POLYNESIE FRANÇAISE

MINISTERE
DE L'EDUCATION,
DE LA MODERNISATION
DE L'ADMINISTRATION,
en charge du numérique

DIRECTION GENERALE
DES RESSOURCES HUMAINES

CONCOURS **EXTERNE** POUR LE RECRUTEMENT DES **INGENIEURS EN CHEF DE 1RE CATEGORIE DE 2E CLASSE DE CATEGORIE A** RELEVANT DE LA FONCTION PUBLIQUE DE LA POLYNESIE FRANÇAISE

PREMIERE EPREUVE D'ADMISSIBILITE :

Rédaction d'une note de synthèse
à partir de l'analyse d'un dossier technique

SUJET PRINCIPAL

Jeudi 13 avril 2023

(Durée : 4 heures – coefficient 5)

Le sujet comporte 35 pages (page de garde incluse).

Aucun autre document n'est autorisé.

Calculatrice électronique de poche – y compris calculatrice programmable, alphanumérique ou à écran graphique – à fonctionnement autonome, non imprimante, non autorisée.
L'usage de tout ouvrage de référence, de tout dictionnaire, de tout autre matériel électronique et de téléphone cellulaire est rigoureusement interdit.

NB : La copie que vous rendrez ne devra, conformément au principe d'anonymat, comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé comporte notamment la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de signer ou de l'identifier.

SUJET :

Dans un premier temps, vous établirez une note de synthèse à partir du dossier joint à l'attention de votre ministre de tutelle polynésien.

Dans un second temps, vous lui présenterez, en qualité d'ingénieur en chef, des propositions de communications aux citoyens et aux professionnels de la Polynésie française visant à renforcer leurs connaissances sur les différents aspects des rayonnements ionisants.

Barème de notation :

Technicité : 14 points
Expression: 6 points
Les deux parties ont la même pondération

DOCUMENTS JOINTS :

Document N°1 (2 pages) **:** Institut de Radioprotection et de Sûreté Nucléaire (IRSN), www.irsn.fr - 21/05/2012
Savoir et Comprendre.
Document N°2 (1 page) : Autorité de Sûreté Nucléaire (ASN), www.asn.fr - 11/08/2009
L'ASN et la Polynésie française signent une convention de coopération pour le contrôle de la radioprotection des installations médicales utilisant des rayonnements ionisants
Document N°3 (1 page) : Centre Hospitalier de la Polynésie française (CHPF), www.chpf.pf – 20/03/2023
La médecine isotopique.
Document N°4 (2 pages) : Centre National de la Recherche Scientifique (CNRS), www.cnrs.fr –01/01/2018
Réglementation relative aux rayonnements ionisants
Document N°5 (7 pages) : La Présidence de la Polynésie française, www.presidence.pf – 01/02/2020
Conséquences sanitaires des essais nucléaires français dans le Pacifique.
Document N°6 (7 pages) : Lexpol, www.dlexpol.cloud.pf -23/01/2023
Loi du pays n° 2023-15 du 23 janvier 2023 relative à la protection des personnes et de l'environnement contre les risques liés à l'exposition aux rayonnements ionisants (extraits)
Document N°7 (7 pages) : Santopta, www.santopta.fr – 17/01/2014
La nouvelle directive 2013/59/Euratom est parue
Document N°8 (1 page) : Tahiti-infos, www.tahiti-infos.pf – 13/05/2015
Inauguration de l'unité d'hospitalisation complète en oncologie du CHPF
Document N°9 (1 page) : TNTV news, www.tntv.pf – 04/11/2022
Du nouveau matériel pour le traitement du cancer de la prostate au CHPF
Document N°10 (3 pages) : Lexpol, www.dlexpol.cloud.pf -23/01/2023
Loi du pays n° 2023-14 du 23 janvier 2023 relative à la prévention des risques d'exposition aux rayonnements ionisants en milieu professionnel

DOCUMENT N°1

Institut de Radioprotection et de Sûreté Nucléaire (IRSN) - 21/05/2012

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

IRSN
INSTITUT DE RADIOPROTECTION ET DE SÛRETÉ NUCLÉAIRE

Toute notre expertise pour vous protéger

Savoir et comprendre

Qu'est-ce qu'un rayonnement ionisant ?

Dans notre quotidien, nous sommes entourés par de nombreux types de rayonnement (couramment appelés rayons), visibles ou invisibles . Mais la plupart des rayonnements de notre quotidien - radio, téléphonie mobile, micro-ondes - ne sont pas ionisants.
Un rayonnement est une émission d'énergie et/ou un faisceau de particules.
Certains rayonnements (X et gamma) sont dits ionisants car ils émettent des « rayons » d'énergies suffisantes pour transformer les atomes qu'ils traversent en ions (un atome qui a perdu ou gagné un ou plusieurs électrons). Cela peut rendre la matière instable.
Un atome – instable de nature ou après un contact avec un rayonnement – va chercher à se stabiliser en émettant différents rayonnements :

- en perdant des protons et des neutrons : rayonnement alpha ;
- en transformant un neutron en proton ou vice-versa : rayonnement beta moins ou beta plus ;
- en émettant des photons (particules composants la lumière) : rayonnements X et gamma.

Les rayonnements provoquent des effets différents sur l'organisme en fonction du type de rayonnement et de la dose reçue.
L'énergie dégagée n'est en effet pas identique pour tous les rayonnements, et les moyens de s'en protéger sont donc différents. Par exemple, une feuille de papier est suffisante pour arrêter les rayonnements alpha, mais il faut un mètre de béton ou de plomb pour arrêter des rayonnements gamma.

Les unités de mesure

Trois unités sont fréquemment utilisées dans le domaine du nucléaire : le becquerel (Bq), le gray (Gy) et le sievert (Sv).
Le becquerel (Bq) mesure l'activité (nombre de désintégration par seconde) de la matière radioactive. Anciennement, l'unité de mesure utilisée était le curie (Ci). Un curie (1 Ci) équivaut à 3,7.10 10 Bq.
De son côté, le gray (Gy) mesure la dose physiquement « absorbée » par la matière . Elle représente l'énergie absorbée par un kilogramme exposé à un rayonnement ionisant apportant une énergie d'1 joule : 1 Gy = 1 J/kg. Anciennement, l'unité de mesure utilisée était le rad (1 gray = 100 rad).
Enfin, le sievert (Sv) est l'unité de mesure des doses équivalente et efficace, qui permet d'évaluer l'impact du rayonnement sur la matière vivante. Ainsi peut-on comparer l'effet d'une même dose délivrée par des rayonnements de nature différente à l'organisme entier, des organes ou des tissus qui n'ont pas la même sensibilité aux rayonnements. Anciennement, l'unité de mesure utilisée était le rem (1 rem = 0,01 Sv).

La période radioactive

La période (ou demi-vie) est **le temps nécessaire pour que la moitié des atomes se désintègrent naturellement.**
Cela ne dépend pas de l'environnement (température, pression) mais c'est une propriété liée à l'élément radioactif - radionucléide - considéré.
Par exemple, le césium 137 a une période radioactive de 30,2 ans. Cela signifie qu'au bout de ce laps de temps, la moitié du fragment de césium 137 s'est désintégré, soit en un élément stable, soit en un autre élément radioactif qui se désintègrera à son tour. Au bout de deux périodes, la moitié de la moitié du fragment d'origine sera devenue stable.
Cette durée peut varier considérablement d'un isotope à l'autre, comme le montre ces quelques exemples suivants :
Technétium 99m,6 heures ; Iode 123 ;13 heures ; Thallium 201, 73 heures ; Tellure 132, 78 heures ; Iode 131, 8 jours ; Césium 134, 2.2 ans ; Tritium, 12.3 ans ; Plutonium 241, 13.2 ans ; Césium 137, 30.2 ans ; Uranium 238, 4,5 milliards d'années

Les concepts de dose

Les effets que peuvent provoquer les rayonnements ionisants sur la santé dépendent de plusieurs paramètres :

- la **dose d'irradiation**, c'est-à-dire la quantité d'énergie transmise par les rayonnements dans l'organe ou le tissu touché ;
- la **nature du rayonnement** (X, gamma, alpha notamment) ;
- les **modalités d'exposition** (interne - par ingestion notamment - ou externe) ;
- l'**organe ou le tissu atteint** (poumons, peau...).

Différents concepts de dose sont utilisés pour comprendre l'impact de multiples rayonnements sur de multiples types de tissus ou d'organes.
Tout d'abord, on calcule la **dose absorbée** (en Gray, Gy). Ensuite, pour prendre en compte l'influence de deux paramètres - le type de tissu ou d'organe touché et le type de rayonnement – on calcule deux doses :

- la première, appelée **dose équivalente** (en Sievert, Sv), prend en compte le type de rayonnement. Elle est calculée en multipliant la dose absorbée par un facteur dépendant du type de rayonnement (X, gamma...) ;
- la seconde, appelée **dose efficace,** prend en compte le type de tissu ou d'organe touché.

Ainsi on peut déterminer l'impact d'un type de rayonnement sur un type de tissu ou d'organe touché. Seule la dose absorbée est mesurée, les autres - dose équivalente et dose efficace - sont calculées.
Exprimée en Gray (Joules/kg), la « dose absorbée » représente l'énergie cédée par le rayonnement à l'organisme ou à un objet qu'il rencontre.
Dans le cas d'une irradiation aigue localisée à un organe ou tissu (par exemple la peau), on sait que pour une dose absorbée de plus de 1 Gy, des rougeurs apparaissent. Pour une dose supérieure à 5 Gy, la peau devient brulée.
Autorité de Sûreté Nucléaire (ASN) - 11/08/2009

DOCUMENT N°2

Autorité de Sûreté Nucléaire (ASN), 11/08/2009

L'ASN et la Polynésie française signent une convention de coopération pour le contrôle de la radioprotection des installations médicales utilisant des rayonnements ionisants

Note d'information

André-Claude Lacoste, Président de l'Autorité de sûreté nucléaire (ASN), et Oscar Temaru, Président de la Polynésie française, ont signé le 8 juillet 2009 une convention de coopération. Celle-ci prévoit que l'ASN apportera son concours et son expertise aux autorités polynésiennes pour le contrôle de la radioprotection des installations médicales utilisant des rayonnements ionisants.

La Polynésie française est responsable du contrôle de la radioprotection sur son territoire. La Polynésie française et l'ASN ont décidé de coopérer afin d'améliorer le contrôle de la radioprotection des installations de Polynésie utilisant des rayonnements ionisants à visée diagnostique ou thérapeutique (radiologie, médecine nucléaire, radiothérapie). La signature de cette convention intervient au moment où le Centre hospitalier de Polynésie française à Papeete se dote d'un nouveau service de radiothérapie.
Cette coopération prévoit quatre domaines prioritaires d'action :
- l'élaboration de la réglementation relative à la radioprotection en Polynésie française. L'ASN donnera son avis au gouvernement polynésien sur les projets de décret et d'arrêté ministériel et sur les décisions réglementaires à caractère technique ;

- la vérification du respect des règles et des prescriptions auxquelles seront soumises les installations médicales polynésiennes utilisant des rayonnements ionisants. L'ASN apportera son appui technique aux autorités polynésiennes en charge du contrôle de ces installations ;

- la participation à l'information du public ;

- l'assistance aux autorités polynésiennes en cas de situation d'urgence : l'ASN adressera en particulier à l'autorité compétente ses recommandations sur les mesures à prendre sur les plans médical et sanitaire.

La division de Paris de l'ASN sera chargée d'assister les autorités polynésiennes pour le contrôle des activités médicales. Une première mission, consacrée notamment au contrôle du Centre hospitalier de Polynésie française, interviendra avant la fin de l'année 2009.

