chiffrement pour en déceler et mettre en évidence les faiblesses de conception ou les fautes éventuelles d'utilisation.

Architecture fonctionnelle : Décrit les objets du système essentiel : traitements, données, contrôles. L'architecture fonctionnelle constitue le premier niveau – niveau conceptuel – dans le cycle d'abstraction de la conception.

Architecture technique : Décrit les ressources nécessaires au système de traitement de l'information : transformation, mémorisation/acquisition/visualisation, communication. L'architecture technique constitue le deuxième niveau – niveau logique – dans le cycle d'abstraction de la conception.

Archivage : « Dès qu'ils ne font plus l'objet d'une utilisation habituelle, les documents classifiés présentant un intérêt administratif et historique doivent être versés aux dépôts d'archives suivants : soit les services historiques des armées pour le département ministériel de la Défense et les services rattachés, soit les archives du ministère des Relations extérieures, pour ce qui les concerne, soit la direction des Archives de France – Archives Nationales – pour toutes les administrations et organismes civils gérant des archives publiques, ces services étant seuls équipés, en effet, pour recevoir des documents classifiés, jusqu'au niveau Secret Défense inclus... »

Assurance : Propriété d'une cible d'évaluation permettant de s'assurer que ses fonctions de sécurité respectent la politique de sécurité de l'évaluation.

Attributs de sécurité : Informations (telles que l'identité, le niveau d'habilitation, le besoin d'en connaître, etc.) relatives à un utilisateur autorisé, permettant d'établir ses droits et privilèges.

Attestation de reconnaissance de responsabilité : Elle a pour objet de faire prendre conscience au titulaire d'une décision d'admission ou d'agrément des responsabilités particulières qui viennent s'ajouter à ses responsabilités administratives du fait de l'autorisation d'accès aux informations classifiées. Il est nécessaire, en raison de la gravité des infractions en matière de protection des informations classifiées, sanctionnées par les dispositions du code pénal, que le titulaire de la décision d'admission en soit informé au préalable.

Audit : Examen méthodique d'une situation relative à un produit, un processus, une organisation, réalisé en coopération avec les intéressés en vue de vérifier la conformité de cette situation aux dispositions préétablies, et l'adéquation de ces dernières à l'objectif recherché. [définition ISO, d'après la norme AFNOR Z61-102]

Audit d'agrément : Examen méthodique et indépendant en vue de déterminer si les activités et résultats relatifs à l'agrément satisfont aux dispositions préétablies, si ces dispositions sont mises en œuvre de façon efficace et si elles sont aptes à atteindre les objectifs.

Auditabilité : Garantir une maîtrise complète et permanente sur le système et en particulier pouvoir retracer tous les événements au cours d'une certaine période.

Audité : Il s'agit d'une personne physique ou d'un groupe de personnes ayant en charge le système soumis à audit. Il assure les deux fonctions suivantes : – responsable du système, – responsable de la sécurité du système. Il est l'interlocuteur privilégié de l'auditeur.

Auditeur : C'est l'intervenant (personne seule ou groupe d'individus) responsable de la mission d'audit.

Authenticité : Fait de ne pas permettre, par la voie de modifications autorisées, une perte du caractère complet et juste de l'information.

Authentification/identification : L'authentification a pour but de vérifier l'identité 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.

Autorité de certification (AC) : Tierce partie de confiance pour la génération, la signature et la publication des certificats de clés publiques.

Autorité fonctionnelle : Autorité responsable du point ou du réseau sensible et habilitée à traiter sur le plan territorial avec les pouvoirs publics, de tous les problèmes concernant la préparation et la mise en œuvre des mesures de sécurité.

Autorité de sécurité (AS) : Entité responsable de la définition, de l'implémentation et de la mise en œuvre d'une politique de sécurité.

Besoin de sécurité : Expression *a priori* des niveaux requis de disponibilité, d'intégrité et de confidentialité associés aux informations, fonctions ou sous-fonctions étudiées.

Besoins de sécurité : Définition précise et non-ambiguë des niveaux de confidentialité, d'intégrité et de disponibilité qu'il convient d'assurer à une information.

Biens sensibles : Éléments du système qu'il est indispensable de protéger pour satisfaire les objectifs de sécurité. Ils sont identifiés par une analyse propre à chaque système, qui prend en compte en particulier les conditions d'environnement et les menaces auxquelles celui-ci est soumis. Les résultats de cette analyse sont consignés dans le dossier de sécurité et doivent préciser si les biens sensibles font l'objet d'une classification. Dans le cas présent, les biens sensibles incluent au minimum les données d'enregistrement.

Bi-clé : Couple clé publique, clé privée (utilisées dans des algorithmes de cryptographie asymétriques).

Certificat : Déclaration formelle confirmant les résultats d'une évaluation, et le fait que les critères d'évaluation ont été correctement utilisés.

Chiffrement : Transformation cryptographique de données produisant un cryptogramme. [ISO 7498-2]

Chiffrement de bout en bout : Chiffrement de données à l'intérieur ou au niveau du système extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système extrémité de destination. [ISO 7498-2]

Chiffrement de liaison : Application particulière du chiffrement à chaque liaison du système. Le chiffrement de liaison implique que les données soient du texte en clair dans les entités relais. [ISO 7498-2]

Cible d'étude : Système d'information ou partie de celui-ci qui est soumis à l'étude de sécurité EBIOS.

Cible de sécurité : Spécification de la sécurité qui est exigée d'une cible d'évaluation et qui sert de base pour l'évaluation. La cible de sécurité doit spécifier les fonctions dédiées à la sécurité de la cible d'évaluation. Elle spécifiera aussi les objectifs de sécurité, les menaces qui pèsent sur ces objectifs ainsi que les mécanismes de sécurité particuliers qui seront employés. [ITSEC]

Cible d'évaluation : Système d'information ou produit qui est soumis à une évaluation de la sécurité. [ITSEC]

Clé de base : Clé utilisée pour chiffrer/déchiffrer les clés de trafic transmises sur le réseau ou mémorisées dans les moyens de cryptophonie.

Clé de chiffrement : Série de symboles commandant les opérations de chiffrement et de déchiffrement. [ISO 7498-2]

Clé de session : Clé dont la validité dure le temps d'une session.

Clé publique : Clé librement publiable et nécessaire à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour des opérations de chiffrement ou de vérification de signature. Ainsi, une clé publique est une clé mathématique qui peut être rendue publique et dont l'usage est de vérifier les signatures électroniques réalisées par la clé privée associée.

Clé publique : Un système à clé publique (ou asymétrique) utilise deux clés, une clé secrète et une clé publique ayant la propriété suivante : la clé publique étant dévoilée, il est impossible de retrouver par calcul la clé secrète.

Clé privée : Une clé privée est associée à une clé publique pour former une bi-clé. Elle est gardée secrète par son détenteur. Son usage est de signer électroniquement des données et de déchiffrer celles chiffrées par la clé publique associée.

Clé secrète : Clé volontairement non-publiée nécessaire à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour des opérations de chiffrement ou de déchiffrement.

Client : Entité demandant un service.

Client-Serveur : Communication mettant en relation un client et un serveur.

Client Sécurisé ou Serveur Sécurisé : Client ou serveur ayant besoin des services de sécurité.

Condensat : Chaîne de caractères produite par une fonction de hachage [ISO 10118-1].

Confidentialité : Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non-autorisés. [ISO 7498-2]

Confidentiel Défense : Cette mention est réservée aux informations qui ne présentent pas en elles-mêmes un caractère secret mais dont la connaissance, la réunion ou l'exploitation peuvent conduire à la divulgation d'un secret intéressant la Défense nationale et la sûreté de l'État. [article 5 du décret n° 81-514 du 12 mai 1981 relatif à l'organisation de la protection des secrets et des informations concernant la Défense Nationale et la sûreté de l'État].

Contexte de sécurité : Ensemble des éléments nécessaires pour assurer les services de sécurité.

Cryptogramme : Données obtenues par l'utilisation du chiffrement. Le contenu sémantique des données résultantes n'est pas compréhensible. [ISO 7498-2]

Cryptographie : Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur contenu ne passe inaperçu et/ou d'empêcher leur utilisation non-autorisée [ISO 7498-2]. Il existe deux types de cryptographie : la cryptographie symétrique dite à clé secrète et la cryptographie asymétrique dite à clé publique

Cryptopériode : Période de temps pendant laquelle les clés d'un système restent inchangées.

Déchiffrement : Opération inverse d'un chiffrement réversible. [ISO 7498-2]

Décryptement : Vise à rétablir, en utilisant les résultats de l'analyse cryptologique, le libellé clair des informations chiffrées, sans en posséder la clé.

Distribution : Délivrance par une autorité de distribution aux parties communicantes des clés à mettre en œuvre pour chiffrer ou déchiffrer des informations, y compris, le cas échéant, des éléments propres à d'autres abonnés.

Domaine : Ensemble des ressources et entités sur lesquelles s'applique une même politique de sécurité, cet ensemble étant administré par une autorité unique.

Donnée : Représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement.

Entité : Individu utilisateur, processus ou serveur sécurisé.

Entité sujet : Élément du modèle fonctionnel d'un service de sécurité qui désigne l'acteur ou le bénéficiaire principal de ce service (par exemple un individu vis-à-vis du service d'authentification ou de contrôle d'accès).

Entité objet : Élément du modèle fonctionnel d'un service de sécurité qui désigne la cible ou le bénéficiaire de ce service (par exemple une ressource ou une information vis-à-vis du service de contrôle d'accès).

Entité fonctionnelle : Élément du modèle fonctionnel d'un service de sécurité qui désigne une entité considérée du point de vue de son comportement, indépendamment de sa réalité physique ou technique.

Évaluation : Estimation de la sécurité d'un produit ou d'un système par rapport à des critères d'évaluation définis.

Fonction de hachage : Fonction qui transforme une chaîne de caractères en une chaîne de caractères de taille inférieure et fixe. Cette fonction satisfait deux propriétés : il est difficile pour une image de la fonction de calculer l'antécédent associé ; il est difficile pour un antécédent de la fonction de calculer un antécédent différent ayant la même image.

Fonction de sécurité : Mesure technique, susceptible de satisfaire un objectif de sécurité.

Fonction de service : Action attendue d'un produit (ou réalisée par lui) pour répondre à un élément du besoin d'un utilisateur donné (source NF X 50-150). Le terme utilisateur désigne ici des personnes ou des entités fonctionnelles du système.

Homologation : Autorisation d'utiliser, dans un but précis ou dans des conditions prévues, un produit ou un système (en anglais : *accreditation*). C'est l'autorité responsable de la mise en œuvre du produit ou du système qui délivre cette autorisation, conformément à la réglementation en vigueur.

Infrastructure à clés publiques (ICP) : Également appelée PKI (Public Key Infrastructure) en anglais. Ensemble de moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques.

Identification : Procédé permettant de reconnaître un utilisateur de manière sûre par la récupération de données qui lui sont propres.

Information : Élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué. Renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.

Intégrité : Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire à la garantie de son origine et de sa destination. [ISO 7498-2]

Mécanisme de sécurité : Logique ou algorithme qui implémente par matériel ou logiciel une fonction particulière dédiée à la sécurité ou contribuant à la sécurité. [ITSEC]

Politique de sécurité : Ensemble des critères permettant de fournir des services de sécurité. [ISO 7498-2]

Politique de sécurité technique : Ensemble des lois, règles et pratiques qui régissent le traitement des informations sensibles et l'utilisation des ressources par le matériel et le logiciel d'un système d'information ou d'un produit. [ITSEC]

Répudiation : Fait de nier avoir participé à des échanges, totalement ou en partie.

Révocation : Annonce qu'une clé privée a perdu son intégrité. Le certificat de la clé publique correspondante ne doit plus être utilisé.

Service : Regroupement cohérent de fonctions de service visant à répondre à un élément du besoin d'un utilisateur ou d'entités fonctionnelles du système. Sauf précision contraire, dans le présent document, le terme service désigne un regroupement de fonctions de sécurité ou de fonctions assurant le support de celles-ci.

Session : Une session représente l'intervalle de temps entre le début d'un échange ou d'une communication et sa fin.

Système d'information : Tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.

Système informatique : Ensemble formé par un ordinateur et les différents éléments qui lui sont rattachés. Ceci concerne les matériels et les logiciels.

Organismes

ADAE : Agence pour le développement de l'administration électronique.

BRCI : Brigade centrale de la répression de la criminalité informatique.

CCSDN : Commission consultative du secret de la Défense nationale.

CEMA : Chef d'État-Major des Armées.

CEMAA : Chef d'État-Major de l'armée de l'air.

CEMAT : Chef d'État-Major de l'armée de terre.

CMM : Chef d'État-Major de la marine.

CERT-RENATER : centre d'alerte et de réponse aux attaques informatiques dédié aux membres de la communauté GIP-RENATER – Réseau national de télécommunication pour la Technologie, l'Enseignement et la Recherche.

CERTA : Centre d'expertise gouvernemental de réponse et de traitement des attaques informatisées – relié au DCSSI.

CESTI : Centres d'évaluation de la sécurité des technologies de l'information reconnus par la DCSSI.

CFSSI : Centre de formation à la sécurité des systèmes d'information.

CIGREF : Club informatique des grandes entreprises françaises.

CIRT-IST : CERT privé réalisé par Alcatel, le CNES, Total et France Télécom.

CISI : Comité interministériel pour la société de l'information.

CISSI : Commission interministérielle pour la sécurité des systèmes d'information.

CLUSIF : Club de la sécurité informatique des systèmes d'information français.

CNIL : Commission nationale informatique et libertés.

CNIS : Commission nationale de contrôle des interceptions de sécurité.

COSSI : Centre opérationnel de la sécurité des systèmes d'information.

DCSSI : Direction centrale de la sécurité des systèmes d'information.

DGA : Délégation générale pour l'armement.

DGGN : Direction générale de la gendarmerie nationale.

DGSE : Direction générale de la sécurité extérieure.

DPSD : Direction de la protection et de la sécurité de la défense.

DST : Direction de la surveillance du territoire.

DSTI : Direction des systèmes terrestres et d'information.

INHES : Institut national des hautes études de sécurité (ex IHESI).

INPS : Institut national de police scientifique.

OCLCTIC : Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

OPVAR : Organisation permanente de veille alerte réponse.

OSSIR : Observatoire de la sécurité des systèmes d'information & des réseaux.

PAGSI : Programme d'action gouvernemental pour l'entrée de la France dans la société de l'information.

RECIF : Recherches et études sur la criminalité informatique française.

STSI : Service des technologies et de la société de l'information (Minefi/DGE).

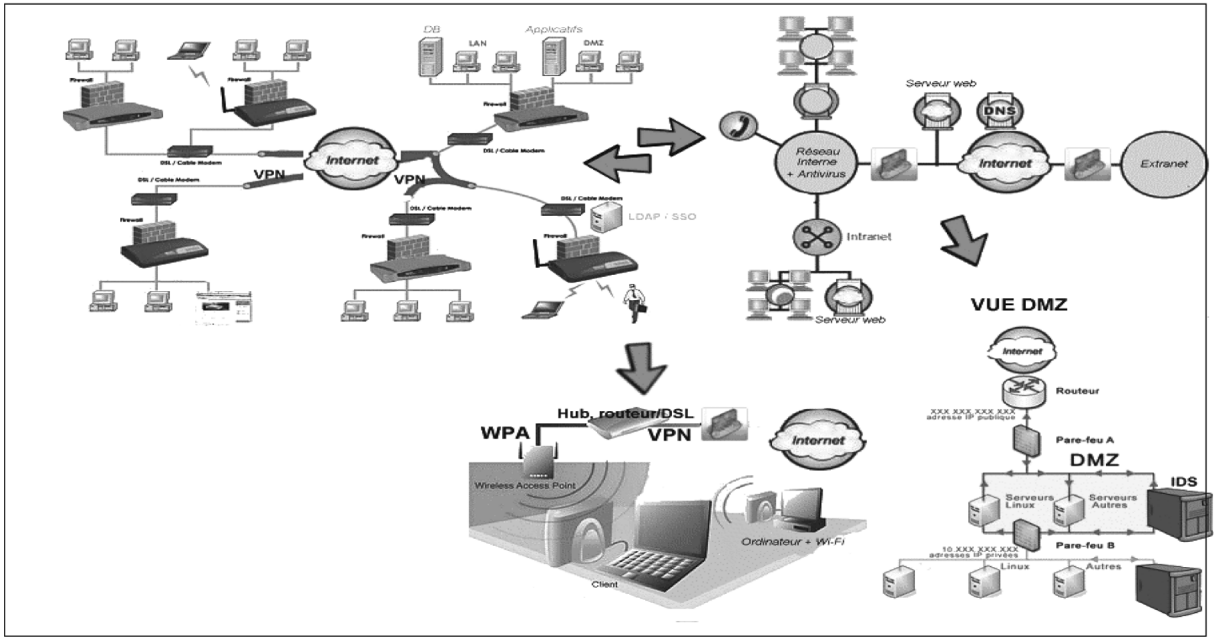
SEFTI : Service d'enquête des fraudes aux technologies de l'information.

SGA : Secrétariat général pour l'administration.

SGDN : Secrétariat général de la Défense nationale.

Annexe IV

Schéma de principe des systèmes d'information



Considérations techniques non exhaustives

Le WEP et le WPA sont deux des méthodes de cryptage du trafic sans fil entre clients et point d'accès sans fil.

Un VPN est un « tunnel » de communication chiffré entre deux points.

DMZ ou zone démilitarisé est un espace intermédiaire sécurisé entre le réseau extérieur et intérieur.

Serveur LDAP : annuaire d'entreprise sécurisé permettant de gérer les autorisations d'accès

SSO : permet à un utilisateur d'accéder à des services en ne devant s'identifier qu'une seule et unique fois via LDAP

IDS : système combinant logiciel et matériel, qui permet de détecter en temps réel les tentatives d'intrusion sur un réseau interne

LAN : réseau interne d'une entreprise

Extranet : réseau informatique étendu à la communication avec des filiales ou partenaires

Intranet : réseau strictement local et privé qui utilise les technologies de l'Internet : web, e-mail, non ouvert aux connexions publiques

Serveur : ordinateur gérant l'accès aux ressources et aux périphériques et les connexions des différents utilisateurs :
– un serveur de fichiers prépare la place mémoire pour des fichiers ;
– un serveur d'impression gère et exécute les sorties sur imprimantes du réseau
– un serveur d'apllications rend disponible sur son disque dur des programmes « partagés ».

DNS : permet d'effectuer la corrélation ebntre les adresses IP (82.64.52.31) et le nom de domaine associé (xxx.gouv.fr)

Sensibilité de l'information : exemples de la DCSSI et de l'AFNOR

Classifier l'information

La recommandation N° 901 de la DCSSI s'attache quant à elle à distinguer 2 niveaux d'informations pour tout ce qui concerne les informations non-classifiées défense :

- *Les informations sensibles, qui englobent tous les documents dont la consultation ou la communication mettrait en cause la responsabilité pénale du propriétaire ou du dépositaire, ou causerait un préjudice à eux-mêmes ou à des tiers matérialisés par :*
  – les informations énumérées à l'article 6 de la loi n° 78-753 du 17 juillet 1978, modifiée par la loi 2000-321 du 12 avril 2000 ;
  – les informations qui ne présentent pas un caractère de secret, mais qui restent soumises à l'obligation de réserve ou de discrétion professionnelle ;
  – les informations constitutives du patrimoine scientifique, industriel et technologique ;
- *Les informations vitales pour le fonctionnement d'un système.*

Le traitement des données par un système nécessite la mise en œuvre d'une suite d'actions élémentaires internes dont l'association assure les fonctionnalités du système d'information. Ainsi, un site Internet est un ensemble de documents (fichiers. php, fichiers. sql qui sont interprétés par le serveur ou le navigateur et permettent d'afficher une page Web). L'accès à certains de ces documents mal protégés (droits étendus sur un fichier config. php par exemple) permet d'obtenir rapidement un contrôle total sur un site internet.

La classification des informations selon l'AFNOR

Les informations sont le plus souvent consignées dans des documents papier ou numérisés. Toutefois, des objets (maquettes, prototypes, machines...), des installations, des procédés, des techniques, des méthodes commerciales, des organisations, des projets de publicité, le

savoir-faire de l'entreprise, etc., sont d'autant d'indications qui constituent des informations.

Aussi, une démarche de protection de l'information commencera par l'identification des informations, quelles que soient leur forme, dont la confidentialité doit être protégée, en raison :
– des avantages que leur divulgation procurerait à la concurrence ou aux partenaires ;
– des exigences légales et réglementaires encadrant ces informations.

C'est aussi l'analyse de risques qui permet de déterminer le nombre de niveaux de protection nécessaire à chaque structure.

Exemple de système de classification des informations :

Niveau	3 : secret	2 : confidentiel	1 : diffusion contrôlée
Préjudice potentiel	Préjudice inacceptable Séquelles très graves et durables	Préjudice grave Séquelles compromettant l'action à court et moyen terme	Préjudice faible Perturbations ponctuelles
Risques tolérés	Aucun risque même résiduel n'est acceptable	Des risques très limités peuvent être pris	Des risques sont pris en connaissance de cause
Protection	Recherche d'une protection maximale	Prise en compte de la notion de probabilité d'occurrence	La fréquence et le coût du préjudice potentiel déterminent les mesures prises

Recommandations

Une attente particulière est apportée aux possibilités de compilation ou de croisement des données. En effet, la consolidation de données, *a priori* peu sensibles lorsqu'elles sont prises séparément, peut constituer une information confidentielle.

Afin d'assurer un niveau de protection homogène et juste nécessaire – ni trop, ni pas assez – il est recommandé de désigner explicitement les personnes responsables de la classification des informations [1], de leur fournir un *vade-mecum* pour les aider dans cette mission et d'actualiser régulièrement ce document.

1. L'attribution de cette responsabilité variera suivant la taille de l'entreprise, son organisation, l'origine, la forme ou la finalité des informations, etc. Par exemple, dans des structures de taille importante, un responsable dans chaque secteur d'activité peut être en charge de la classification et de l'application des mesures de protection, dans d'autres, chaque personne à l'origine d'une information est responsable de sa protection.