L'ASN est une autorité administrative indépendante créée par la loi n° 2006-686 du 13 juin 2006 relative à la transparence et à la sécurité en matière nucléaire (loi TSN). Elle a notamment pour mission d'élaborer et de contrôler l'application de la réglementation de la radioprotection et de participer à l'information du public. La Polynésie française est un pays d'outre-mer bénéficiant d'une large autonomie politique. Elle compte plus de 250 000 habitants, répartis dans 5 archipels (118 îles au total dont 80 sont habitées) et s'étend sur une zone aussi vaste que l'Europe. La Polynésie française est compétente en matière de contrôle de la radioprotection notamment en application de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie française et de l'article 14 de la loi n° 2004-193 du 27 février 2004 complétant le statut d'autonomie de la Polynésie française.

Date de la dernière mise à jour : 03/09/2021

DOCUMENT N°3

Centre Hospitalier de la Polynésie française (CHPF), 20/03/2023

La médecine isotopique

Depuis juillet 2016, le CHPF permet aux patients polynésiens d'avoir accès à une nouvelle technologie d'imagerie sur un appareil dénommé Gamma caméra, permettant de réaliser des diagnostics d'une grande précision, notamment en matière de pathologies cancéreuses, cardiaques, infectieuses et rénales.
Ce service permet également de mettre en place des traitements des pathologies thyroïdiennes à base d'iode 131. (Irathérapie) Les examens étaient auparavant effectués en Nouvelle-Zélande ou en métropole, mais grâce à l'ouverture de ce service, les Polynésiens n'auront plus à partir pour les réaliser.
Les évacuations sanitaires ainsi évitées permettent un financement partiel, dans sa phase de lancement, du fonctionnement du service de médecine isotopique.
La mise en place de l'unité a nécessité une autorisation de la Direction de la Santé pour cet équipement lourd et a demandé un très gros travail d'organisation et de procédures. Il s'agissait d'assurer la sécurité, la qualité des diagnostics et des traitements et la radioprotection pour les patients, le personnel et l'environnement.
Le service de médecine isotopique du CHPF est unique dans le Pacifique insulaire.

LE CHEF DE SERVICE est Dr Philippe- Emmanuel Dupire.
L'équipe est composée :
– d'un médecin isotopiste, Professeur Olivier-François Couturier,
-de radio pharmaciens, Tumatarii Cross et François Gonnet,
-d'un cadre de santé, Joël, Patea Anania
-de préparateurs en pharmacie, Teheva Mariteragi et Jean-Marie Tehahe,
-de deux manipulateurs d'électroradiologie, Albane Banzouzi et Céline Torrado,
-d'un physicien médical, Bruno Tchong Len
-et d'une secrétaire, Maiana Chanzy.

TECHNIQUE (imagerie/diagnostic/traitement)
Les isotopes (différentes formes d'un même atome) émettent des radiations permettant de réaliser des images médicales (rayons X, rayons gamma) ou de soigner (radiothérapie interne).
Les isotopes utilisés en médecine isotopique sont généralement couplés à un médicament. (On parle de médicament radiopharmaceutique) pour faire des images d'organes appelées scintigraphies. (scintigraphie des os, du cœur, des poumons, des reins...)
Grâce à cette technique, l'organe devient lui-même émetteur de lumière gamma et cela permet d'obtenir une image de son fonctionnement ou de son métabolisme.
Par ailleurs, l'irathérapie (administration de l'iode 31) permet de traiter à l'échelle cellulaire et moléculaire des lésions cancéreuses (radiothérapie interne sélective)
Le principe de la médecine isotopique consiste en l'administration au patient d'une très petite quantité de radio pharmaceutique (dose traceuse), généralement par voie veineuse.
Il s'agit d'une imagerie médicale par émission de rayon gamma par l'organe étudié.
Ce procédé est très différent du diagnostic par rayons X (radiologie standard et scanner) où le rayonnement est externe et traverse le corps pour former une image morphologique.
On comprend donc que l''imagerie isotopique est une imagerie en 3D de la fonction de l'organe alors que la radiologie (et notamment le scanner) fournit des informations sur l'anatomie.

DOCUMENT N°4

Centre National de la Recherche Scientifique (CNRS), 01/01/2018

Les cahiers de prévention • Guide Risques radioactifs et Radioprotection

1. Réglementation relative aux rayonnements ionisants

La transposition de la directive 96/29/Euratom du 13 mai 1996 avait introduit des modifications importantes dans la réglementation française relative aux rayonnements ionisants. Elle a induit la parution de nombreux textes concernant d'une part l'organisation de la radioprotection et d'autre part la protection des personnes contre les dangers présentés par les rayonnements ionisants.

Cette directive et la réglementation française qui en découle traduisent et mettent en œuvre les recommandations et principes définis par la commission internationale de protection radiologique (CIPR), dans sa publication n° 60.

La loi 2006-686 du 13 juin 2006 relative à la transparence et à la sécurité nucléaire, dite loi TSN, a créé une autorité de sûreté nucléaire (ASN), autorité administrative indépendante.

L'ASN assure, au nom de l'État, le contrôle de la sûreté nucléaire et de la radioprotection en France pour protéger les travailleurs, les patients, le public et l'environnement des risques liés aux activités nucléaires. Elle est également chargée de l'information des citoyens dans ces domaines.

L'ASN a notamment pour missions :

• de contribuer à l'élaboration de la réglementation en prenant des décisions réglementaires à caractère technique ;

• de vérifier le respect des règles et prescriptions auxquelles sont soumises les installations et activités. L'ASN dispose de pouvoir d'injonction et de sanction. Ce contrôle s'exerce sur toutes les activités nucléaires civiles (y compris les opérations de transport) comportant un risque d'exposition des personnes aux rayonnements ionisants émanant soit d'une source artificielle, soit d'une source naturelle ;

• d'assister le gouvernement en cas de situation d'urgence ;

• d'instruire les dossiers de demande d'autorisation relatifs à la fabrication, la détention et l'utilisation de sources de rayonnements ionisants utilisés à des fins médicales, industrielles ou de recherche.

Elle s'appuie sur un organisme d'expertise et de recherche, l'institut de radioprotection et de sûreté nucléaire (IRSN).

Pour ces deux organismes, les missions qui concernent les activités et les laboratoires de recherche sont :

• pour l'IRSN (décret 2016-283 du 10 mars 2016) :

- la gestion de l'inventaire des sources radioactives et de leurs mouvements,

- le contrôle des matières nucléaires,

- la gestion et l'exploitation des données dosimétriques des travailleurs,

- la surveillance radiologique de l'environnement,

• pour l'ASN (loi TSN) :

- la délivrance des autorisations de détention et d'utilisation de sources de rayonnements ionisants,

- l'inspection et le contrôle de l'organisation de la radioprotection, du transport des matières radioactives et de la gestion des déchets radioactifs.

Les textes traitant de la protection des personnes et des travailleurs contre les dangers résultant de l'exposition aux rayonnements ionisants sont principalement :

• l'ordonnance 2001-270 du 28 mars 2001 relative à la transposition de directives communautaires dans le domaine de la protection contre les rayonnements ionisants.

• le décret 2002-460 du 04 avril 2002, relatif à la protection générale des personnes contre les dangers des rayonnements ionisants, complété par le décret 2003-462 modifié par le décret 2007-1582 (articles R. 1333-1 à R. 1333-112 du Code de la santé publique).

• les décrets 2003-296 du 31 mars 2003 et 2007- 1570 du 05 novembre 2007, relatifs à la protection des travailleurs contre les dangers des rayonnements ionisants (articles R. 4451-1 à R. 4451-144 du Code du travail).

• différents arrêtés d'application parmi lesquels :

- l'arrêté du 17 juillet 2013 relatif au suivi médical et à la dosimétrie des travailleurs,

- l'arrêté du 06 décembre 2013 modifié, relatif à la formation de la personne compétente en radioprotection,

- l'arrêté du 21 mai 2010 relatif aux contrôles de radioprotection,

- l'arrêté du 15 mai 2006 modifié, relatif aux conditions de délimitation et de signalisation des différentes zones.

Des décisions ASN homologuées ainsi que différents guides techniques complètent ce dispositif. Les dispositions inscrites dans ces réglementations sont développées dans le présent guide.

L'annexe 1 présente la liste des principaux textes applicables aux activités nucléaires développées par les organismes de recherche.

Avertissement

> Cette réglementation est appelée à évoluer prochainement (2018) afin de prendre en compte les dispositions de la directive 2013/59/EURATOM du Conseil du 5 décembre 2013 fixant les normes de base relatives à la protection sanitaire contre les dangers résultant de l'exposition aux rayonnements ionisants et abrogeant les directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom et 2003/122/Euratom.

> Cette directive prend en compte les dernières recommandations publiées par la CIPR en 2007 (publication 103). Une partie de cette directive a d'ores et déjà été transcrite en droit français par l'ordonnance 2016-128 du 10 février 2016 portant diverses dispositions en matière nucléaire. Elle induit des modifications aux Codes de la santé publique, de l'environnement, du travail et de la défense.

La Présidence de la Polynésie française, 01/02/2020

Centre Médical de Suivi

des anciens travailleurs civils et militaires
des sites du centre d'expérimentation du Pacifique
et des populations vivant ou ayant vécu à proximité de ces sites

---

Conséquences Sanitaires des Essais Nucléaires Français dans le Pacifique

Contexte

À partir de 1966, 193 essais nucléaires ont été conduits par la France en Polynésie française, dont 41 essais atmosphériques. Depuis le début des années 60, la société polynésienne a connu de profonds changements d'ordre économique, sanitaire, et concernant les modes de vie en partie liés à l'implantation du Centre d'expérimentation du Pacifique (CEP) qui était en charge de la réalisation des essais nucléaires menés par la France.
Suite au démantèlement du CEP en 1996, la Polynésie française aborde une nouvelle transition sociodémographique, tandis que la prise de conscience collective quant aux conséquences potentielles des retombées radioactives sur la santé de la population polynésienne et du personnel civil et militaire suscite des inquiétudes croissantes et motive une demande de reconnaissance en vue d'obtenir réparation.

1. Données actuelles sur les effets des rayonnements ionisants

L'exposition aux rayonnements ionisants est susceptible d'entrainer de nombreux effets sur les organismes vivants, dont la caractérisation est très variable selon le type d'exposition (externe à distance, externe au contact, interne), le niveau de dose, le type de rayonnements (X, Gamma, neutrons, Beta, etc.), la durée d'exposition (débit de dose), l'organe concerné, l'âge de l'individu, etc. Compte tenu des modalités d'exposition ayant concerné les populations polynésiennes et certains travailleurs des sites d'expérimentation (détaillé au paragraphe suivant), seuls les effets cancérogènes et transgénérationnels seront abordés.
En préambule, il convient de comprendre, sans entrer dans les détails, à quoi correspond le Sievert (Sv) permettant de caractériser la dose « efficace ». Il s'agit d'un concept dosimétrique de radioprotection qui permet d'estimer le détriment global à l'échelle de l'organisme en termes d'effets dits stochastiques[1] liés à l'ensemble des types de rayonnements impliqués par les différents organes en utilisant des facteurs de pondération en fonction de leur radiosensibilité.
Les études épidémiologiques permettent d'estimer de façon directe, dans les populations humaines, le risque sanitaire lié à leur exposition aux rayonnements ionisants. Lorsqu'elles sont de qualité suffisante (en termes de puissance, reconstitution précise et individuelle de l'exposition, prise en compte de facteurs de confusion, précision des données sanitaires) et dès lors que les résultats sont convergents, ces études épidémiologiques contribuent pour une part déterminante à fonder un jugement de causalité entre une exposition et la survenue des pathologies observées.
Les résultats de quelques études épidémiologiques majeures, effectuées sur des populations caractéristiques de plusieurs dizaines de milliers d'individus, comme celle des survivants des bombardements atomiques d'Hiroshima et Nagasaki[2], celle de travailleurs de la filière nucléaire, ou encore celle des « liquidateurs » de Tchernobyl permettent d'approcher au mieux ce qui se passe à faible ou relativement faible dose (environ 100 mSv). Concernant ce domaine des faibles doses, il est intéressant de retenir les points suivants :
- l'excès de risque estimé de décès par cancer solide pour une vie entière se situe dans les différentes cohortes autour de 50 % par Sv. Le risque est modulé par l'âge au moment de l'exposition : à dose égale, il est d'autant plus marqué que l'individu a été exposé jeune et que le débit de dose est important.