Annexe VI

Profils détaillés des attaquants de systèmes d'information

Les scripts kiddies

Script kiddie est un terme familier désignant les pirates informatiques néophytes qui, dépourvus des principales compétences en matière de gestion de la sécurité informatique, passent l'essentiel de leur temps à essayer d'infiltrer des systèmes, en utilisant des scripts ou autres programmes mis au point par d'autres.

Malgré leur niveau de qualifications faible, les *script kiddies* sont parfois une menace réelle pour la sécurité des systèmes. En effet, outre le fait qu'ils peuvent, par incompétence, altérer quelque chose sans le vouloir ou le savoir, d'une part les *script kiddies* sont très nombreux et, d'autre part, ils sont souvent obstinés au point de passer parfois plusieurs jours à essayer toutes les combinaisons possibles d'un mot de passe, avec le risque d'y parvenir.

Les hacktivistes

L'*hacktivisme* est une contraction de *hacker* et activisme. Ici l'on retrouve deux concepts rassemblés. Le *hacktiviste* infiltre les réseaux en mettant son talent au service de ses convictions politiques, éthiques ou religieuses et pratique des piratages, détournements de serveurs, remplacement de pages d'accueil par des tracts, spamming...

Chacune de ces catégories peut répondre à une ou plusieurs motivations comme par exemple la création d'un cheval de Troie commandité par une entreprise qui correspond à une motivation stratégique (accès frauduleux aux informations) et une menace cupide (gagner des parts de marché).

Si l'outil est mis en libre disposition sur Internet il pourra par la suite répondre également à une menace ludique ou une menace terroriste.

Les hackers

Le jargon informatique définit différentes catégories de *hackers* en fonction de leur champ d'implication (légal ou illégal) ou de leur impact sur les réseaux informatiques :

– les chapeaux blancs – ou *white hats* : consultants en sécurité, administrateurs réseaux ou cyber-policiers ; ils ont un sens de l'éthique et de la déontologie ;
– les chapeaux gris – ou *grey hats* : s'ils n'hésitent pas à pénétrer dans les systèmes sans y être autorisés, ils n'ont pas pour but de nuire. C'est souvent l'exploit informatique qui les motive, une façon de faire la preuve de leur habileté ;
– les chapeaux noirs – ou *black hats* : créateurs de virus, cyber-espions, cyber-terroristes et cyber-escrocs, sont, eux, dangereux et n'ont aucun sens de l'éthique. Ils correspondent alors à la définition du pirate telle que conçue par les journaux.

Ces catégories peuvent elles-mêmes être divisées en sous-catégories en fonction de leur spécialité :
– le *cracker* s'occupe de casser la protection des logiciels ;
– le *carder* s'occupe de casser les systèmes de protections des cartes à puces comme les cartes bancaires, mais aussi les cartes de décodeur de chaîne payante ;
– le *phreaker* s'occupe de casser les protections des systèmes téléphoniques.

On peut enfin, dans cette typologie, tenir compte d'un phénomène d'interpénétration : ainsi, le *pirate* au début joueur, acquiert un savoir-faire en matière d'attaque de systèmes d'information, dont il peut ensuite chercher à tirer un profit financier (menace cupide). Déçu par la société, il peut ensuite accepter des propositions de recruteurs de réseaux terroristes ou d'agents de renseignement (menace ludique devenant terroriste ou stratégique).

Exemples de menaces

Menaces électroniques

La menace Tempest

L'adversaire peut chercher à tirer parti des signaux compromettants qu'émet tout système électronique. Il faut savoir que ce rayonnement peut être perceptible jusqu'à plus d'une centaine de mètres. De plus, par conduction, soit sur les conducteurs d'alimentation de l'appareil cible, soit sur des conducteurs passant à proximité, des tensions électriques révélatrices peuvent aussi révéler des informations intéressantes.

*L'analyse des signaux parasites compromettants classiques s'est enrichie, en 2004, d'une nouvelle technique de cryptanalyse acoustique des cœurs d'unités centrales (*Core Process Units*).*

Cette menace Tempest, bien connue des services de renseignement et de protection, l'est moins du grand public. La parer est difficile et coûteux : on peut, bien sûr, mettre tous les équipements sensibles dans des cages de Faraday..., ou acquérir des matériels conçus et réalisés pour émettre un minimum de signaux compromettants, généralement vendus à prix d'or...

L'exemple des puces RFID (Radio-Frequency Identification)

Les étiquettes d'identification radio (ou RFID) sont des puces sans contact transmettant des données à distance par moyens radioélectriques. On les appelle aussi étiquettes intelligentes, ou encore parfois étiquettes-transpondeurs. C'est, par exemple, ce type de puces qui est utilisé dans le système Navigo dans les transports en Île-de-France ou pour le marquage des animaux. Les utilisations potentielles de ce genre de technologie sont nombreuses : gestion de stocks, grands magasins, télépéages d'autoroutes, jusqu'aux nouveaux passeports...

Avec des moyens de détection un peu sophistiqués, la distance d'accès effective aux étiquettes RFID peut atteindre plusieurs dizaines, voire centaines de mètres. La plupart des dispositifs ne chiffrant pas (ou mal) les données transmises, les informations peuvent donc être interceptées à cette distance.

Considérant, par exemple, l'intérêt que pourrait trouver un concurrent à lire à distance l'ensemble du flux logistique de distribution d'un industriel, et dans la mesure où ce type de technologie est envisagé pour transmettre des données personnelles (sur des passeports par exemple) l'emploi de la technologie RFID pour des données à caractère personnel ou dans des systèmes de haute sécurité nécessite une analyse poussée des risques.

Menaces logicielles

Les chevaux de Troie

Des chevaux de Troie discrets

Un rootkit *est un outil qui fournit des services destinés à masquer la présence d'un intrus sur un système (dissimulation de processus, de fichiers par exemple) et certains outils d'aide à l'administration ont fait leur apparition dans des* rootkits*. Ces outils touchent donc à des tâches critiques, à proximité du noyau des systèmes d'exploitation.*

L'utilisation de rootkits, combinée avec des codes malveillants (virus, chevaux de Troie...) s'appuyant sur des failles de sécurité pour s'introduire dans une machine, devient une solution idéale pour les attaques informatiques en permettant l'accès à des commandes bas niveau.

Mais cette menace est d'autant plus sérieuse qu'elle se situe au niveau du système d'exploitation, soit avant la couche de sécurité traditionnelle offerte par les antivirus. Ainsi, un pirate peut-il empêcher le lancement d'un logiciel antivirus, ou au contraire forcer l'exécution d'un programme préalablement installé sur le disque dur. C'est ainsi qu'une machine infectée peut être, ***à l'insu de son utilisateur légitime****, entièrement corrompue : on parle alors de zombie. De fait, elle devient une plate-forme privilégiée pour le pirate pour lancer, relayer ou contribuer à une large variété d'attaques.*

*C'est en 2003 que sont apparus les premiers chevaux de Troie opérant en mode noyau en environnement Windows (*Slanret, IERK, Backdoor Ali...*).*

En 2005, les attaques combinées, associant diverses techniques malveillantes, sont devenues un sujet majeur de préoccupation en matière de sécurité informatique. Microsoft lui-même, en mars 2005 lors de la conférence RSA, s'en est inquiété, compte tenu de la multiplication d'attaques à base de rootkits *Windows.*

Les vers

Utilisant une technique d'ingénierie sociale (tromper les internautes par un message d'amour), le ver *I love you* subtilisait les codes d'accès, et, une fois installé, lançait des attaques par déni de services sur des serveurs Web distants.
En 2001, les vers se sont multipliés. Code Rouge (*Red Code*), à la différence de ces prédécesseurs, s'appuyait, pour se déplacer, sur une faille dans les serveurs IIS (*Internet Information Server*) de Microsoft. Il engendrait une modification de la page d'accueil des sites tournant sous plate-forme Windows.

Des menaces de plus en plus polymorphes

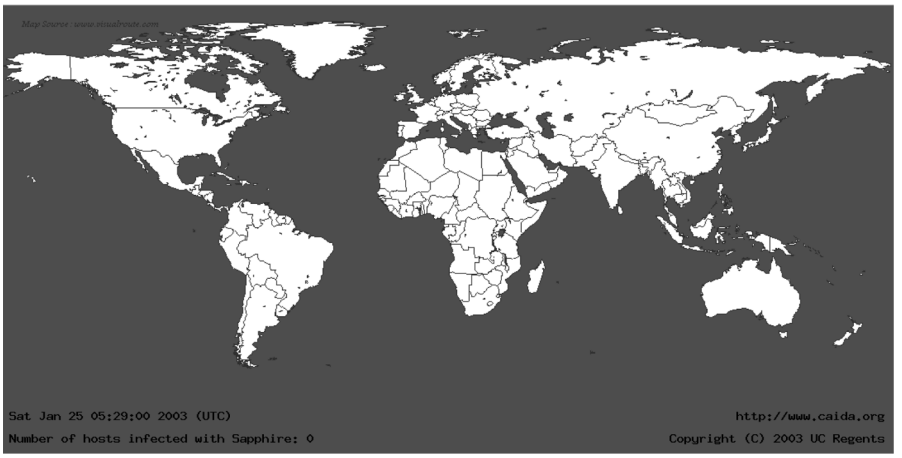
Pour mieux déjouer les tentatives de blocage et les contre-mesures, les menaces sont désormais conçues polymorphes. Ce sont des blended threats*, c'est-à-dire capables de se transformer d'un type à l'autre, en utilisant différents modes de transport et en exploitant plusieurs vulnérabilités à la fois. Ce fut par exemple le cas du ver* Nimda*, qui se propagea via le protocole HTTP (pages Web) en exploitant une faille sur les serveurs IIS, via la messagerie SMTP et aussi via le système de partage de fichiers de Microsoft.*

En 2002, c'est au tour de *Slammer* et *Blaster* de faire leur apparition. Des dizaines de milliers de serveurs ont été touchés en 10 minutes. Quant à *Blaster*, il utilisait comme moyen de transport, le module DCOM RPC d'appel à distance de Windows (2000 et XP). Les attaques passaient notamment par le dispositif de mise à jour à distance de Microsoft (Windows Update).

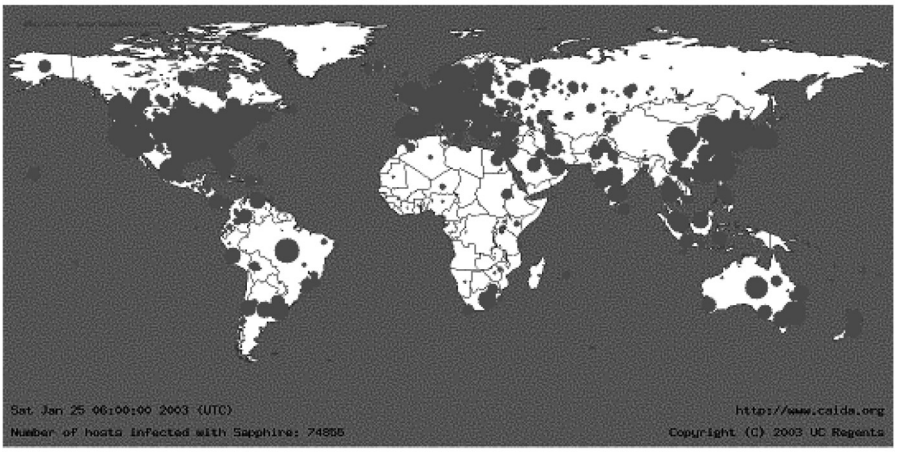
L'exemple du ver *Sapphire* [1] montre également l'augmentation croissante de la vitesse de propagation de ce type de ver corrélative au développement des systèmes d'information dans le monde entre 2001 et 2003.

1. Source : **www.caida.org**

25 janvier 2003-05 : 29 -0 victime



25 janvier 2003-06 : 00 -74 855 victimes



Virus

Selon Sophos et Clusif, les meilleurs scores de propagation des virus ont été les suivants en 2004 :

Clt	Nom	Type	Type d'attaque
1	Netsky-P	Mass Mailer	
2	Zafi-B	Mass Mailer	Désactive certaines sécurités
4	Netsky-B	Mass Mailer	
4	Netsky-D	Mass Mailer	
5	Netsky-Z	Mass Mailer	
6	MyDoom	Mass Mailer	Déni de service + Ouvre un accès distant

Les antivirus

La quasi-totalité des éditeurs d'antivirus mettent à disposition de leurs clients de nouvelles définitions virales dans les heures qui suivent l'identification d'un virus. Autrement dit, ils proposent les fichiers de mise à jour grâce auxquels le logiciel pourra résister à une attaque et, le cas échéant, traiter un ordinateur infecté. Certains éditeurs proposent désormais en outre un scan à distance de votre disque dur, et parfois même sa désinfection.

La mise à jour d'un antivirus se fait de façon transparente par téléchargement des définitions virales, du moins dans les mois qui suivent son achat. Mais par la suite, ou si par exemple l'utilisateur ne se connecte à l'Internet que rarement, il lui faudra procéder manuellement au téléchargement des mises à jour en allant sur le site de l'éditeur. Il existe aussi des patchs gratuitement téléchargeables.

Les éditeurs d'antivirus ne sont pas à l'abri de la découverte de failles de sécurité dans leurs produits. Ils le sont même plutôt moins que d'autres, puisque les antivirus doivent analyser les pièces jointes, passer en revue une très grande variété de fichiers, et possèdent donc plus de risques potentiels d'avoir des failles que d'autres types de logiciels. Il existe principalement 2 sortes de vulnérabilité : l'attaque par déni de service (DoS), pouvant saturer l'espace disque de l'antivirus et l'empêcher de fonctionner, et celle du débordement de mémoire tampon, ou buffer overflow*, qui permet d'exécuter des commandes arbitraires.*

De façon générale, quand ils ont été touchés, les principaux acteurs du marché de la sécurité ont pris le parti de la transparence, c'est-à-dire d'informer systématiquement leurs clients quand une faille est découverte. Il faut alors la patcher et le client doit mettre à jour son antivirus. Si le patch n'est pas immédiatement disponible, il faut éditer des règles pour limiter les effets d'éventuelles attaques. C'est là la situation aujourd'hui ; mais l'évolution du marché (avec l'intrusion de géants comme Microsoft) et l'évolution du risque d'attaques Zero Day *pourraient les amener à changer d'état d'esprit.*

Les dénis de service

Encore et toujours plus d'attaques DNS

L'actualité de la sécurité informatique en 2005 aura été notamment marquée par la réapparition des attaques sur les serveurs de noms de domaines (ou DNS).

Alors que la majorité des attaques de fraude en ligne actuelles nécessite une action de la part de l'utilisateur, l'avantage d'une attaque des serveurs de noms de domaines pour le pirate est de supprimer toute nécessité d'interaction avec l'utilisateur. Le pirate

s'assure que tous les utilisateurs souhaitant accéder à un serveur donné (qui peut être un serveur de messagerie, un serveur Web...) sont automatiquement redirigés vers une adresse IP préalablement choisie. Il peut aussi choisir de ne le faire que pour une partie seulement du trafic, ce qui rend la détection plus difficile.

Ce détournement des flux permet, par analyse des courriels ou grâce à un site contrefait, de recueillir des informations confidentielles, ou encore, quand plusieurs serveurs DNS ont été attaqués, de monter une attaque en déni de services distribué (DDoS) en surchargeant de requêtes la cible.

Les réseaux de robots

*Les robots (*bots*)*

Les bots *font partie de la nouvelle vague des menaces de sécurité, silencieuse et à propagation rapide. Les bots, nom dérivé de robots, désignent une catégorie de programmes malveillants s'installant sans l'accord de l'internaute se connectant à un serveur de « commande et contrôle ».*

*Les menaces ne sont plus désormais physiques et perceptibles à court terme, mais elles donnent accès aux pirates à de nouvelles ressources informatiques pour, le moment venu, relayer à partir des machines infectées du spam, ou d'autres virus, ou des attaques en déni de service, pour se livrer à de l'écoute réseau ou de l'écoute clavier (*keylogging*).*

Le but est de faire de l'argent, en louant des réseaux de bots pour relayer du spam par exemple. Pour rentabiliser son programme, l'auteur doit donc s'arranger pour limiter au maximum la visibilité externe de son bot. En outre, les machines infectées peuvent contenir aussi des données personnelles, qui peuvent intéresser, donc se vendre.

*Fragiles, car rapidement détruits par les antivirus du marché, ces réseaux de bots ne survivent qu'en contaminant sans cesse de nouvelles victimes. Aujourd'hui, la forme la plus simple et la plus exploitée pour mettre les machines en réseau passe par les canaux IRC (*Internet Relay Chat*). L'avantage d'un tel mode d'accès est que les serveurs IRC sont librement disponibles et aisément configurables.*

Pour s'installer et se répandre, les bots utilisent le plus souvent des vulnérabilités qui touchent les serveurs Web (IIS et Apache), les procédures d'appel à distance de Windows (RPC), le serveur SQL Microsoft, MySQL, WINS et les portes dérobées laissées préalablement ouvertes par certains virus.

Dans la mesure où, une fois réunis, ces réseaux de PC zombies ne peuvent presque plus être arrêtés, il est important de prévenir la contamination.

Pour faciliter leur éradication, les spécialistes de la sécurité multiplient les analyses de ces réseaux. Souvent, il leur suffit de sniffer le trafic des serveurs IRC pour remonter la piste. Mais, pour certains d'entre eux, placés dans des pays juridiquement difficiles d'accès, ce n'est pas toujours possible.

La méthode alors utilisée par les professionnels de la sécurité se calque sur celles de détection des virus : elle consiste à s'infiltrer dans ces réseaux, en plaçant des machines cibles appelées pots de miel *(*honeypots*). Elle consiste à placer un réseau de machines volontairement vulnérables sur Internet et à se laisser infecter pour mettre la main sur l'exécutable du drone.*

Annexe VIII

Exemples de vulnérabilités

Vulnérabilités organisationnelles

Comment bâtir un plan de continuité de l'activité ?

Le processus d'élaboration de ce plan est le suivant : après avoir défini, sans se préoccuper des moyens associés et du système d'information, les activités qu'elle considère comme essentielles, une entreprise identifiera toutes les composantes qui y contribuent : ressources humaines, produits, ressources informatiques, etc. Puis, elle définira des modes opératoires permettant de contourner la difficulté rencontrée.

C'est sur la base des modes opératoires et des moyens nécessaires pour la continuité des opérations métier que l'on va « construire », progressivement, pas à pas, un « plan de continuité des opérations ».

On reviendra ensuite sur les différents cas de figure, pour identifier les fonctions support qui y contribuent, au premier rang desquelles il y a, bien entendu, le « système d'information » de l'entreprise. Ce terme doit ici être pris dans son acception la plus large, il ne faut surtout pas le limiter au système informatique. (Ainsi, on pourrait imaginer une situation de crise où un « brouillage » temporaire du système de contrôle d'accès, supposé non-relié et distinct du système informatique central, (par exemple, capteurs et dispositifs de lecture badigeonnés avec de la peinture métallique) empêcherait l'accès du personnel à l'usine. Cela bien entendu désorganiserait la production, mais ne peut être considéré ni comme un incident, ni comme une agression informatique).

On s'intéressera aux conditions minimales de fonctionnement des différentes ressources informatiques impactées (là aussi, bien des surprises nous attendent...). Puis, on tentera d'imaginer un mode opératoire, et les moyens de la continuité du système d'information.

On construit ainsi, pas à pas, un « plan de continuité informatique ».

C'est l'ensemble de ces deux plans (plan de continuité des opérations et son alter ego *technique, le plan de continuité informatique), qui constitue le plan de continuité de l'activité.*

Vulnérabilités techniques

Celles qui sont publiées peuvent l'être de manière officielle et donner alors lieu à des alertes, via des CERT (*Computer Emergency Response Team*) ou des CSIRT (*Computer Security Incident Response Team*), qui les caractérisent et les valident à travers 3 ou 4 niveaux de gravité (« critique », « élevée », « moyenne » et « faible »). Elles peuvent aussi l'être de manière non-officielle, au sein de communautés de *hackers*.

À partir du moment où une vulnérabilité est publiée, le facteur temps joue de façon cruciale pour éviter des exploitations malveillantes.

Publier ou non les vulnérabilités ?

La publication ou non des vulnérabilités logicielles a constitué de tout temps un sujet difficile. L'enjeu, pour les chercheurs indépendants, consiste à voir leur travail reconnu ainsi qu'à sensibiliser clients et éditeurs sur les risques des différents produits. Au contraire, les éditeurs cherchent avant tout à protéger leurs produits et leurs clients d'une attaque éventuelle qui pourrait être la conséquence fâcheuse d'une publication hâtive, ou non-maîtrisée, d'une vulnérabilité.

Dans ce jeu, les grands éditeurs de logiciels craignent les failles découvertes mais non-divulguées, dont peuvent tirer parti les créateurs de vers ou de virus bien informés. Tout éditeur doit donc s'arranger pour être, en priorité et avant tout autre, mis au courant de toute faille dans ses produits.

Ce sujet a pris, lors de la conférence Black Hat 2005 qui s'est tenue à Las Vegas du 23 au 28 juillet 2005, une tournure intéressante. Michael Lynn, chercheur en sécurité chez Internet Security System (ISS), avait prévu de dévoiler, à l'occasion du discours officiel planifié pour la conférence par ISS, les grandes lignes d'une faille majeure affectant les routeurs Cisco. Compte tenu de l'interdiction de son employeur de s'exprimer, il a alors démissionné pour pouvoir communiquer librement sur cette vulnérabilité en public. Après une double procédure en justice engagée d'une part, par Cisco pour violation des droits d'auteurs sur le logiciel Cisco, d'autre part, par ISS pour non-respect du secret professionnel, l'affaire s'est finalement résolue à l'amiable. Le chercheur a accepté de remettre l'ensemble des documents relatifs à la faille à Cisco, mais aussi de ne plus en parler.

Jusqu'à présent, les éditeurs comptaient avant tout sur la bonne volonté des chercheurs indépendants pour leur transmettre leurs découvertes. Mais, de plus en plus, ils mettent en œuvre une stratégie à deux volets : d'une part, ils cherchent à racheter des sociétés spécialisées dans la recherche de vulnérabilités, d'autre part, ils proposent aux chercheurs indépendants des primes, de manière à les inciter à leur communiquer leurs travaux au plus tôt.