- L'excès de risque est variable selon le type d'organe concerné, permettant ainsi de classer les cancers par catégories selon leur radioinductibilité (UNSCEAR 2006) et déterminer, in fine, dans les systèmes de réparation, quels sont les cancers indemnisables. - Les évaluations internationales (UNSCEAR 2007) portant sur le risque de cancer radio-induit concluent à l'existence d'un risque avéré, croissant avec la dose, pour des doses efficaces supérieures à 100 mSv (seuil de détectabilité).
- Néanmoins, par mesure de précaution et en l'absence de données suffisamment concluantes dans le domaine des très faibles doses (0-100 mSv), la Commission Internationale de Protection Radiologique suggère l'utilisation d'une relation dose-réponse sans seuil. Si l'on retient cette hypothèse, toute dose, même minime, est porteuse d'excès de risque. Les recommandations de gestion du risque radiologique sont fondées sur ce principe probabiliste.
- Les cancers radio-induits ne possèdent aucune spécificité, et il n'existe à ce jour aucun marqueur permettant d'estimer avec certitude un lien de causalité entre une dose reçue et l'apparition d'une telle pathologie. Autrement dit, aux faibles doses, il n'est pas possible d'affirmer qu'un cancer est dû aux rayonnements.

2. Conséquences sanitaires immédiates liées aux retombées des essais nucléaires

Estimation des doses reçues par les populations

Selon le ministère de la Défense (2006)[3], la population de la Polynésie française a été exposée aux rayonnements ionisants principalement suite aux essais d'Aldébaran (2 juillet 1966), Rigel (24 septembre 1966), Arcturus (2 juillet 1967), Encelade (12 juin 1971), Phoebe (8 août 1971) et Centaure (17 juillet 1974). Les zones les plus affectées par les retombées radioactives ont été les îles Gambier, Tureia et Tahiti. Les reconstructions de doses portent sur les populations de ces zones.
Les estimations de doses disponibles sont celles réalisées par les autorités françaises et celles effectuées dans le cadre d'une étude épidémiologique indépendante menée par l'Inserm[4] . Les rapports publiés par les autorités françaises, présentant le système de surveillance et les doses estimées sur chacun des sites, ont fait l'objet d'une évaluation par un groupe d'experts indépendants mandatés par l'AIEA (International Atomic Energy Agency).
Sur le plan des effectifs concernés, on estime à 2000 habitants de Mangareva, Reao, Pukarua et Tureia dont 600 enfants de moins de 15 ans, qui auraient pu dépasser le seuil de 5 mSv de 1966 à 1974. Il convient d'ajouter 8000 personnes dans la zone de Tahiti (côte Est et presqu'île de Taravao).[5]

En 2019, des estimations de doses ont été réalisées par l'IRSN dans le cadre d'une étude sollicitée par le CIVEN (Comité d'indemnisation des victimes des essais nucléaires). Il s'agit d'une évaluation des doses efficaces consécutives aux retombées des essais atmosphériques, potentiellement reçues par les populations polynésiennes ayant résidé à Tureia, aux îles Gambier et sur quatre communes de Tahiti, entre 1975 et 19816
. Cette étude repose d'une part sur l'analyse des données des rapports annuels établis de 1974 à 1981 par le Service mixte de contrôle biologique (SMCB) de la Direction des centres d'expérimentations nucléaires (DIRCEN) pour la surveillance des denrées alimentaires (ces rapports initialement classés Confidentiels Défense, ont été déclassifiés par décret en 2013) et, d'autre part, sur des mesures de terrain réalisées en 1982 et entre 2017 et 2018. Pour la période 1975-81, les nouvelles estimations de doses efficaces annuelles chez les sujets adultes sont comprises entre 18 et 68 µSv. Pour les enfants, les doses efficaces totales estimées sont pour la plupart très proches de celles des adultes. Pour la classe d'âge des 12-17 ans ayant résidé à Tahiti, les valeurs peuvent être légèrement supérieures à celles des adultes, mais n'excèdent pas 49 µSv/an. Après 1981, les doses efficaces annuelles diminuent progressivement pour atteindre au milieu des années 1990 des valeurs inférieures à 10 µSv/an, mis à part un effet notable en 1987 des denrées importées de l'hémisphère nord et marquées par les retombées de l'accident de Tchernobyl. Ces valeurs prennent en compte également les retombées de l'ensemble des essais nucléaires atmosphériques, sans pouvoir

distinguer leurs contributions respectives. À partir du milieu des années 1980, ces estimations de doses ne sont plus exclusivement liées aux retombées globales des essais nucléaires en Polynésie française, mais aux principaux radionucléides artificiels présents dans les denrées consommées en Polynésie, quelles que soient leurs origines (locales ou importées).

Il est important de noter que d'une manière générale, les estimations rétrospectives qui ont été réalisées montrent que les doses reçues par les populations polynésiennes exposées aux retombées de l'ensemble des 43 essais nucléaires aériens sont de l'ordre du mSv et de l'ordre de quelques mGy à quelques dizaines de mGy pour la dose à la thyroïde, soit environ 10 fois inférieures à celles reçues par les populations exposées aux retombées des essais nucléaires réalisés dans le Nevada par les ÉtatsUnis et d'environ 100 fois inférieures à celles reçues par les populations exposées aux retombées des essais nucléaires réalisées par l'URSS dans le Kazakhstan.

Estimation des doses reçues par les travailleurs Les doses reçues par le personnel civil et militaire, présent sur les sites d'essai, sont issues d'expositions externes et internes, les premières étant déterminées principalement par les dosimètres individuels (300000 résultats archivés) et les secondes estimées par anthropogammamétries ou par analyses d'échantillons biologiques (154000 résultats enregistrés). Les doses d'expositions externes les plus élevées (supérieures à 50 mSv) ont été enregistrées pour le personnel de l'aviation militaire et ne concernent que 8 personnels. Les doses de contamination interne varient de quelques dizaines de µSv à 30 mSv. Concernant les travailleurs polynésiens, selon le rapport du Comité de Liaison pour la Coordination du Suivi Sanitaire des Essais Nucléaires Français (CSSEN) de mai 2007, sur 16 000 personnes identifiées comme ayant participé aux essais, 345 travailleurs ont reçu des doses cumulées supérieures à 5 mSV.

Pathologies liées à la Ciguatera

Il paraît important de rappeler le rôle de cette intoxication lié à la consommation de certains produits de la mer au cours des campagnes de tirs, notamment souterrains. Plusieurs études7 ont montrées que les explosions souterraines s'accompagnaient d'une augmentation significative de cette pathologie polymorphe. De nombreux travailleurs polynésiens, grands consommateurs de poissons, attribuent souvent les symptômes de cette maladie avec ceux d'une éventuelle contamination par des radioéléments. Une enquête récente menée auprès de 454 vétérans montre que cette perception semble être liée à un défaut d'information à l'époque de leur activité sur les sites d'expérimentation.

3. Données actuelles sur les conséquences sanitaires à long terme des essais nucléaires en Polynésie française

En septembre 1996, le Président Jacques Chirac a commandité une étude auprès de l'agence internationale de l'énergie atomique (AIEA) sur la situation radiologique des atolls de Moruroa et Fangataufa ainsi que de leurs lagons. Cette étude réalisée à l'issue de l'ultime campagne française d'expérimentations nucléaires, concluait :

- « ...qu'aucun groupe de population n'est susceptible, à un moment futur quelconque, de recevoir une dose attribuable aux matières radioactives résiduelles présentes à Mururoa et à Fangataufa qui soit supérieure à environ 1 % de la dose due au fond de rayonnement que ce groupe recevra inévitablement du fait des sources naturelles de rayonnements ».
- « ...qu'il n'y aura aucun effet sur la santé qui puisse être diagnostiqué médicalement chez un individu ou décelé dans un groupe par des études épidémiologiques et qui serait attribuable aux doses de rayonnements estimées qui sont reçues actuellement ou qui seraient reçues à l'avenir par des personnes du fait des matières radioactives résiduelles présentes à Mururoa et à Fangataufa ».

- « ...qu'aux très faibles niveaux de doses estimés dans celle-ci il n'y aura aucune modification des taux d'incidence du cancer dans la région qui soit attribuable à l'exposition aux rayonnements provoquée par les matières radioactives résiduelles présentes à Mururoa et à Fangataufa»

Pathologies cancéreuses

Données épidémiologiques publiées

En dépit de ces conclusions, et en application du principe de précaution, plusieurs études épidémiologiques sur les conséquences sanitaires des essais nucléaires ont été menées par l'INSERM en Polynésie française sous l'égide des académies des sciences et de médecine. Ces études, dirigées par Florent de Vathaire, aboutissent de façon globale aux résultats suivants :

- L'incidence globale des cancers en Polynésie française sur la période 1985-95 (étudiée) est identique à celle de la population hawaiienne mais plus faible que celle de la population Maori de Nouvelle-Zélande sur la période 1987-92 ;
- La principale découverte de cette étude est la faible incidence des cancers digestifs en Polynésie française comparée à celle de Hawaii et des Maoris de NZ ;
- Il existe un risque significativement plus élevé de cancer de la thyroïde en Polynésie française (pour les deux sexes) comparé aux deux autres populations de référence.

Il est également rappelé dans ces études que le Pacifique est une région à haut risque pour le cancer de la thyroïde, sachant que le taux le plus élevé de cancer de la thyroïde a été mis en évidence en Nouvelle-Calédonie chez les mélanésiennes sur la période 1985-92 (34 pour 100 000 hab.). A ce jour, les causes exactes qui entrainent l'accroissement du risque de cancer de la thyroïde dans l'ensemble de la région du Pacifique ne sont pas connues. Néanmoins, l'âge de la première grossesse, le nombre de grossesses, l'obésité et l'apport alimentaire en iode sont jugés significatifs dans l'approche de ce risque chez la femme.

En revanche, à aucun moment, une incidence plus élevée de leucémies en Polynésie française n'est rapportée dans les différentes études.

L'impact sanitaire des essais nucléaires français en Polynésie française n'est cependant pas nul, et si aucune augmentation significative des pathologies cancéreuses ne peut être rattachée aux retombées radioactives des essais aériens, la modification des habitudes alimentaires, la sédentarité et la perturbation du mode de vie traditionnel de la société polynésienne a aujourd'hui encore de graves conséquences en terme de santé publique (obésité, diabète, maladies cardio-vasculaires, maladies métaboliques...).

Les études descriptives n'incluent pas d'informations individuelles sur certains facteurs de risque présumés, y compris une possible exposition aux rayonnements ionisants, et ne peuvent donc pas permettre d'établir la (ou les) raison(s) de l'augmentation de l'incidence du cancer de la thyroïde en Polynésie française.