Ainsi, la société 3Com a-t-elle racheté l'acteur TippingPoint, spécialisé dans la recherche de vulnérabilités logicielles, pour 430 millions de dollars, et vient-elle d'annoncer son projet Zero Day Initiative *: selon le niveau de dangerosité de la vulnérabilité découverte, 3Com offrira jusqu'à 20 000 dollars de prime aux chercheurs indépendants. Même modèle économique pour VeriSign, qui vient de racheter mi-2005 pour 40 millions de dollars iDefense, autre acteur connu dans le milieu, qui proposait en moyenne 2 000 dollars par faille découverte aux acteurs indépendants. Même schéma enfin pour la fondation Mozilla, responsable du navigateur Web Firefox, pour lui permettre d'être informée en priorité sur les bugs affectant ses logiciels, mais cette fois pour 500 dollars seulement (l'ordre de grandeur n'est pas le même, on est dans le monde des logiciels libres).*

Cette stratégie d'enchères a le double avantage d'épauler le manque de compétences internes et de stimuler, en théorie au moins, la recherche de failles sur un produit donné. Mais la contrepartie est qu'elle risque d'engendrer une « inflation des cours », qui, une fois encore, devrait plutôt profiter aux riches.

Annexe IX

Les principaux textes relatifs à l'organisation institutionnelle

Au niveau interministériel, le décret 96-67 fixe les compétences du secrétariat général de la défense nationale (SGDN) en matière de SSI. Le SGDN dispose, pour conduire ses missions, de la direction centrale de la sécurité des systèmes d'information (DCSSI) créée par le décret 2001-693. Une commission interministérielle de la SSI (CISSI) créée par le décret 2001-694 a pour mission d'assurer la concertation avec les départements ministériels sur les questions de SSI. Au niveau ministériel, la responsabilité de l'application de la politique en SSI incombe au haut fonctionnaire de défense (HFD) dont les missions sont précisées par le décret 80-243. Une directive du Premier ministre (4201/SG) vient préciser cette organisation en définissant les responsabilités particulières de chaque ministère en SSI.

Au niveau de l'Union européenne (UE), l'agence de sécurité des réseaux et de l'information (ENISA) créée par le règlement 460/2004 du Parlement européen et du Conseil n'a pas, de par ses missions et son statut, vocation à être une agence européenne de régulation de la SSI. En revanche, elle pourra proposer à la Commission européenne des initiatives dans ce domaine conduisant à des directives européennes applicables aux États membres.

Les principaux textes relatifs à la protection des systèmes d'information

Dans le domaine de la réglementation SSI, une distinction majeure est faite entre les informations classifiées de défense et les autres informations sensibles mais non-classifiées.

La protection des informations classifiées de défense définies par l'article 413-9 du code pénal est l'objet d'une instruction générale interministérielle (arrêté du 25 août 2003) qui contient notamment un volet sur les mesures spécifiques en SSI (articles 45 à 48). De nombreux textes viennent compléter et détailler ces mesures SSI sous la forme de directives, instructions, recommandations, ou autres guides techniques. De façon générale, la responsabilité de l'application de ces mesures incombe à chaque ministère pour ses systèmes d'information (décret 98-608). En cas de non-respect de ces mesures qui conduirait à une compromission d'information, il s'expose aux peines prévues à l'article 413 du code pénal.

Dans le domaine du « classifié », il convient de rappeler que la réglementation du Conseil de l'UE (décision du Conseil 2001/264/CE) en matière de protection des informations classifiées de l'UE s'applique aux États membres lorsqu'ils traitent ces informations dans leurs systèmes d'information. Il en va de même avec la réglementation de l'OTAN (politique de sécurité CM (2002) 49) pour les informations classifiées de l'OTAN confiées aux États Membres.

Les informations sensibles non-classifiées ne sont pas définies en tant que telles par une loi. En revanche, de nombreuses lois définissent des catégories d'information qui doivent être protégées car relevant de différents secrets. À titre d'exemple, citons le secret professionnel (article 226-13 du code pénal), le secret des correspondances (article 226-15 du code pénal), les intérêts fondamentaux de la nation (articles 410 et 411 du code pénal), le secret de la vie privée (loi 78-17, article 226-16 à 226-24 du code pénal), etc. Les informations sensibles ne constituent pas un ensemble homogène et ne bénéficient pas d'un corpus réglementaire fixant des mesures de sécurité pour ces informations comme il en existe dans le domaine des informations classifiées de défense. En revanche, les sanctions prévues par la loi sont ici encore susceptibles de s'appliquer en cas de compromission d'information résultant de la mauvaise application de mesures de sécurité.

La loi d'habilitation 2004-1343 de simplification du droit

L'article 3 de cette loi est consacré au développement de l'administration électronique et, en particulier, prévoit que des mesures seront prises par ordonnance pour assurer la sécurité des échanges électroniques entre usagers et administrations. Cette ordonnance, encore en discussion, permettra de fixer les exigences de sécurité applicables aux produits et prestations mis en œuvre pour sécuriser ces échanges. Elle introduira notamment une procédure de qualification de ces produits et prestataires de sécurité reposant sur une procédure existante définie par le décret 2002-535. Elle mettra en place, avec ces textes d'application, un cadre commun de mesures de sécurité dans ce domaine des informations sensibles des usagers qui sont traitées par l'administration.

Les textes relatifs à la cryptologie

Dans le domaine particulier de la cryptologie, une des composantes de la SSI, il existe une réglementation visant à contrôler l'utilisation, la fourniture, l'exportation des produits ou des prestations de cryptologie. Cette technologie est contrôlée car considérée comme sensible à certains égards. La réglementation française en ce domaine transpose notamment le règlement européen 1334/2000 sur le contrôle des biens et technologies à double usage. Le texte législatif de base est la loi 2004-575 (titre III) pour la confiance dans l'économie numérique qui instaure un régime de déclaration ou d'autorisation selon les cas pour les moyens et prestations de cryptologie. Les décrets d'application n'étant pas encore pris, certaines dispositions de l'ancienne législation (loi 90-1170) restent en vigueur.

Certains produits de cryptologie sont soumis au régime des matériels de guerre (décret du 18 avril 1939) lorsqu'ils sont intégrés dans des armes ou permettent la mise en œuvre des forces armées (article 39 de la loi 2004-575).

Les textes relatifs à la signature électronique

La signature électronique est une composante de la SSI en ce qu'elle permet d'authentifier l'émetteur d'un document et d'en garantir l'intégrité. La loi 2000-230 modifiant l'article 1316 du code civil reconnaît la signature électronique comme fiable sous certaines conditions précisées par le décret 2001-272. La réglementation nationale transpose la directive européenne 1999/93/CE sur un cadre communautaire pour les signatures électroniques.

Quelques textes relatifs à la cybercriminalité

De nombreuses dispositions existent dans les domaines où les systèmes d'information servent à commettre ou préparer un crime ou un délit ou lorsqu'ils sont la cible d'une attaque.

Les articles 323-1 à 323-7 du code pénal sanctionnent les atteintes aux systèmes de traitement automatisé de données. L'article 163-4 du code monétaire et financier sanctionne la fabrication, détention, et cession de moyens informatiques permettant d'attaquer les cartes bancaires. La sécurité des cartes de paiement fait, en outre, l'objet d'un observatoire créé par l'article 39 de la loi 2001-1062 modifiant le code monétaire et financier.

La loi 2004-575 consacre un chapitre à la lutte contre la cybercriminalité (articles 41 à 46). L'article 31 de la loi 2001-1062 porte obligation de remise de clés cryptographiques aux autorités habilitées et judiciaires et l'article 37 de la loi 2004-575 aggrave les peines encourues lorsqu'il a été fait usage de cryptologie pour commettre ou préparer un crime ou délit.

D'autres textes permettent la saisie de données informatiques par les autorités (article 17 de la loi 2003-239 par exemple), ou obligent la conservation de données informatiques par les opérateurs permettant *a posteriori* de conduire des enquêtes (article 29 de la loi 2001-1062, article 18 de la loi 2003-239 par exemple), etc.

Un certain nombre de ces dispositions sont prises en conformité avec des textes internationaux comme la convention du Conseil de l'Europe sur la cybercriminalité (23 novembre 2001), ou la décision-cadre du Conseil de l'UE (2005/222/JAI) relative aux attaques visant les systèmes d'information.

Annexe X

Quelques principes généraux de sécurité

– Besoin d'une approche **globale :** afin que le dispositif ne présente pas de possibilités de contournement.

– La politique de sécurité doit être **apparente** : l'existence de mesures de protection doit être perçue sans pour autant être connue de façon détaillée.

– Nécessité d'une **gestion dynamique** du risque.

Le risque doit être géré de façon continue et dynamique dans un monde qui change très vite dans le domaine des technologies de l'information et de la communication.

Pour une entité donnée, il faut, à tout moment, être informé des menaces les plus probables et des vulnérabilités publiées et préparer un certain nombre de plans : réactions, de continuité des opérations... applicables en cas d'incident, ou en cas d'attaque.

Enfin, au-delà de ces plans, il peut s'avérer judicieux de faire appel, pour la gestion des incidents informatiques, à des spécialistes capables de caractériser l'attaque, d'évaluer les dégâts, et de prendre des mesures de confinement et de réaction.

On voit donc qu'une gestion dynamique du risque nécessite un minimum d'organisation. Il faut bien sûr constamment avoir des spécialistes de la question, capables d'exposer aux décideurs les enjeux, les parades, les mesures à prendre, mais aussi disposer d'une structure de prise de décision rapide.

Enfin, pour améliorer la connaissance du niveau de sécurité du système d'information, il est nécessaire de faire mener périodiquement des audits et des tests d'intrusion.

– **Principe de *minimalité***, ou « tout ce qui n'est pas autorisé est interdit ».
Seuls les protocoles et les services nécessaires à l'exécution du métier ou de la mission seront autorisés. Toute ouverture de nouveau service ou toute modification du routage des flux sera étudiée et donnera lieu à analyse de risque.

– **Principe d'*autoprotection*,** ou « tout ce qui est extérieur ne peut être considéré comme sûr ».
Le réseau d'organisme traitera initialement les autres réseaux auxquels il est connecté comme non-fiables, et appliquera des mesures de protection lors des échanges d'informations.

– **Principe de *confinement*,** ou « il faut toujours pouvoir isoler un membre infecté ».
Ceci est particulièrement utile en cas d'attaque par de ver ou de virus. Une application de ces deux principes est, par exemple, la mise en place de DMZ : une passerelle, ou pare-feu, placée en coupure entre un réseau non-protégé (par exemple l'Internet) et les réseaux qu'il protège, fait passer les informations qui transitent par une sorte de « sas de décontamination ». Ce sas peut lui-même constituer un sous-réseau, où une politique de sécurité particulière, moins stricte que celle du réseau interne, est mise en œuvre, et sur lequel on peut placer des machines dédiées (serveurs Web, antivirus, de messagerie), mais aussi des outils de détection d'intrusion...

– **Mise en place d'une *défense en profondeur***, ou « plusieurs lignes de défense valent mieux qu'une ».
Partant du constat que, dans les systèmes complexes, il faut toujours prévoir plusieurs lignes de défense, des mesures de protections bien distinctes, en particulier fonctionnellement, seront appliquées sur différentes composantes, de manière à ce qu'il n'y ait pas une ligne de défense unique.

– **Principe de *responsabilisation des utilisateurs*** ou gérer le « besoin d'en connaître » de chaque utilisateur, interne ou externe.