En pratique, la présence d'un « cluster » de cancers thyroïdiens focalisés au niveau des îles soumises à des retombées lors des tirs aériens, et notamment aux Gambier, laisse peu de doute sur le rôle des rayonnements ionisants, et notamment de l'exposition thyroïdienne à l'iode radioactif, dans la survenue de cet excès de cancers.

Données récentes du Registre des Cancers

Les statistiques actuelles du cancer en Polynésie française, exposées lors du dernier Comité de Pilotage du Plan Cancer en octobre 2019, et non encore officiellement publiées, présentent un travail de comparaison entre les données de 2015 de ce registre et les données internationales (Globocan) de 2012.

On en retient les points suivants :

DOCUMENT N°5

- 749 nouveaux de cancers en Polynésie en 2015, dont les âges médians au diagnostic sont respectivement de 58 ans chez la femme et 65 ans chez l'homme. A noter qu'un cancer sur 3 chez la femme survient avant 50 ans (32%).
- Il n'existe pas de différence significative entre les 5 archipels dans la distribution géographique des cas déclarés.
- En ce qui concerne les taux d'incidence standardisés (méthode de calcul du nombre de nouveaux cas annuels pour 100 000 personnes, dans lequel la standardisation permet de gommer l'effet des tranches d'âges), on retient 255,7 cas chez l'homme et 238.8 chez la femme. A titre de comparaison, chez l'homme : 373 en Australie, 356 en métropole, 298 en Nouvelle Calédonie. Chez la femme : 278 en Australie, 261,9 en métropole, 270 en Nouvelle Calédonie.

Ainsi, on ne relève pas d'excès significatif de cancers déclarés en 2015 en Polynésie française par rapport à la plupart des pays étudiés en 2012.

- Concernant la répartition de l'incidence des cancers par organe, on note que chez l'homme les 3 premiers cancers sont les mêmes qu'en métropole (prostate/poumon/colorectal), mais avec des taux d'incidence plus faibles. Chez la femme, le cancer du sein apparait en tête comme ailleurs (40% des cancers). En revanche, les polynésiennes souffrent plus du cancer du poumon et de la thyroïde, et moins des cancers digestifs. Pour mémoire, la forte prévalence des cancers thyroïdiens est également retrouvée dans les autres populations du Pacifique (Nouvelle Calédonie). Au niveau du cancer broncho-pulmonaire, la situation est assez préoccupante car on note une mortalité particulièrement élevée chez des femmes jeunes. Près de 50% des cancers évitables (avant l'âge de 50 ans) sont des cancers du poumon en Pf.

La tenue du registre des cancers en Polynésie permet de relever un taux moyen de déclaration de 3.3 sources déclarantes par cancer diagnostiqué (médecin anatomopathologiste, oncologue, médecin traitant, etc...), ce qui est un bon indicateur de qualité dans l'exhaustivité du recueil des données.

Néanmoins, ce registre du cancer en Polynésie fait l'objet de nombreuses critiques et reste sujet à caution. En effet, selon les spécialistes de l'INSERM, il est indispensable que la Polynésie française se dote d'un état des lieux exhaustif, fiable et pérenne du nombre de cas de cancer de ses résidents, avec une description spatiale et temporelle précise par localisation de cancer. Le registre des cancers doit donc rapidement réobtenir puis maintenir au cours du temps sa qualification auprès des instances nationales (telles que le Comité d'évaluation des registres, ou CER). Cela suppose qu'il puisse avoir accès à toutes les sources de données existantes pour permettre des notifications exhaustives des cas et leur confirmation histologique, et qu'il dispose des ressources humaines suffisantes. Par ailleurs, le registre des cancers doit :

- suivre les guidelines françaises et internationales ;
- collaborer étroitement avec le réseau Francim[8] qui rassemble l'ensemble des registres de cancer du territoire français ;
- publier ses résultats dans des revues scientifiques à comité de lecture ;
- effectuer des comparaisons nationales et internationales en participant à des projets de recherche et de surveillance, collaborer avec les registres internationaux de la zone Pacifique.

Un tel registre des cancers pourra permettre la mise en place d'études étiologiques.

Un tel dispositif ne peut s'obtenir que si le registre peut travailler en toute transparence et indépendance : il pourrait par exemple se doter d'un conseil scientifique indépendant, apte à valider et orienter ses travaux. À noter que la Polynésie française est maintenant le seul territoire d'Outremer qui ne dispose pas d'un registre de cancer qualifié, à l'exception de Mayotte (et des tous petits territoires comme Wallis et Futuna et Saint-Pierre et Miquelon).

Etudes concernant les travailleurs

Le ministère de la défense, par l'intermédiaire de l'observatoire de la Santé des Vétérans (OSV) a fait réaliser une étude épidémiologique de mortalité sur une cohorte d'anciens travailleurs des essais nucléaires (étude Sépia-santé) originaire de métropole. Cette étude portant sur 26 000 individus, ne

montre pas d'excès de mortalité par maladies radio-induites (cancers) par rapport à la population générale. Ces données, datant de 2009, sont actuellement en cours de réactualisation par l'OSV et sont complétées par une étude de morbidité par le biais des affections de longue durée dans cette cohorte.
Une analyse épidémiologique de la cohorte du Centre Médical de Suivi est en cours grâce aux données collectées depuis 2007 sur 8732 visites réalisées jusqu'au 1er avril 2019. Cette étude se fixe comme objectif de décrire l'état de santé de 2078 travailleurs suivis depuis 2007. L'analyse concerne les mesures biométriques, la mortalité, la morbidité en affections de longue durée et les données liées à la descendance de ces vétérans polynésiens des sites d'expérimentation (fausses couches, malformations à la naissance, sex ratio).

Pathologies non cancéreuses

Le suivi épidémiologique sur le long terme de certaines populations citées précédemment (survivants des bombardements japonais, travailleurs du nucléaire, etc.) révèle l'apparition d'effets non létaux, non cancérogènes, qui se traduisent par un vieillissement accéléré de tissus spécifiques. C'est le cas notamment des cataractes et des effets cardiovasculaires. Toutefois, la Commission internationale de protection, radiologique (CIPR), dans sa publication n°107, considère que le caractère radio-induit de ces affections n'est évident que pour des doses supérieures à 0,5 Gy (500 mSv). Ainsi, dans le cas des expositions liées aux essais nucléaires en Polynésie française, majoritairement inférieures à 30 mSv, ce champ de pathologies ne peut scientifiquement pas être pris en compte dans un dispositif de réparation.

4. Effets sur la descendance ou effets « transgénérationels »

Les effets transgénérationnels sont les effets observés dans la descendance après irradiation d'un ou des deux parents avant la conception. De vives préoccupations ont été soulevées en Polynésie suite à la publication de certains travaux[9] très contestables sur le plan médical et scientifique[10].
Il convient de rappeler l'état actuel des connaissances scientifiques, validées par les institutions internationales concernant l'occurrence de conséquences transgénérationelles suite à une exposition préconceptionnelle aux rayonnements ionisants.
L'existence de ces effets est démontrée chez les animaux, notamment chez la souris, à des doses élevées (>500 mSv).
Chez l'homme, un grand nombre d'études ont porté sur le risque de malformations congénitales et de cancers à la suite d'une exposition préconceptionnelle. Ces études ont principalement été menées sur les descendants de survivants des bombardements d'Hiroshima et Nagasaki, de travailleurs de l'industrie nucléaire, et de survivants d'un cancer traités par radiothérapie. Bien que portant sur des milliers de cancers et de malformations congénitales observés après irradiation, ces études n'ont pas mis en évidence de corrélation entre l'irradiation préconceptionnelle et le risque de survenue de ces pathologies et malformations chez les descendants d'individus exposés. Étant donné le nombre de sujets et le niveau des doses, et par conséquent la puissance statistique, ainsi que la diversité du type d'irradiation dans ces études, ces résultats peuvent être considérés comme fiables.
Les études menées par la Radiation Effects Research Foundation[11] sur les enfants de survivants des bombardements d'Hiroshima et Nagasaki entre 1946 et 2009 sont particulièrement éloquentes dans ce domaine. Basées sur le suivi de plus de 70 000 enfants, nés de parents ayant reçus des doses moyennes entre 250 et 360 mSv, elles concluent à l'absence de relation entre la dose de radiation reçue par l'un des parents ou les deux parents et le risque de malformations, le décès par cancer, l'apparition de pathologies cardiovasculaires et métaboliques dans la descendance de ces survivants.
Des études à caractère génétiques (recherche d'anomalies chromosomiques et de mutations génétiques spécifiques de cellules germinales) menées chez des patients ayant reçus de fortes doses aux gonades à l'occasion de radiothérapie ou des travailleurs de l'industrie électro-nucléaire ne

montrent pas d'augmentation significative de ces anomalies en comparaison à un groupe témoin non irradié.

Données sur les malformations congénitales en Polynésie française

La question des malformations congénitales en Polynésie est associée à la problématique des effets transgénérationnels des rayonnements ionisants.
Il n'existe pas encore de registre des malformations et la principale source de données provient du CHPF (dépistage anténatal (échographie lors des grossesses) et le suivi post-natal). La centralisation des accouchements et notamment des grossesses pathologiques vers le CHPF renforce l'exhaustivité des données collectées par les praticiens hospitaliers.
Selon les données du Dr Besnard, et malgré une inter-comparaison avec la métropole difficile à faire (faible nombre de cas, méthodes de recensement différentes), il n'existe pas d'augmentation des 21 malformations étudiées en Polynésie française (prévalence en Pf 3.3% vs 3.5% en France).

Aujourd'hui, la littérature scientifique internationale ne mentionne aucune preuve d'effets transgénérationnels pour des doses inférieures au Sv, ce qui réduit drastiquement la probabilité de transmission pour des doses de l'ordre du mSv, comme c'est le cas pour les retombées des essais nucléaires en Polynésie française.
D'autre part, l'absence de registre des malformations, les effectifs modestes de la population polynésienne, le niveau faible des doses auxquelles les populations et la majorité des travailleurs ont été soumises, les difficultés à définir un groupe témoin et à effectuer des reconstitutions dosimétriques individuelles, l'absence de centre de référence de recherche en santé publique et en dépistage génétique, le contexte passionnel du débat local sur cette question sont autant de limites méthodologiques à la conduite d'une étude dans ce domaine en Polynésie française.

1 Les effets stochastiques apparaissent de manière aléatoire à long terme après irradiation. Par opposition, les effets déterministes se produisent de manière certaine au-delà d'un certain seuil de dose et plus précocement. Les effets stochastiques
dépendent de nombreux facteurs : dose, nature du rayonnement (particules alpha, rayonnements bêta, gamma, X, neutrons),
faible/fort transfert d'énergie linéique, voie d'exposition (inhalation, ingestion, irradiation externe), débit de dose (dose unique,
fractionnée, chronique), partie du corps irradiée (corps entier, sensibilité, latence selon l'organe), facteurs individuels (sexe, âge,
comportements tels que le tabagisme).
2 La cohorte Life Span Study (ou LSS) suit l'état de santé de 86 600 survivants des bombardements atomiques d'Hiroshima et Nagasaki.
3 Ministère de la Défense. La dimension radiologique des essais nucléaires français en Polynésie. 2006.
4 Drozdovitch V, Bouville A, Doyon F, et coll. Reconstruction of individual radiation doses for a case-control study of thyroid cancer in French Polynesia. Health Phys 2008 ; 94 : 418-33.
5 Rapport Assemblée Nationale Calméjane du 17 juin 2009
6 IRSN. Évaluation de l'exposition radiologique des populations de Tureia, des Gambier et de Tahiti aux retombées des essais atmosphériques d'armes nucléaire entre 1975 et 1981. Rapport IRSN/2019-00498.
7 Ciguatera in the Pacific : a link with military activities, Tilman A. RUFF, The Lancet, January 28, 1989
8 Francim : France Cancer Incidence et Mortalité
9 Sueur C. Les Conséquences génétiques des essais nucléaires français dans le Pacifique, chez les petits-enfants des vétérans du
Centre d'Expérimentation du Pacifique et des habitants des Tuamotu Gambiers. Rapport, janvier 2018 : 115 p.
10 Inserm. Analyse scientifique du rapport : « Les Conséquences Génétiques des Essais Nucléaires français dans le Pacifique, chez les petits-enfants des Vétérans du Centre d'Expérimentation du Pacifique et des habitants des Tuamotu Gambiers ». Décembre 2018.
11 Fondation scientifique américano-japonaise ouverte à tous les chercheurs du monde et qui fait office de référence dans la recherche faisant suite aux bombardements d'Hiroshima et Nagasaki.