– **Vérification régulière de la mise en œuvre de la sécurité**, ou « mieux vaut prévenir que guérir ».

L'application de ces principes et la mise en œuvre des mesures de protection qui en résultent seront vérifiées au départ, puis périodiquement, pour éviter des dérives, peut-être non-intentionnelles, mais bien réelles.

Annexe XI

Les 12 clés de la sécurité selon l'AFNOR

D'après le Référentiel de bonnes pratiques de l'AFNOR – août 2002
Sécurité des Informations Stratégiques – Qualité de la confiance
Comment préserver la confidentialité des informations ?

1 – Admettre que toute entreprise possède des informations à protéger (plans de recherche, prototypes, plans marketing, stratégie commerciale, fichiers clients, contrats d'assurance...).

2 – Faire appel à l'ensemble des capacités de l'entreprise (chercheurs, logisticiens, gestionnaires de personnel, informaticiens, juristes, financiers...) pour réaliser l'inventaire des informations sensibles, des points faibles, des risques encourus et de leurs conséquences.

3 – Exploiter l'information ouverte sur l'environnement dans lequel évolue l'entreprise, observer le comportement des concurrents, partenaires, prestataires de service, fournisseurs, pour identifier les menaces potentielles.

4 – S'appuyer sur un réseau de fournisseurs de confiance pour ceux d'entre eux qui partagent ou accèdent à des informations sensibles.

5 – Ne pas chercher à tout protéger : classifier les informations et les locaux en fonction des préjudices potentiels et des risques acceptables.

6 – Mettre en place les moyens de protection adéquats correspondant au niveau de sensibilité des informations ainsi classifiées, s'assurer qu'ils sont adaptés et, si besoin, recourir à des compétences et expertises extérieures.

7 – Désigner et former des personnes responsables de l'application des mesures de sécurité.

8 – Impliquer le personnel et les partenaires en les sensibilisant à la valeur des informations, en leur apprenant à les protéger et en leur inculquant un réflexe d'alerte en cas d'incident.

9 – Déployer un système d'enregistrement des dysfonctionnements (même mineurs), et analyser tous les incidents.

10 – Ne pas hésiter à porter plainte en cas d'agression.

11 – Imaginer le pire et élaborer des plans de crise, des fiches « réflexe » afin d'avoir un début de réponse, au cas où...

12 – Évaluer et gérer le dispositif, anticiper les évolutions (techniques, concurrentielles...) et adapter la protection en conséquence en se conformant aux textes législatifs et réglementaires en vigueur.

Annexe XII

Exemples de chartes d'utilisateurs dans les entreprises et l'État [1]

Les chartes d'utilisation des systèmes d'information, dont quelques points clés sont indiqués ci-après, se diffusent désormais de manière croissante dans les entreprises et au sein de l'État.

Quelques points clés :

• **Les objectifs de ces chartes :** définir les bonnes pratiques comportementales devant être respectées et qui relèvent :
– du comportement loyal et responsable de chacun. La responsabilité individuelle est la base de la SSI ;
– de règles déontologiques et de législations applicables ;
– de règles principales de sécurité.

• **Bases juridiques des chartes :**
– elles peuvent faire l'objet d'une consultation des comités d'entreprises (CE) et d'une déclaration auprès de la CNIL ;
– elles peuvent engager, pour certaines, les salariés à des sanctions en cas d'usage abusif ;
– elles sont annexées dans certains cas au contrat de travail ou au règlement intérieur de l'entreprise ;
– dans certaines administrations, l'utilisateur peut être amené à signer une reconnaissance de responsabilité.

• **Quelques principes directeurs :**
– les chartes **s'appliquent à tous les utilisateurs quel que soit leur niveau hiérarchique** : dirigeants, salariés, intérimaires, stagiaires, consultants, prestataires... ;
– les utilisateurs **doivent prendre connaissance** des règles qui sont définies dans les documents de politique de sécurité des entreprises destinés à garantir la bonne gestion ainsi que la sécurité des ressources informatiques et de communication ;
– un rappel de la **législation en vigueur** relative par exemple à la fraude informatique, aux atteintes à la personnalité et aux mineurs et les infractions à la propriété intellectuelle (copies illicites...) est fourni avec les chartes. Les utilisateurs doivent en prendre connaissance et **s'engager** à user des ressources informatiques dans le respect de ces lois et réglementations ;

1. Sources auditions.

– l'utilisateur **fait de la sécurité une priorité** et met en œuvre les règles pratiques de sécurité comme :
· la protection de l'accès à son poste de travail et à ses données (mots de passe, mise en veille avec mot de passe...) ;
· se protéger contre le vol ;
· éviter les doubles connexions Intranet/Internet ;
· une protection spécifique lors des déplacements notamment à l'étranger ;
– les ressources informatiques et de communication sont destinées à un **usage professionnel**. L'usage privé peut être toléré, s'il n'affecte pas la circulation normale de l'information ;
– les utilisateurs s'engagent à **respecter la configuration** de leur poste de travail et à ne pas installer leurs propres logiciels ou matériels ;
– les utilisateurs ont une **obligation de confidentialité** sur les informations stockées ou transmises au moyen des ressources informatiques qui lui sont affectées ;
– l'utilisateur doit faire preuve de **vigilance** vis-à-vis des informations recueillies sur Internet ou reçues par messagerie (possibilité de désinformation, s'assurer de l'émetteur...) ;
– chaque utilisateur doit être conscient que certains échanges avec des tiers **peuvent engager** l'entreprise (contractuellement éventuellement) ou porter atteinte à son image. Le respect des délégations de pouvoirs établies doit s'appliquer également.
– ...

Annexe XIII

Exemples de produits logiciels et matériels de SSI

Antivirus

Les logiciels contre les codes illicites doivent permettre de détecter les codes malveillants, virus et vers. Les antivirus doivent être acquis avec un service de mise à jour sur abonnement pour être efficaces. Les antivirus, qui constituent le premier marché de la sécurité en chiffre d'affaires, sont donc à classer plus encore dans le marché de services que dans celui de produits. Les logiciels antivirus font parties du segment SCM (*Secure Content Management*).
L'effet de l'apparition récente de Microsoft est la seule incertitude sur ce segment qui reste promis à quelques fructueuses années.

Antispam

Comme les logiciels antivirus, des versions pour les serveurs d'organisation et des versions pour les particuliers ont été développées.
Ce segment de marché, qui appartient au segment SCM, compte tenu de la baisse du volume du spam, pourrait entrer en déflation.

Sécurité de messagerie

Le chiffrement applicatif des messages est la mesure de sécurité nécessaire pour protéger des mails d'une interception durant leur transfert.
À côté des logiciels gratuits ou intégrés, les solutions spécifiques n'ont pas encore trouvé un segment de marché viable. Ce segment fait partie du segment SCM.
En dehors de solutions à haut niveau de confiance développées pour le ministère de la Défense, sans doute faute de besoins, aucune offre nationale ne subsiste dans le domaine.

Pare-feu (ou coupe-feu)

Les pare-feux, (*Firewall*) ont pour fonction de contrôler la connexion entre deux réseaux appliquant des politiques de sécurité différentes en contrôlant la licité de tous les échanges vis-à-vis d'une politique d'interconnexion. Le marché adresse les grandes entreprises jusqu'aux particuliers. Ils peuvent être sous forme d'*appliances* (boîtiers intégrés) pour la protection des réseaux des entreprises ou logiciels pour les postes individuels par exemple.

Il est à noter que les dernières versions du logiciel d'exploitation de Microsoft incluent en standard un coupe-feu susceptible de convenir aux particuliers, ce qui pourrait conduire à une contraction de ce segment de marché pour les autres acteurs de ce marché. Le coupe-feu étant un point naturel d'accroche d'autres services de sécurité : VPN, antivirus, etc., les fournisseurs disposent d'une plate-forme idéale pour étendre les services offerts.

Détection et prévention d'intrusion

Les logiciels de détection d'intrusion sont destinés à permettre aux organisations de réagir dès lors qu'une attaque a réussi à franchir les défenses. Cette fonction est souvent ajoutée aux fonctions de coupe-feu. En général, les études de marché intègrent dans un même segment les pare-feux et les fonctions de prévention et de détection d'intrusion.
Les logiciels de prévention d'intrusion effectuent un audit d'un système d'information et doivent détecter les éléments de configuration non-sûrs et identifier les axes potentiels d'attaque.
L'évolution de ce segment est très incertaine. Les produits de détection d'intrusion doivent améliorer à la fois leur capacité de détection et réduire leur taux de fausse alarme.

Administration sûre

Les logiciels d'administration sûrs doivent permettre en centralisant la gestion des identités, des droits, des secrets, de la configuration d'équipements de sécurité d'offrir une version synthétique de la sécurité d'un système d'information. Ces logiciels sont souvent désignés en anglais sous le vocable *Security 3A Software* (3A pour Authentification, Autorisation et Administration) que l'on peut résumer en management des identités et de l'accès. Ces produits sont plus destinés à des organisations qu'à des particuliers.

Authentification renforcée

Une amélioration notable de la sécurité d'un système d'information vient aussi de la mise en place de moyens d'authentification des utilisateurs plus sophistiqués que le mot de passe. Ce segment est lié au segment précédent. Parmi les types de solutions qui existent on retiendra :
– les cartes à puces, les *tokens* stockant des clés secrètes ou clés USB ;
– la biométrie.
Ce marché devrait connaître une croissance soutenue, l'identification et l'authentification restant un préalable à toute tentative de sécurisation.

VPN/chiffrement IP

Pour relier en toute sécurité deux parties d'un même système d'information, en complément d'un coupe-feu, afin de parer aux risques

d'interception passive, il est nécessaire de chiffrer les flux échangés et de créer ainsi un tunnel de communication protégé dit VPN [1].
L'offre nationale provient principalement de groupes importants.

Chiffrement de fichiers

Le segment de marché du chiffrement de fichiers avant leur envoi comme pièce jointe par messagerie ou simplement pour leur stockage souffre des mêmes maux que le marché de la messagerie sécurisée, des fonctions de chiffrement de fichiers sont soit incluses dans les principaux systèmes d'exploitation, soit disponibles assez largement en logiciel libre.
Il existe toutefois une offre française émanant de PME.
L'offre insuffisante a conduit l'administration à développer des solutions en interne.

Mémoires de masse chiffrante

Le chiffrement d'un disque dur est indiscutablement la meilleure solution aux risques de pertes ou de vol d'ordinateurs portables par exemple.
Sans appui de la commande publique, le risque est réel cependant qu'aucune société française n'offre ce type de produits avec un haut niveau d'assurance. Ce segment devrait rester confidentiel en l'absence de prise de conscience par les grands comptes.

Téléphones chiffrants

Le téléphone, soit fixe, soit mobile, sera bientôt le dernier vestige de l'ancêtre du système d'information, le réseau de télécommunications. Les réseaux de télécommunications sont principalement menacés du point de vue de l'utilisateur par l'interception.
Bien que cette menace soit réelle, sa perception n'est pas suffisante pour inciter les organisations à s'en préoccuper. Il en résulte un segment de marché restreint aux applications gouvernementales principalement.

1. Virtual Private Network.

Annexe XIV

Normalisation et principes de l'évaluation/certification, de la qualification et de l'agrément

La normalisation

Les organismes de normalisation

Filière	Niveau international	Niveau européen	Instance nationale
Généraliste	ISO	CEN	AFNOR
Télécoms	UIT	ETSI	AFNOR
Électrique	CEI	CENELEC	UTE

La norme ISO 17 799

D'après le *Référentiel de bonnes pratiques de l'AFNOR*
Sécurité des informations stratégiques – Qualité de la confiance
Comment préserver la confidentialité des informations
Août 2002

Le référentiel Qualité de la confiance est un document visant à aider les entreprises à engager une réflexion globale en vue d'assurer la maîtrise de la confidentialité de leurs informations stratégiques. Il rassemble l'essentiel des bonnes pratiques qui permettent d'assurer la sécurité des informations, mais il ne prétend pas fournir des solutions exhaustives et normalisées dans ce domaine.

Les entreprises souhaitant s'appuyer sur une norme, pourront utiliser l'ISO 17 799 qui, au travers de 36 objectifs de contrôle associés à 128 contrôles, couvre les points-clé du management de la sécurité de l'information :

- Politique sécurité et démarche associée.
- Organisation et sécurité.
- Classification des objets et contrôles.
- Sécurité et personnel.
- Sécurité et environnement physique.
- Réseau et administration informatique.
- Contrôle d'accès aux systèmes et applications.
- Développement et maintenance informatique.
- Plan de continuité.
- Conformité légale et audits de contrôle.

De plus, il existe dans différents pays des schémas d'évaluation et de certification par rapport à la norme ISO 17 799, selon une démarche similaire aux schémas portant sur les systèmes de management de la qualité (ISO 9000).

Dans le cas de l'ISO 17 799, la certification porte sur le système de management de la sécurité de l'information mis en place par l'entreprise.

De manière générale, un système de management correspond à l'ensemble des moyens, ressources, procédures, etc., qu'il faut définir, organiser, mettre en œuvre et maintenir dans le temps, afin d'assurer une activité répondant aux besoins de l'entreprise, des clients et des partenaires ainsi qu'aux exigences réglementaires.

La norme ISO 17 799 (« guide de bonnes pratiques pour le management de la sécurité de l'information ») fournit les éléments permettant la conception, la documentation et la mise en place d'un système de management de la sécurité de l'information.

Les principes de l'évaluation/certification

Le processus d'évaluation et de certification

On se place dans le cas de figure d'une entreprise qui paye l'évaluation et souhaite faire certifier un produit :
– l'entreprise définit une cible de sécurité et s'adresse à un ou plusieurs centres d'évaluation (CESTI) agréés par la DCSSI (5 en France) pour obtenir un devis ;
– il choisit un CESTI pour mener à bien l'évaluation et dépose un dossier de demande de certification au centre de certification de la DCSSI après avoir affiné la cible de sécurité ;
– la DCSSI analyse le dossier pour vérifier si le CESTI est effectivement en mesure de réaliser l'évaluation, si le devis est réaliste pour le type de produit, si la cible de sécurité du produit est pertinente... Si le dossier est accepté, la DCSSI nomme un certificateur chargé de suivre l'évaluation et enregistre la demande ;
– la DCSSI peut proposer une réunion de lancement aux différents acteurs ;
– le CESTI réalise l'évaluation. Cette évaluation est suivie par le certificateur ;
– le CESTI rédige le rapport technique d'évaluation et le transmet à la DCSSI ;
– la DCSSI valide le rapport technique d'évaluation, rédige le rapport de certification et propose la certification au directeur central ;
– la DCSSI organise une revue finale.

Présentation des critères d'évaluation de la sécurité des technologies de l'information.

La sécurité d'une organisation passe en premier lieu par la prise de conscience d'un fait : il y a des biens à protéger et il existe des menaces qui pèsent sur eux [1]. Cette étape franchie (car elle n'est pas évidente pour tout le monde), elle conduit à traduire les objectifs de l'organisation (profits, services publics, notoriété, etc.) dans une politique de sécurité.

L'objet n'est pas ici d'indiquer comment aboutir à une politique de sécurité. Tout juste faut-il rappeler qu'une fois définie, elle implique la mise en place de contre-mesures de sécurité (des parades) destinées à contrer les menaces retenues. Ces contre-mesures sont réalisées par un assemblage subtil de mesures organisationnelles et techniques. Cet article s'intéresse pour l'essentiel aux contre-mesures techniques qui sont fournies par des produits techniques (antivirus, firewall, chiffrement de données, etc.) dont l'offre est parfois pléthorique. Lesquels choisir ?

Dans le domaine de la sécurité, un critère de choix primordial devrait être la confiance que l'on peut avoir dans le fait qu'un produit donné réalise bien la fonctionnalité de sécurité qu'il propose. Par « bien », on peut comprendre au minimum :
– que le produit réalise effectivement la fonctionnalité de sécurité ;
– que la fonctionnalité de sécurité proposée est efficace pour parer les menaces retenues.

Lorsque l'on achète un téléviseur, on peut assez facilement vérifier que sa principale fonctionnalité, celle de recevoir et afficher des images sonorisées, est plus ou moins bien réalisée.

Lorsque l'on utilise un produit de chiffrement, qu'est-ce qui nous prouve que le produit chiffre réellement ? Qu'est-ce qui nous prouve que la clé de 128 bits a réellement 128 bits d'entropie ? Qu'est-ce qui nous prouve que cette clé n'accompagne pas le message chiffré ? etc.

Ce besoin de confiance a amené certaines organisations à élaborer des critères d'évaluation de la sécurité visant à mesurer le niveau de confiance d'un produit technique et ce, de la façon la plus objective possible. Trois grands documents ont marqué les vingt dernières années : Le Livre orange ou TCSEC, les ITSEC et les CC. Cet article présente rapidement les ITSEC et les CC.

Les critères pour l'évaluation de la sécurité des technologies de l'information (ITSEC)

Les ITSEC ont été développés à la fin des années quatre-vingt à l'initiative de quatre pays européens (la France, le Royaume-Uni, l'Allemagne et la Hollande). Ils ont été repris et publiés en juin 1991 par la

1. On partira des objectifs généraux de l'organisation (profits, services public, notoriété, etc.) dans un contexte légal donné que l'on traduira sous l'angle de la sécurité dans une politique de sécurité en passant par une analyse de risques.

commission des communautés européenne. Ils visent à satisfaire les besoins des marchés civils et gouvernementaux et s'intéressent aux aspects *confidentialité*, *intégrité* et *disponibilité*.

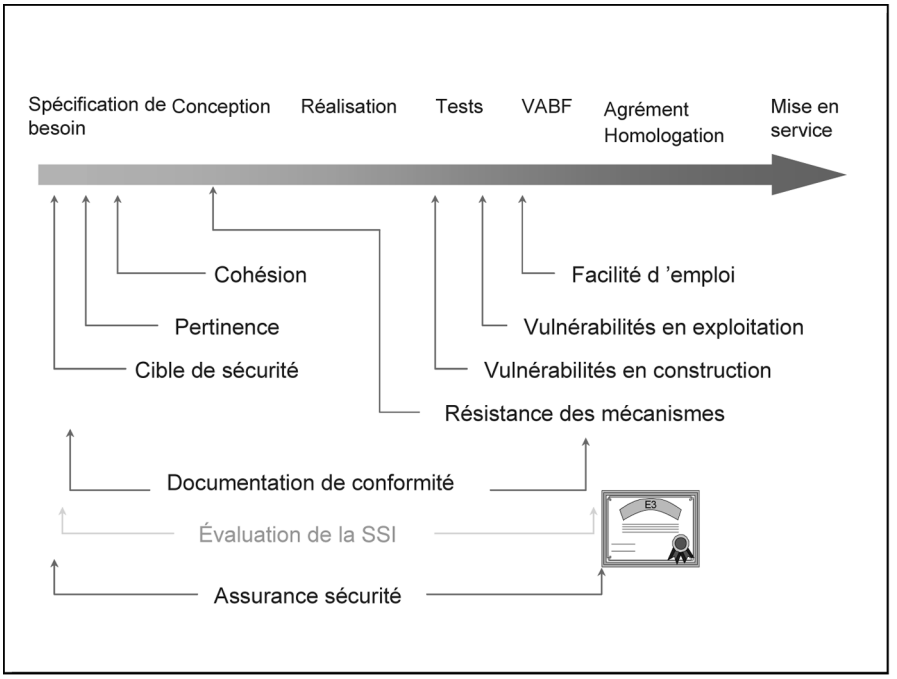
Une évaluation ITSEC porte sur une *cible d'évaluation* (l'objet à évaluer) qui peut être un produit ou un système : un système est utilisé dans un environnement réel parfaitement connu alors qu'un produit est utilisé dans un environnement supposé décrit sous la forme d'hypothèses.

La description précise des caractéristiques de sécurité de la cible d'évaluation est fournie par un document nommé *cible de sécurité* (la spécification de besoin en sécurité). Ce document doit contenir une description de la politique de sécurité du système ou l'argumentaire du produit. Elle fournit également une description des objectifs de sécurité, les menaces qui sont parées par le produit, la spécification des fonctions de sécurité qui parent les menaces (avec éventuellement, une description des mécanismes de sécurité qui implémentent ces fonctions). Enfin, la cible doit préciser le niveau de confiance visé et la résistance des mécanismes, ces deux notions étant expliquées plus loin.

Le but d'une évaluation ITSEC consiste à vérifier deux aspects de la sécurité de la cible d'évaluation : la conformité (assurance conformité) et l'efficacité (assurance efficacité).

Pour l'assurance conformité, l'évaluation porte sur les points suivants :
– le processus de développement (spécification de besoin, conception générale et détaillée, réalisation) ;
– l'environnement de développement (méthodes de travail, contrôle de configuration, choix des langages et des outils, mesures de sécurité dans le développement) ;
– le fonctionnement opérationnel (documentation utilisateur et administrateur, livraison, configuration, démarrage et utilisation).

Pour l'assurance efficacité, l'évaluation porte sur les aspects suivants :
– la pertinence de la fonctionnalité : les fonctions de sécurité doivent contrer efficacement les menaces identifiées ;
– la cohésion de la fonctionnalité : les fonctions et mécanismes de sécurité doivent former un tout cohérent ;
– la résistance des mécanismes : la cible doit résister à des attaques directes selon le niveau de résistance des mécanismes annoncés dans la cible de sécurité ;
– les vulnérabilités de constructions : les éventuelles faiblesses connues de réalisation de la cible ne doivent pas compromettre la sécurité de la cible d'évaluation ;
– les vulnérabilités d'exploitation : les éventuelles faiblesses connues en exploitation ne doivent pas compromettre la sécurité de la cible d'évaluation ;
– la facilité d'emploi : la cible ne doit pas être configurable ou utilisable de manière non-sûre mais qu'un utilisateur ou un administrateur pourrait croire sûre.



Dans les ITSEC, le niveau de confiance visé est noté E1 à E6. Plus il est élevé, plus la confiance est élevée (si le niveau est atteint). Plus il est élevé, plus les éléments de preuve fournis à l'évaluateur au titre de **l'assurance conformité** doivent être importants et plus l'évaluateur doit réaliser des travaux de vérification au titre de la conformité.

– E0 : le produit ne répond pas à sa cible de sécurité. Ce n'est pas un niveau visé !