DOCUMENT N°6

Lexpol, 23/01/2023

Loi du pays n° 2023-15 du 23 janvier 2023 relative à la protection des personnes et de l'environnement contre les risques liés à l'exposition aux rayonnements ionisants
Version en vigueur au 23/01/2023 (extraits)

CHAPITRE IER - PRINCIPES GÉNÉRAUX

Article LP. 1er

Les dispositions de la présente loi du pays s'appliquent :
1° Aux activités comportant un risque d'exposition des personnes aux rayonnements ionisants lié à la mise en œuvre d'une source artificielle, qu'il s'agisse de substances ou de dispositifs, dans le cadre d'un usage industriel ou médical ;
2° Aux actions nécessaires pour prévenir ou réduire les risques dans les situations d'exposition définies à l'article LP. 3.
Les activités de recherche utilisant une source artificielle radioactive, qu'il s'agisse de substances ou de dispositifs, ne sont pas autorisées en Polynésie française, à l'exclusion de celles intéressant la médecine isotopique.

Art. LP. 2

Les activités utilisant des rayonnements ionisants satisfont aux principes suivants :
1° Le principe de justification, selon lequel une activité utilisant des rayonnements ionisants ne peut être entreprise ou exercée que si elle est justifiée par les avantages qu'elle procure sur le plan individuel ou collectif, notamment en matière sanitaire, sociale, économique ou scientifique, rapportés aux risques inhérents à l'exposition aux rayonnements ionisants auxquels elle est susceptible de soumettre les personnes ;
2° Le principe d'optimisation, selon lequel le niveau de l'exposition des personnes aux rayonnements ionisants résultant d'une de ces activités, la probabilité de la survenue de cette exposition et le nombre de personnes exposées doivent être maintenus au niveau le plus faible qu'il est raisonnablement possible d'atteindre, compte tenu de l'état des connaissances techniques, des facteurs économiques et sociétaux et, le cas échéant, de l'objectif médical recherché ;
3° Le principe de limitation, selon lequel l'exposition d'une personne aux rayonnements ionisants résultant d'une
de ces activités ne peut porter la somme des doses reçues au-delà des limites fixées par arrêté pris en conseil des ministres, sauf lorsque cette personne est l'objet d'une exposition à des fins médicales.

SECTION II - PROCÉDURE DE DÉCLARATION, D'ENREGISTREMENT ET D'AUTORISATION

Art. LP. 8

Le Président de la Polynésie française délivre un récépissé des déclarations, procède aux enregistrements et accorde les autorisations, selon les modalités fixées par la présente loi du pays et les arrêtés pris en conseil des ministres pour son application.
Le déclarant ou le titulaire d'un enregistrement ou d'une autorisation, qui peut être une personne physique ou une personne morale, est le responsable de l'activité utilisant des rayonnements ionisants.

Art. LP. 9

Si une activité utilisant des rayonnements ionisants relevant du régime de déclaration ou d'enregistrement est exercée par le même responsable dans le même établissement qu'une activité utilisant des rayonnements ionisants soumise à autorisation, une seule demande d'autorisation peut être présentée pour l'ensemble des activités. Le Président de la Polynésie française délivre, le cas échéant, une autorisation couvrant l'ensemble des activités exercées.
Les dispositions de l'alinéa précédent ne s'appliquent pas aux activités utilisant des rayonnements ionisants mises en œuvre à des fins de diagnostic médical, dentaire ou médico-légal.

CHAPITRE III - OBLIGATIONS DU RESPONSABLE

Art. LP. 26

Le responsable d'une activité utilisant des rayonnements ionisants transmet à l'Institut de radioprotection et de sûreté nucléaire, chargé de l'inventaire national des sources de rayonnements ionisants, des informations portant sur les caractéristiques des sources, l'identification des lieux où elles sont détenues ou utilisées, ainsi que les références de leurs fournisseurs et acquéreurs.

Les modalités de transmission sont définies par arrêté pris en conseil des ministres.

Art. LP. 27

Le responsable d'une activité utilisant des rayonnements ionisants met en place un système d'enregistrement et d'analyse des événements pouvant conduire à une exposition accidentelle ou non intentionnelle des personnes aux rayonnements ionisants. Ce système est proportionné à la nature et à l'importance des risques encourus.

Ces événements, lorsqu'ils sont susceptibles de porter une atteinte significative aux intérêts mentionnés à l'article LP. 6, sont déclarés, par le responsable de l'activité, à l'agence de régulation de l'action sanitaire et sociale, qui en avise l'autorité de sûreté nucléaire.

Art. LP. 28

Les événements susceptibles de conduire à une situation incidentelle grave ou les événements liés à la malveillance sont déclarés sans délai par le responsable d'une activité utilisant des rayonnements ionisants à l'agence de régulation de l'action sanitaire et sociale, qui en avise immédiatement le représentant de l'Etat en Polynésie française, le Président de la Polynésie française et l'autorité de sûreté nucléaire.

On entend par situation incidentelle grave toute situation impliquant une source de rayonnements ionisants et nécessitant une réaction rapide pour atténuer des conséquences négatives graves pour la santé, l'environnement ou les biens, ou un risque qui pourrait entraîner de telles conséquences négatives graves.

Art. LP. 29

L'accès à certaines catégories de sources mentionnées au 1° de l'article LP. 1er, le convoyage de celles-ci ou l'accès aux informations portant sur les moyens et mesures de protection mise en œuvre contre les actes de malveillance sont autorisés par le responsable de l'activité utilisant des rayonnements ionisants, qui peut demander un avis de sécurité.

Cette demande est adressée au Président de la Polynésie française qui rend son avis à la suite d'une enquête administrative.

Art. LP. 30

Les personnes qui participent à l'exercice ou au contrôle d'une activité utilisant des rayonnements ionisants ou à la préparation, à la mise en œuvre et au contrôle d'une action destinée à protéger les personnes vis-à-vis d'un risque dans la situation énoncée à l'article LP. 3, bénéficient dans leur domaine de compétence d'une information et d'une formation, initiale et continue, relative à la radioprotection.

Art. LP. 31

I - Le responsable d'une activité utilisant des rayonnements ionisants désigne au moins un conseiller en radioprotection, dans les conditions fixées par les dispositions de la loi du pays n° 2023-14 du 23 janvier 2023 susmentionnée, pour l'assister et lui donner des conseils sur toutes questions relatives à la radioprotection de la population et de l'environnement, ainsi que celles relatives aux mesures de protection collective des travailleurs vis-à-vis des rayonnements ionisants mentionnées à l'article LP. 32.

II - Le responsable de l'activité utilisant des rayonnements ionisants met à disposition du conseiller en radioprotection les moyens nécessaires à l'exercice de ses missions. Dans le cas où plusieurs conseillers en radioprotection sont désignés, leurs missions respectives sont précisées par le responsable.

Art. LP. 32

Les prescriptions, moyens et mesures visant la protection de la santé des travailleurs vis-à-vis des rayonnements ionisants pris en application de la présente loi du pays portent sur les mesures

de protection collective qui incombent au responsable de l'activité utilisant des rayonnements ionisants et de nature à assurer le respect des principes de radioprotection définis à l'article LP. 2.
Elles concernent les phases de conception, d'exploitation et de démantèlement de l'installation et, sont sans préjudice des obligations incombant à l'employeur en application de la réglementation du travail en vigueur en Polynésie française, relative à la prévention.

Art. LP. 33

Le responsable d'une activité utilisant des rayonnements ionisants ne peut acquérir de sources radioactives scellées qu'auprès d'un fournisseur de sources radioactives scellées, autorisé par l'Autorité de sûreté nucléaire et qui est tenu de récupérer, sur demande du détenteur, toute source qu'il a distribuée.

Art. LP. 34

L'acquéreur de dispositifs contenant des sources radioactives ou de générateurs de rayonnements ionisants doit s'assurer que son fournisseur lui transmette des informations adéquates sur les risques radiologiques potentiels associés à leur utilisation et sur les conditions d'utilisation, d'essai et de maintenance, ainsi qu'une démonstration que la conception permet de réduire les expositions aux rayonnements ionisants à un niveau aussi bas que raisonnablement possible.
En outre, dans le cas des dispositifs médicaux émettant des rayonnements ionisants, ces informations doivent être complétées par des informations adéquates sur l'évaluation des risques pour les patients et sur les éléments disponibles de l'évaluation des données cliniques.

CHAPITRE IV - APPLICATIONS MÉDICALES

Art. LP. 35

Sans préjudice des dispositions de la présente loi du pays, des dispositions prises en application de la réglementation du travail de la Polynésie française relative à la santé et à la sécurité au travail et de l'article 42 bis du code des douanes de la Polynésie française, les rayonnements ionisants ne peuvent être utilisés sur le corps humain qu'à des fins de diagnostic médical, de prise en charge thérapeutique, de dépistage ou de prévention.

Art. LP. 36

Le responsable d'une activité utilisant des rayonnements ionisants soumise à déclaration ou à enregistrement est soumis à une obligation de mise en place d'un processus de retour d'expérience, d'un système de déclaration interne des situations indésirables et des dysfonctionnements, et d'une organisation dédiée à l'analyse des déclarations internes et à la détermination des actions d'amélioration.
Il est également soumis à une obligation de mise en place d'analyses des pratiques professionnelles portant sur la justification des actes médicaux utilisant des rayonnements X et l'optimisation des doses délivrées aux patients.

I - Le responsable d'une activité utilisant des rayonnements ionisants soumise à autorisation est soumis à une obligation d'assurance de la qualité portant sur toutes les étapes du traitement, depuis la justification du choix de l'acte, l'optimisation des doses délivrées aux patients et jusqu'au rendu du résultat de cet acte. Cette démarche d'assurance de qualité comprend une obligation de mise en place d'un processus de retour d'expérience et d'analyses des pratiques professionnelles sur la justification des actes médicaux utilisant des rayonnements X et l'optimisation des doses délivrées aux patients.

Art. LP. 37

Les professionnels réalisant des actes de radiodiagnostic, de radiothérapie ou de médecine isotopique à des fins de diagnostic médical, de prise en charge thérapeutique, de dépistage, de prévention exposant les personnes à des rayonnements ionisants et les professionnels participant à la réalisation de ces actes et au contrôle de réception et de performances des dispositifs médicaux doivent bénéficier, dans leur domaine de compétence, d'une formation, initiale et continue, théorique et pratique, relative à l'exercice pratique et à la protection des personnes exposées à des fins médicales.
Les professionnels de santé, demandeurs d'actes de diagnostic médical utilisant des

rayonnements ionisants, doivent bénéficier d'une formation initiale et continue portant sur les risques liés aux rayonnements ionisants et sur l'application à ces actes du principe de justification mentionné à l'article LP. 2.