– E1 : vérification de la conception générale, tests fonctionnels...

– E2 : E1 + vérification de la conception détaillée, gestion de configuration, processus de diffusion...

– E3 : E2 + vérification de la réalisation (ce qui implique le code source et/ou les schémas matériels)...

– E4 : E3 + modèle formel de la politique de sécurité, spécification semi-formelle des fonctions de sécurité, de la conception générale...

– E5 : E4 + correspondance étroite entre conception détaillée et code source...

– E6 : E5 + spécification formelle des fonctions dédiées à la sécurité, source des bibliothèques...

La seconde échelle d'assurance concerne la résistance des mécanismes. La résistance visée peut être qualifiée d'élémentaire (mis en échec par des utilisateurs compétents), de moyenne (protection contre des agresseurs dont les opportunités et les ressources sont limitées) ou d'élevée (mise en échec par des agresseurs disposant d'un haut degré d'expertise, d'opportunité et de ressources avec le succès d'une attaque jugé exceptionnel).

Les CC ou critères communs (ISO15408)

Les CC reprennent les concepts des ITSEC mais introduisent quelques nouveautés. Ils utilisent un formalisme permettant de désigner des classes d'exigences se subdivisant en famille qui, elles-mêmes, se subdivisent en composants.

Les classes d'exigences peuvent être fonctionnelles ou d'assurance.

Une classe fonctionnelle décrit les fonctionnalités de sécurité qu'un produit peut mettre en œuvre alors qu'une classe d'assurance décrit les moyens d'acquérir la confiance dans le fait que la fonctionnalité de sécurité est conforme et efficace.

Un composant est le plus petit ensemble sélectionnable d'élément (fonctionnel ou d'assurance).

Une famille est un regroupement de composants qui ont en commun des objectifs de sécurité mais qui peuvent différer en terme d'importance ou de rigueur. Il peut exister des dépendances entre les composants : par exemple, le composant traitant de la distribution des clés cryptographique peut dépendre du composant générant les clés cryptographiques.

Tous ces éléments sont regroupés dans des catalogues permettant de construire :
– des paquets : regroupement réutilisable de composants visant à satisfaire des objectifs de sécurité bien identifiés ;
– des cibles de sécurité comme pour les ITSEC ;
– des profils de protection (PP) qui correspondent en pratique à une cible de sécurité générique et qui se situent donc à un niveau d'abstraction supérieur. Par exemple, on pourra trouver un profil de protection pour les pare-feux en général. Un pare-feu particulier devra disposer d'une cible de sécurité propre qui pourra être conforme au profil de protection des pare-feux en général. La cible de sécurité est associée à une cible d'évaluation réelle alors que le profil de protection est associé à un produit virtuel.

Avec les PP, les CC disposent d'un outil permettant de *normaliser* des fonctionnalités et des niveaux d'assurances pour des produits ou des systèmes. Ainsi, les cibles de sécurité de produits d'une même famille peuvent se référer à un même PP ce qui facilite la comparaison entre les produits certifiés.

Les CC comportent sept niveaux de confiance (ou niveaux d'assurance) notés EAL1 à EAL7. Ont peut établir une correspondance avec les niveaux ITSEC : EAL2 → E1, EAL3 → E2... EAL7 → E6. À chaque niveau de confiance est associé un certain nombre de classes d'assurances avec des composants impliquant une rigueur et des exigences croissantes dans l'évaluation. Les niveaux peuvent être augmentés. Cette augmentation consiste par exemple à sélectionner un composant d'assurance impliquant des exigences plus élevées que ce qui est requis par la norme. On note cette augmentation par le signe +. Par exemple, EAL4 augmenté est noté EAL4+.

Certification et reconnaissance des certificats

Une évaluation réussie aboutie normalement à l'émission d'un certificat indiquant que la cible d'évaluation est conforme à sa cible de sécurité. L'évaluation est un processus qui peut s'avérer long et coûteux. Il n'était donc pas envisageable que les produits soient obligés de se faire évaluer dans chaque pays où ils sont diffusés. C'est pourquoi une exigence qui est apparue dès les ITSEC a été la reconnaissance mutuelle des certificats indépendamment du pays et de l'organisme où l'évaluation a été réalisée.

Cet objectif est atteint par la mise en place d'un schéma décrivant l'organisation adoptée pour réaliser les évaluations et leur certification. En France, les évaluations sont réalisées par des centres d'évaluation de la sécurité des technologies de l'information (CESTI) qui doivent être accrédités selon la norme EN17025 par le comité français pour l'accréditation (COFRAC) et agréés par la direction centrale de la sécurité des systèmes d'information (DCSSI).

L'accréditation garantie, entre autres, l'existence d'un manuel qualité propre au laboratoire, d'une organisation adaptée et surtout, de l'absence de pression sur les évaluateurs qui pourraient biaiser les résultats de l'évaluation. L'agrément garanti, entre autres, la compétence du laboratoire dans son domaine d'activité et sa capacité à assurer la confidentialité, tant du déroulement de l'évaluation que des fournitures qu'il manipule et qui peuvent contenir des secrets industriels. Plus généralement, l'objectif de ces schémas est d'assurer :
– la répétabilité (la constance) : une même évaluation menée par un même laboratoire doit donner le même résultat ;
– la reproductibilité : une même évaluation menée par deux laboratoires différents doit donner le même résultat ;
– l'objectivité : les opinions et jugements subjectifs sont réduits au minimum ;
– l'impartialité : le laboratoire ne subit pas de pression pouvant biaiser les résultats ;
– la compétence : le laboratoire est compétent pour mener l'évaluation dans un domaine technique donné avec des critères donnés (ITSEC ou CC) pour un niveau maximum d'évaluation donné.

Aujourd'hui, les certificats CC sont reconnus formellement par un grand nombre de pays jusqu'au niveau EAL4.

Durée des évaluations

Une évaluation est un processus long. Certaines ont duré deux ans pour des niveaux visés EAL4 ce qui est une situation anormale. Une des principales raisons de cet état de fait a longtemps été liée à l'inexpérience des développeurs qui n'étaient pas en mesure de fournir les éléments de preuve attendus par le CESTI. Cette situation s'améliore aujourd'hui et on peut envisager des évaluations en moins de six mois, toujours pour ces niveaux. Les développeurs maîtrisent de mieux en mieux les critères ou se font accompagner par des sociétés qui les aident à les mettre en œuvre. On ne saurait trop conseiller à un développeur vierge sur ce

sujet de se faire accompagner par un conseil compétent lors de sa première évaluation afin d'éviter bien des déboires.

Coût des évaluations

Le coût d'une évaluation se décompose en deux parties et est variable en fonction du niveau de confiance visé : le coût induit par la prise en compte des critères dans le développement du produit à faire évaluer et le coût de l'évaluation elle-même qui est dû au CESTI. En France, l'organisme de certification (la DCSSI) ne fait pas payer ses prestations.

Le premier coût est d'autant plus important que le développeur n'a pas introduit les exigences d'assurance des critères dès le début de son développement. On considère que pour un niveau E3 – EAL4, le coût associé à l'assurance conformité devrait être faible si le développement se fait sous contrôle qualité. Par contre, le coût de production des fournitures associées à l'assurance efficacité n'est généralement pas pris en compte dans les processus de développement sous contrôle qualité et doit donc être intégralement ajouté au coût de réalisation du produit.

Le coût d'une évaluation EAL4 pour un produit de complexité moyenne (un pare-feu par exemple) est de l'ordre de 100 à 150 k€ ce qui est loin d'être négligeable.

Ce coût élevé explique le peu de succès de l'évaluation pour des produits de faible coût à la diffusion limitée. Pour ces produits, la seule façon de pouvoir se faire certifier est de trouver un ou plusieurs clients fortement concernés par la sécurité et qui acceptent de jouer le rôle du commanditaire.

Conclusions

L'évaluation de la sécurité selon des critères normalisés est aujourd'hui l'outil le plus élaboré pour certifier le niveau de confiance d'un produit ou d'un système, en particulier, dans le cas où l'on a besoin de faire partager cette confiance. Son coût le réserve aujourd'hui à des produits de diffusion telle qu'un retour sur investissement est possible ou à des organisations qui ont les moyens de leurs ambitions en matière de sécurité.

L'évaluation n'est pas antinomique avec l'expertise. En particulier, une organisation qui veut se convaincre de la sécurité d'un produit sans avoir besoin de faire partager cette confiance à d'autres utilisera ce moyen pour obtenir cette conviction à moindre coût. D'autant plus que certaines officines proposant ce type de prestation ont elles-mêmes fait évoluer leur pratique en intégrant les critères communs dans leur démarche d'analyse.

Les CC, ITSEC et autres documents d'application des critères sont téléchargeables sur le site www.ssi.gouv.fr. On y trouve également la liste des CESTI agréés, la liste des produits certifiés en France et des liens sur des sites d'organismes homologues à la DCSSI à l'étranger.

On pourra consulter également le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

La qualification

Les administrations souhaitent disposer de produits de sécurité dans lesquels elles peuvent avoir confiance et qui répondent à leurs besoins de sécurité. La certification offre un élément de réponse au premier point mais pas au second.

Il faut en effet se rappeler qu'un produit est évalué selon sa cible de sécurité (sa spécification de besoin de sécurité). Cette cible est réalisée sous la responsabilité du développeur qui y met ce qu'il veut.

Ainsi, deux pare-feux peuvent être évalués au même niveau de confiance mais sur des spécifications de besoins différentes. Et peut-être qu'aucune des deux ne répondra aux besoins d'une certaine catégorie de client.

Ce qu'introduit le processus de qualification créé par la DCSSI est de s'assurer que les cibles de sécurité des produits (en terme notamment de périmètre et de profondeur de l'évaluation) répondent aux besoins des administrations.

On distingue trois niveaux de qualification : *standard*, *renforcé* et *élevé*.

Les deux premiers niveaux ont été définis et leurs processus sont rendus publics. Ils correspondent respectivement, en matière de niveau d'assurance des critères communs, à une certification EAL2+ pour le niveau standard et EAL4+ pour le niveau renforcé. La qualification fait aussi appel à la cotation des mécanismes cryptographiques par la DCSSI et à l'évaluation des signaux compromettants (à partir de niveau renforcé).

Ce qui est également primordial, c'est de définir les usages de la qualification : ainsi, la DCSSI et l'ADAE référencent la qualification dans le référentiel sécurité de l'administration électronique (Politique de référencement intersectorielle de sécurité, PRIS), et la DCSSI exploite la qualification en vue de la délivrance des cautions et agréments.

La caution et l'agrément

La caution est l'attestation délivrée par la DCSSI qu'un produit offrant des services de chiffrement est apte, dans certaines conditions, à protéger de l'information sensible non-classifiée de défense au sens de la réglementation (recommandation 901). Cette caution s'appuie directement, pour la protection des informations sensibles de niveau diffusion limitée, sur la qualification de niveau standard, les conditions correspondant aux restrictions d'usage du produit figurant dans le rapport de certification.

L'agrément est l'attestation délivrée par la DCSSI qu'un produit de chiffrement est apte dans certaines conditions, à protéger des informations sensibles classifiées de défense au sens de la réglementation (instruction interministérielle 900). L'exploitation de la qualification pour un agrément fait l'objet de procédures spécifiques.