Art. LP. 38

Toute publicité relative à l'emploi de rayonnements ionisants dans la médecine humaine ou vétérinaire est interdite, sauf auprès des médecins, des vétérinaires et des pharmaciens.
L'autorisation de mise sur le marché des spécialités pharmaceutiques contenant des radionucléides ne peut être donnée que sous le nom commun ou la dénomination scientifique du ou des radionucléides entrant dans la composition desdites spécialités.

Art. LP. 39

Pour les applications médicales des rayonnements ionisants, lorsque l'autorisation ou l'enregistrement est délivrée à une personne morale, celle-ci désigne, pour la spécialité concernée, un médecin coordonnateur, titulaire des qualifications requises, chargé de veiller à la coordination des mesures prises pour assurer la radioprotection des patients. Dans ce cas, la demande d'autorisation ou d'enregistrement est cosignée par le médecin coordonnateur. Le changement de médecin coordonnateur fait l'objet d'une information du Président de la Polynésie française.

Art. LP. 40

Les professionnels de santé participant à la prise en charge thérapeutique ou au suivi de patients exposés à des fins médicales à des rayonnements ionisants, ayant connaissance d'un événement susceptible de porter atteinte à la santé des personnes lié à cette exposition, en font la déclaration dans les meilleurs délais à l'Agence de régulation de l'action sanitaire et sociale, qui en avise l'Autorité de sûreté nucléaire.

CHAPITRE V - CONTRÔLE ET SANCTIONS

SECTION I - CONTRÔLE ADMINISTRATIF ET MESURES DE POLICE ADMINISTRATIVE

PARAGRAPHE 1ER - CONTRÔLE ADMINISTRATIF

Art. LP. 41

Dans le cadre de leurs compétences respectives, les médecins inspecteurs, les médecins, les pharmaciens inspecteurs et les pharmaciens de l'Agence de régulation de l'action sanitaire et sociale assurent le contrôle du respect des dispositions de la présente loi du pays et des actes réglementaires et individuels pris pour son application.
Ils peuvent être assistés par des agents de tout service ou établissement de la Polynésie française, dont l'expertise est jugée nécessaire.
Les inspecteurs du travail assurent le respect des prescriptions, moyens et mesures visant la protection de la santé des travailleurs vis-à-vis des rayonnements ionisants.
Les fonctionnaires et agents chargés des contrôles sont astreints au secret professionnel conformément aux dispositions des articles 226-13 et 226-14 du code pénal.

Art. LP. 42

Les médecins inspecteurs, les médecins, les pharmaciens inspecteurs et les pharmaciens de l'agence de régulation de l'action sanitaire et sociale assurent le contrôle des dispositifs médicaux et de leur utilisation dans les applications médicales des rayonnements ionisants.

Art. LP. 43

Toute personne physique ou morale qui entre dans le champ d'application de la présente loi du pays est tenue de se soumettre au contrôle, sur pièces ou sur place, des agents chargés du contrôle. Ce contrôle porte notamment sur le respect des conditions de déclaration, d'enregistrement ou d'autorisation.

Art. LP. 44

Les fonctionnaires et agents chargés des contrôles peuvent recueillir sur convocation ou sur place les renseignements et justifications propres à l'accomplissement de leur mission.
Le secret professionnel ne peut être opposé aux agents agissant dans le cadre des pouvoirs qui leur sont conférés par le présent chapitre.

Art. LP. 45

Tout refus de contrôle ou obstacle à la réalisation du contrôle peut entraîner l'annulation de la déclaration ou le retrait de l'enregistrement ou de l'autorisation.

Le responsable de l'activité doit alors cesser son activité selon les modalités fixées à l'article LP. 25.

PARAGRAPHE II - MESURES ET SANCTIONS ADMINISTRATIVES

Art. LP. 46

Lorsqu'un agent chargé du contrôle établit un rapport faisant état de faits contraires aux prescriptions applicables, en vertu de la présente loi du pays ou des arrêtés pris pour son application, à une activité utilisant des rayonnements ionisants, il en remet une copie à l'intéressé qui peut faire part de ses observations au Président de la Polynésie française.

Art. LP. 47

Indépendamment des poursuites pénales qui peuvent être exercées, lorsqu'une activité utilisant des rayonnements ionisants fonctionne sans avoir fait l'objet de la déclaration, de l'enregistrement ou de l'autorisation requis en application de la présente loi du pays, le Président de la Polynésie française met l'intéressé en demeure de régulariser sa situation dans un délai qu'il détermine, et qui ne peut excéder une durée d'un an.

Il peut suspendre le fonctionnement de l'activité utilisant des rayonnements ionisants jusqu'à ce qu'il ait été statué sur la déclaration ou sur la demande d'enregistrement ou d'autorisation, à moins que des motifs d'intérêt général et en particulier la préservation des intérêts protégés par la présente loi du pays ne s'y opposent.

I - S'il n'a pas été déféré à la mise en demeure à l'expiration du délai imparti, ou si la demande initiale ou le renouvellement d'enregistrement ou d'autorisation est rejetée, le Président de la Polynésie française ordonne la cessation de l'activité et la remise des lieux dans un état ne portant pas préjudice aux intérêts protégés par la présente loi du pays, selon les modalités fixées à l'article LP. 25.

Elle peut faire application du II de l'article LP. 48 aux fins d'obtenir l'exécution de cette décision.

II - Sauf en cas d'urgence, et à l'exception de la décision prévue au premier alinéa du I du présent article, les mesures mentionnées au présent article sont prises après avoir communiqué à l'intéressé les éléments susceptibles de fonder les mesures et l'avoir informé de la possibilité de présenter ses observations dans un délai déterminé.

Art. LP. 48

Indépendamment des poursuites pénales qui peuvent être exercées, en cas d'inobservation des prescriptions applicables, en vertu de la présente loi du pays, aux activités utilisant des rayonnements ionisants, le Président de la Polynésie française met en demeure la personne à laquelle incombe l'obligation d'y satisfaire dans un délai qu'il détermine.

En cas d'urgence, il fixe, par le même acte ou par un acte distinct, les mesures nécessaires pour prévenir les dangers graves et imminents pour la santé, la sécurité publique ou l'environnement.

En cas d'urgence tenant à la sécurité des personnes, la suspension d'une activité utilisant des rayonnements ionisants régulièrement déclarée, enregistrée ou autorisée peut être ordonnée à titre conservatoire par le Président de la Polynésie française.

I - Si, à l'expiration du délai imparti, il n'a pas été déféré à la mise en demeure, aux mesures d'urgence mentionnées au second alinéa du I du présent article ou aux mesures ordonnées sur le fondement du II de l'article LP. 47, le Président de la Polynésie française peut arrêter une ou plusieurs des sanctions administratives suivantes :

1° Suspendre le fonctionnement de l'activité utilisant des rayonnements ionisants jusqu'à l'exécution complète des conditions imposées et prendre les mesures conservatoires nécessaires, aux frais de la personne mise en demeure ;

2° Ordonner le paiement d'une amende administrative au plus égale à 1 800 000 F CFP, versée au budget de la Polynésie française et recouvrée comme les créances non fiscales ;

3° Procéder au retrait temporaire ou définitif de l'enregistrement ou de l'autorisation, et prescrire la remise en état des lieux, selon les modalités fixées à l'article LP. 25.

Les amendes sont proportionnées à la gravité des manquements constatés.

L'amende ne peut être prononcée au-delà d'un délai de trois ans à compter de la constatation des manquements.

Les mesures mentionnées aux 1° et 2° du présent II sont prises après avoir communiqué à l'intéressé les éléments susceptibles de fonder les mesures et l'avoir informé de la possibilité de présenter ses observations dans un délai déterminé.
Le Président de la Polynésie française peut procéder à la publication de l'acte arrêtant ces sanctions, pendant une durée comprise entre deux mois et cinq ans. Il informe préalablement la personne sanctionnée de la mesure de publication envisagée, lors de la procédure contradictoire prévue à l'avant-dernier alinéa du présent II.

Art. LP. 49

En cas de retrait définitif de l'enregistrement ou de l'autorisation prononcé en application de la présente section, le Président de la Polynésie française prescrit au responsable de l'activité les conditions d'élimination à ses frais des sources radioactives et des déchets radioactifs actuels ou futurs.

SECTION II - DISPOSITIONS PÉNALES

Art. LP. 50

Les infractions à la présente loi du pays et aux actes réglementaires et individuels pris pour son application sont constatées, dans le cadre de leurs compétences respectives, par les agents commissionnés et assermentés suivants :

- les médecins, médecins inspecteurs, pharmaciens et pharmaciens inspecteurs de l'agence de régulation de l'action sanitaire et sociale ;
- les inspecteurs du travail.

Art. LP. 51

Est puni d'un an d'emprisonnement et d'une amende de 1 785 000 F CFP le fait :
1° D'exercer une activité ou d'utiliser un procédé, un dispositif ou une substance interdite en application de l'article LP. 4 ;
2° D'exposer des personnes au-delà des valeurs limites fixées par les arrêtés pris pour l'application du 3° de l'article LP. 2 ;
3° D'entreprendre ou d'exercer une activité mentionnée à l'article LP. 1er sans être titulaire de l'autorisation, sans qu'ait été procédé à l'enregistrement ou sans avoir effectué la déclaration prévue à l'article LP. 7 ;
4° D'utiliser les radiations ionisantes sur le corps humain à des fins et dans des conditions autres que celles prévues par l'article LP. 35 ;
5° De poursuivre l'exercice d'une activité utilisant des rayonnements ionisants en violation d'une mesure de cessation définitive, de retrait ou de suspension d'une activité prise en application des articles LP. 47 et LP. 48.

Art. LP. 52

Est puni de six mois d'emprisonnement et d'une amende de 890 000 F CFP le fait :
1° De ne pas se conformer à une mise en demeure prise en application des articles LP. 47 et LP. 48 ;
2° De ne pas communiquer en application de l'article LP. 26 les informations nécessaires à la mise à jour de l'inventaire national des sources radioactives.

Art. LP. 53

Le fait de faire obstacle aux fonctions des agents mentionnés aux articles LP. 41, LP. 42 et LP. 50 est puni de six mois d'emprisonnement et de 890 000 F CFP d'amende.

Art. LP. 54

Est puni de 440 000 F CFP d'amende toute publicité relative à l'utilisation de rayonnements ionisants en médecine humaine ou vétérinaire, lorsque cette publicité est dirigée vers d'autres personnes que des médecins, vétérinaires ou pharmaciens.

Art. LP. 55

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions définies à l'article LP. 54 encourent, outre l'amende suivant les modalités prévues par l'article 131-38 du code pénal, la peine d'interdiction de vente du produit dont la publicité a été faite en violation de l'article LP. 54.

CHAPITRE VI - MESURES TRANSITOIRES ET FINALES

Art. LP. 56

La mise en conformité avec les dispositions de la présente loi du pays doit intervenir dans un délai maximum de deux ans à compter de sa date de promulgation.

Art. LP. 57

Conformément à l'article 21 de la loi organique statutaire, les peines d'emprisonnement prévues par la présente loi du pays entrent en vigueur après l'adoption d'une loi d'homologation.

Jusqu'à l'entrée en vigueur de la loi d'homologation, seules les peines d'amende et les peines complémentaires sont applicables.

Art. LP. 58

Pour l'application de la présente loi du pays et des textes pris pour son application, la Polynésie française peut solliciter le soutien, par voie de convention, de l'Autorité de sûreté nucléaire et de l'Institut de radioprotection et de sûreté nucléaire.

La convention avec l'Autorité de sûreté nucléaire a notamment pour objet :

- de prévoir les modalités de son appui à la Polynésie française dans le cadre de la procédure de déclaration et d'instruction des demandes d'enregistrement et d'autorisation ;
- d'organiser les modalités de contrôle des installations ;
- d'organiser l'instruction des événements significatifs de radioprotection ;
- de prévoir les modalités d'expertise des situations et l'évaluation des risques sanitaires ;
- de prévoir les modalités d'alerte et d'appui à la Polynésie française en cas de situation incidentelle grave.

La convention avec l'Institut de radioprotection et de sûreté nucléaire a notamment pour objet de fixer les modalités de recueil des informations pour la gestion de l'inventaire national des sources de rayonnements ionisants et la gestion de la dosimétrie.

Le présent acte sera exécuté comme loi du pays.

Fait à Papeete, le 23 janvier 2023.

Santopta - 17/01/2014

La nouvelle directive 2013/59/Euratom est parue

Dr Hervé LECLET

Une nouvelle directive Euratom vient d'être publiée au Journal officiel de l'Union européenne du 17 janvier 2014. C'est la directive 2013/59/Euratom du 5 décembre 2013[1]. Elle fixe les normes de base relatives à la protection sanitaire contre les dangers résultant de l'exposition aux rayonnements ionisants.
Elle concerne toutes les situations d'exposition : des professionnels (industrie, domaine médical, production énergétique, gestion des déchets, ...), du public ou à des fins médicales. Elle traite donc de tous les aspects de la radioprotection, et pas seulement de la radioprotection en imagerie médicale.
Cependant, le domaine médical bénéficie d'un chapitre entier dédié. Cet article fait le point sur cette nouvelle directive et ses conséquences.

Rappel : les principes et l'organisation de la législation européenne et française en matière de radioprotection

Selon le traité instituant la Communauté européenne de l'énergie atomique (connu sous le nom de Traité Euratom[2]), la radioprotection est une compétence communautaire. L'Union européenne élabore donc des normes de bases uniformes (par exemple pour les expositions maximales admissibles ou pour les principes fondamentaux de surveillance aux expositions).

Depuis 1959, ces normes de base sont présentées sous la forme de directives, dites "directives Euratom" qui doivent être transposées dans le droit national de chaque Etat membre de l'Union. Elles sont périodiquement mises à jour.

Les directives européennes Euratom imposent :
- d'une part, une uniformisation des réglementations dans tous les pays de l'Union,
- d'autre part, une uniformisation de la gestion des risques civils qu'ils soient médicaux ou pas.

L'intérêt de ces uniformisations est essentiellement d'améliorer la maîtrise du risque collectif (c'est-à-dire à l'échelle de la population) ou individuel (travailleur ou patient). Ainsi, il est important de connaître tous les risques d'irradiation, qu'ils soient naturels, professionnels ou induits par un acte médical.

Comment est organisée la législation française en matière de radioprotection ?

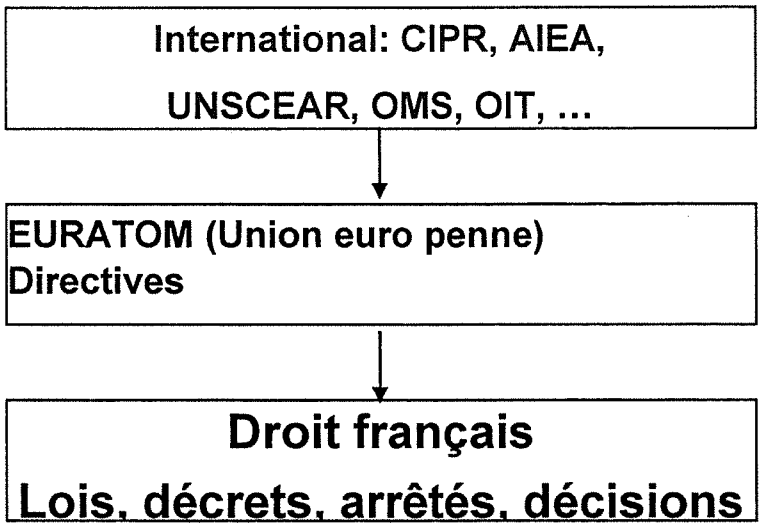
Les textes règlementaires qui organisent la radioprotection sont le résultat d'un long processus d'élaboration. Il existe une filiation logique allant des études, consensus, normes et recommandations des organismes internationaux (AIEA, UNSCEAR, CIPR, OMS, OIT, ...) aux textes internationaux puis nationaux qui réglementent la radioprotection.

---

[1] Directive 2013/59/Euratom du conseil du 5 décembre 2013 fixant les normes de base relatives à la protection sanitaire contre les dangers résultant de l'exposition aux rayonnements ionisants et abrogeant les directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom et 2003/122/Euratom. JOUE du 17 janvier 2014

[2] Traité instituant la Communauté européenne de l'énergie atomique (Traité Euratom) C 84/1Journal officiel de l'Union européenne du 30 mars 2010

Les directives Euratom reprennent les contenus de ces recommandations et les traduisent en exigences. La législation nationale française respecte les directives et les transcrit en lois, décrets, arrêtés et décisions.
Le tableau ci-dessous résume l'organisation de la législation française de la radioprotection.



Pour plus d'informations, l'IRSN a publié un dossier complet sur le sujet dans sa revue Repères en 2011[3].

Les directives Euratom fondatrices
Cinq directives Euratom sont à la base de notre législation actuelle sur la radioprotection. Par ordre chronologique de publication, ce sont :

- La directive 89/618/Euratom du 27 novembre 1989[4] concernant l'information de la population sur les mesures de protection sanitaire applicables et sur le comportement à adopter en cas d'urgence radiologique.
- La directive 90/641/Euratom du 4 décembre 1990[5], concernant la protection opérationnelle des travailleurs extérieur/s exposés à un risque de rayonnements ionisants au cours de leur intervention en zone contrôlée.
- La directive 96/29 Euratom du 13 mai 1996[6], fixant les normes de base relatives à la protection sanitaire de la population et des travailleurs contre les dangers résultant des rayonnements ionisants.
- La directive 97/43 Euratom du 30 juin 1997[7], relative à la protection sanitaire des personnes contre les dangers des rayonnements ionisants lors d'expositions à des fins médicales, remplaçant la directive 84/466/Euratom.

[3] Repères n° 11, novembre 2011, pages 9 à 1 Dossier : De l'international à la France : élaboration des normes de radioprotection. Repères n° 11, novembre 2011, pages 9 à 13
http://www.irsn.fr/FR/IRSN/Publications/Magazine-Reperes/Pages/Magazine_Reperes.aspx

[4] Directive 89/618/Euratom du Conseil, du 27 novembre 1989, concernant l'information de la population sur les mesures de protection sanitaire applicables et sur le comportement à adopter en cas d'urgence radiologique. JOCE du 07/12/1989

[5] Directive 90/641/Euratom du Conseil, du 4 décembre 1990, concernant la protection opérationnelle des travailleurs extérieurs exposés à un risque de rayonnements ionisants au cours de leur intervention en zone contrôlée. JOCE du 13/12/1990

[6] Directive 96/29/Euratom du Conseil du 13 mai 1996 fixant les normes de base relatives à la protection sanitaire de la population et des travailleurs contre les dangers résultant des rayonnements ionisants. JOCE du 29 juin 1996

[7] Directive 97/43/Euratom du Conseil du 30 juin 1997 relative à la protection sanitaire des personnes contre les dangers des rayonnements ionisants lors d'expositions à des fins médicales, remplaçant la directive 84/466/Euratom. 9 juillet 1997

- La directive 2003/122/Euratom du 22 décembre 2003[8] relative au contrôle des sources radioactives scellées de haute activité et des sources orphelines.

Ces cinq directives Euratom ont été codifiées en droit français dans le Code de la santé publique qui organise la radioprotection du public et des patients et dans le Code du travail qui organise la radioprotection des travailleurs.

La genèse de la nouvelle directive 2013/59/Euratom
La mise à jour de ces directives a débuté en 2008 en s'appuyant sur des travaux internationaux de recherche sur la radioprotection des vingt dernières années. Elle prend en compte les dernières recommandations de la Commission Internationale de Protection Radiologique publiées en 2007 (Publication ICRP 103)[9] et elle met en cohérence le cadre européen avec les nouvelles normes de base de l'Agence internationale de l'énergie atomique, publiées en 2011[10].

Le texte de la nouvelle directive Euratom a été adopte le 30 mai 2013 par la Commission Européenne et le 5 décembre par le Conseil de l'Union Européenne.
Elle a été publiée le 17 janvier 2014 au Journal officiel de l'Union européenne.
Selon le Conseil de l'Europe, cette directive représente "*un progrès appréciable en matière de radioprotection dans un large éventail de contextes*"

Le contenu synthétique de la nouvelle directive 2013/59/Euratom
La directive 2013/59/Euratom regroupe les cinq directives préexistantes dans un document unique. Elle abroge ainsi les directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom et 2003/122/Euratom.
Elle concerne tous les domaines et toutes les catégories : expositions du public, expositions de tous les professionnels et utilisation des rayonnements ionisants dans le domaine médical.
Elle fixe des normes de base uniformes relatives à la protection sanitaire contre les dangers résultant de l'exposition aux rayonnements ionisants.
Elle s'applique à toutes les situations de risques en cas d'exposition à des rayonnements ionisants, qu'elles soient planifiées, existantes ou d'urgence.
Elle confirme les concepts fondamentaux du principe de justification, du principe d'optimisation et du principe de limitation des doses de radiation pour toutes les situations d'exposition, sauf, évidemment, dans l'usage médical : les États membres de l'Union européenne doivent établir *"des exigences légales et un régime adapté de contrôle réglementaire s'inscrivant, pour toutes les situations d'exposition, dans un système de radioprotection fondé sur les principes de justification, d'optimisation et de limitation des doses".*

Elle établit le principe de la prise en compte graduée des risques liés à l'utilisation des rayonnements ionisants dans la mise en œuvre du système réglementaire

---

[8] Directive 2003/122/Euratom du conseil du 22 décembre 2003 relative au contrôle des sources radioactives scellées de haute activité et des sources orphelines. JOUE du 31/12/2003

[9] Recommandations 2007 de la Commission internationale de protection radiologique : Publication 103 : http://www.icrp.org/docs/P103_French.pdf

[10] AIEA : radioprotection et sûreté des sources de rayonnements : normes fondamentales internationales de sûreté prescriptions générales de sûreté. 2011 :

http://www- ub.iaea.org/MTCD/publications/PDF/P1531interim_LanguageVersions/p1531interim_F.pdf

Elle renforce la protection de la population vis-à-vis des sources naturelles de rayonnements ionisants, en particulier le radon.

Enfin, la directive fixe un cadre en matière d'éducation, de formation et d'information sur la protection contre les radiations ionisantes.

La radioprotection des travailleurs : quoi de neuf en pratique ?

Les limites de doses

La directive 2013/59 affirme à nouveau les contraintes de dose de la directive 96/29/Euratom, mais en y mettant des restrictions.

Elle valide le principe de la limite annuelle de dose efficace de 20 millisieverts (mSv), en remplacement de la valeur de 100 mSv sur cinq années consécutives. La limite de dose efficace pourra dans certains cas être portée à 50 mSv par an, mais sans dépasser une moyenne de 20 mSv sur 5 ans.

En droit français, ce principe est déjà mis en application depuis longtemps par le décret n° 2003-296 du 31 mars 2003[11] , dit "décret travailleurs" et les articles R.4451-10 à R.4451-14 du Code du travail qui définissent des limites de doses pour les travailleurs

: "*La somme des doses efficaces reçues ne doit pas dépasser 20 mSv sur 12 mois consécutifs* ".

En revanche, la limite de dose équivalente sur 12 mois consécutifs pour le cristallin est modifiée (Articles 9 et 11 de la directive 2013/59/Euratom). Elle passe de 150 mSv à 20 mSv par an ou 100 mSv sur 5 ans avec un maximum de 50 mSv sur une année, et à 15 mSv par an pour les apprentis de 16 à 18 ans (au lieu de 50 mSv par an).

Ainsi, les risques de cataractes seront mieux maitrisés, en particulier pour les médecins radiologues qui font beaucoup d'actes interventionnels.

Les autres limites de dose équivalente pour la peau et pour les extrémités ne changent pas : 500 mSv par an pour les professionnels et 150 mSv par an pour les "*apprentis et les étudiants de 16 à 18 ans*".

Les missions de la "personne chargée de la radioprotection" (PCR) L'article 84 de cette nouvelle directive ne fait que préciser les missions de la PCR qui doit "*superviser ou effectuer*" les tâches de radioprotection. Il n'y a pas de véritable nouveauté.

La Surveillance individuelle des travailleurs et le suivi dosimétrique

La directive impose de nouvelles modalités de surveillance individuelle des travailleurs dans son Article 41 :

"2. Les États membres veillent à ce que la surveillance radiologique des travailleurs de la catégorie B suffise au moins à démontrer que leur classement dans cette catégorie se justifie. Les États membres peuvent exiger que les travailleurs de la catégorie B soient soumis à une surveillance radiologique individuelle et, au besoin, à des mesures individuelles, réalisés par un service de dosimétrie.

---

[11] Décret n°2003-296 du 31 mars 2003 relatif à la protection des travailleurs contre les dangers des rayonnements ionisants. JORF du 2 avril 2003

3. Lorsque des mesures individuelles se révèlent impossibles à mettre en œuvre ou inappropriées, la surveillance radiologique individuelle repose sur une estimation effectuée à partir de mesures individuelles réalisées sur d'autres travailleurs exposés, à partir des résultats de la surveillance du lieu de travail prévue à l'article 39 ou sur la base de méthodes de calcul approuvées par l'autorité compétente."

"Article 39
Surveillance radiologique du lieu de travail
...
2. Les résultats de ces mesures sont enregistrés et, au besoin, servent à estimer les doses individuelles, ainsi que le prévoit l'article 41."

Aujourd'hui en France, tous les travailleurs doivent avoir un suivi dosimétrique individuel : dosimétrie active et dosimétrie passive mensuelle pour les travailleurs de catégorie A, dosimétrie passive trimestrielle pour les travailleurs de catégorie B.
Avec cette nouvelle directive, ce ne sera plus le cas pour tous. Il semble que tous les travailleurs de catégorie B n'auront plus forcément besoin d'un suivi dosimétrique individuel systématique par un dosimètre passif personnel. Mais il conviendra de préciser les conditions de mise en œuvre de ces évolutions en imagerie médicale.

L'exploitation des résultats de dosimétrique
L'article 44 de la nouvelle directive intitulé "Accès aux résultats de la surveillance radiologique individuelle" prévoit que les résultats de la surveillance dosimétrique individuelle des travailleurs seront mis à la disposition de "*l'entreprise de l'employeur*".
Cette règle est en contradiction frontale avec la règlementation française actuelle.
Les modalités d'exploitation des résultats de dosimétrie passive (dosimétrie en temps différé) et de dosimétrie active (dosimétrie en temps réel) sont détaillées dans l'arrêté du 23 mars 1999[12] et dans le décret du 2 juillet 2010[13].
Les dosimètres passifs doivent être envoyés par la PCR à l'organisme réalisant les mesures.
Selon l'article R.4451-69 du Code du travail, les résultats doivent être envoyés par l'organisme réalisant les mesures de dosimétrie sous forme nominative au travailleur et au médecin désigné par celui-ci. Ils sont également communiqués au médecin du travail. Ces résultats peuvent être communiqués au chef d'établissement de façon nominative pour la dosimétrie opérationnelle (l'employeur doit alors préserver la confidentialité de ces informations). Le chef d'établissement peut également avoir connaissance de la dosimétrie passive sous une forme excluant toute identification (art R.4451-70 du Code du travail).
Selon l'article R.4451-73 du Code du travail, les inspecteurs du travail peuvent avoir accès aux résultats dosimétriques (dosimétrie passive et dosimétrie active) de façon nominative s'ils en font la demande.
La PCR peut demander communication des résultats sous forme nominative sur une période n'excédant pas les 12 mois (art R.4451-71 du Code du travail). Si au vu des résultats, elle estime que le travailleur est susceptible de recevoir une dose supérieure

---

[12] Arrêté du 23 mars 1999 précisant les règles de la dosimétrie externe des travailleurs affectés à des travaux sous rayonnements en application des articles 20 bis et 25-1 du décret du 28 avril 1975 modifié et des articles 31 bis et 34-1 du décret du 2 octobre 1986 modifié. JORF du 28 avril 1999

[13] Décret n° 2010-750 du 2 juillet 2010 relatif à la protection des travailleurs contre les risques dus aux rayonnements optiques artificiels. JORF du 4 juillet 2010

aux limites fixées, elle doit prévenir le médecin du travail et l'employeur (art R.4451-72 du Code du travail).

Il y a donc là une contradiction entre le niveau européen et la règlementation française qui assure la confidentialité de ces données.

La radioprotection du public : quoi de neuf en pratique ?
La directive 2013/59/Euratom ne modifie pas les limites d'exposition du public aux rayonnements ionisants (1 mSv/an).
Les limites de dose équivalente restent identiques à celles de 1996. Elles sont de 15 mSv par an pour le cristallin et de 50 mSv annuels pour la peau (article 12).
Nous rappelons pour mémoire que la dose annuelle moyenne de l'irradiation naturelle en France est d'environ 2,5 mSv.

En revanche, la nouvelle directive impose d'établir un plan national d'action pour le radon (il est déjà en place en France : Plan d'actions 2011-2015 pour la gestion du risque lié au radon[14]) et de réduire le niveau de référence d'activité dans l'air de 400 Bq/m^3 à 300 Bq/m^3 (article 54).
La directive introduit également un nouveau cadre réglementaire pour contrôler la radioactivité naturelle des matériaux de construction. Cela nécessitera une nouvelle réglementation.

La radioprotection des patients: quoi de neuf en pratique ?
Les expositions à des fins médicales
Cette nouvelle directive contient un chapitre entier (chapitre VII) spécifiquement consacré aux expositions à des fins médicales.
Elle rappelle dans l'article 6 que les limites de dose ne *"s'appliquent pas aux expositions à des fins médicales"* sauf *"en ce qui concerne la protection des personnes participant au soutien et au réconfort des patients et des volontaires participant à des recherches à des fins médicales ou biomédicales"*.
Pour les patients, elle rappelle le principe ALARA (aussi bas que raisonnablement possible) et les exigences de justification et d'information pour les actes de radiologie médicale.
Les règles de justification des examens sont renforcées (article 55) : "*toutes les expositions individuelles à des fins médicales soient justifiées préalablement en tenant compte des objectifs spécifiques de l'exposition et des caractéristiques de la personne concernée*". Reste à voir comment pourra être mise en œuvre cette règle de manière pragmatique et très opérationnelle.
Le principe ALARA, les principes de l'optimisation et la mesure des niveaux de référence diagnostiques sont confirmés (article 56).

L'obligation de rédiger les procédures d'examens est confirmée, sinon renforcée : "*pour chaque type de procédure radiologique médicale courante, des protocoles écrits concernée soient établis pour chaque équipement et chaque catégorie de patients*
" (article 58).

[14] Plan d'actions 2011-2015 pour la gestion du risque lié au radon. ASN 2011 : http://www.asn.fr/Media/Files/Le-plan-national-d- actions-2011-2015-pour-la-gestion-du-risque-lie-au-radon.

Les applications médico-légales des rayonnements ionisants,
L'article 22 de la directive introduit la notion de "*Pratiques impliquant l'exposition délibérée de personnes à des fins d'imagerie non médicale*". On pense en particulier aux techniques d'imagerie utilisées pour la recherche et les études cliniques.
Ces pratiques devront être particulièrement justifiées. Elles devront être soumises à autorisation. En France, les protocoles de recherche sont déjà soumis aux Comités de protection des personnes créés par la loi du 9 août 2004 portant sur la recherche biomédicale chez l'homme.

La fonction "d'expert en physique médicale"
La fonction et les missions de radiophysicien médical font l'objet d'une description très détaillée dans un article dédié (article 83).
Le système de reconnaissance des radiophysiciens devra certainement être organisé et réglementé.

Quoi de neuf en médecine nucléaire ?
Le dispositif d'autorisation d'utilisation des installations concernant "*les pratiques d'administration délibérée de substances radioactives à des fins diagnostiques, thérapeutiques ou de recherche*" sera remplacé par l'octroi d'une licence (Article 28).

Transposition
Les Etats membres ont 4 ans pour transposer la nouvelle directive 2013/59/Euratom en droit national. L'échéance est fixée au 6 février 2018 au plus tard.
A cette date, les directives qu'elle remplace seront abrogées.
En droit français, la transposition modifiera ou complétera la partie législative du code de la santé publique et du code du travail.

Tahiti-infos,13/05/2015

Tahiti Infos

-

Inauguration de l'unité d'hospitalisation complète en oncologie du CHPF

PIRAE, le 13 mai 2015. (COMMUNIQUE DE LA PRESIDENCE) Le ministre de la Santé et des solidarités, Patrick Howell, s'est rendu au Centre hospitalier de Polynésie française, mardi soir, afin de visiter l'ensemble des services et unités dédiés à la prise en charge des cancers (hospitalisation de jour, radiothérapie, hospitalisation complète en hématologie et oncologie) et a notamment procédé, à cette occasion, à l'inauguration de l'unité d'hospitalisation complète en oncologie.

Depuis le 4 mai, le CHPF dispose d'une unité d'hospitalisation complète de 8 lits dédiée uniquement à l'oncologie. L'ouverture de cette nouvelle unité procède de la volonté forte du Pays et du CHPF de structurer la filière de prise en charge locale des cancers.Elle est complétée par la mise en place récente d'une nouvelle technique de radiothérapie, dite IMRT, qui améliorera la qualité des traitements.

Le Centre hospitalier de la Polynésie française est l'établissement de référence pour la prise en charge du cancer. Les traitements de radiothérapie et de chimiothérapie y sont délivrés en externe : à la séance pour la radiothérapie, en hospitalisation de jour pour les chimiothérapies.

Il arrive cependant que les protocoles de traitement ou l'état de santé du patient impliquent une hospitalisation complète. Ces hospitalisations étaient auparavant assurées dans les services correspondant aux organes touchés.

Mi-2011, le service de radiothérapie du Centre hospitalier de la Polynésie française a accueilli ses premiers patients. La filière de prise en charge des cancers en Polynésie permet, depuis, de traiter la quasi-totalité des cas, à quelques exceptions près, nécessitant des traitements très particuliers.

Les 300 à 400 patients pris en charge chaque année peuvent donc l'être sur place. Ceci induit des économies très substantielles pour la collectivité puisque, compte tenu du fait que chaque cas peut impliquer plusieurs séquences de traitement, le nombre d'évacuations sanitaires évitées chaque année est estimé entre 500 et 700. Outre l'aspect financier, cette prise en charge sur place améliore le confort du patient qui ne connaît plus les inquiétudes supplémentaires liées au départ vers la métropole.

Ce qui a également pour conséquence la diminution des refus de soins, puisque, auparavant, certaines personnes ne souhaitaient pas partir pour être traitées.

TNTV news, 04/11/2022

TNTV news

Du nouveau matériel pour le traitement du cancer de la prostate au CHPF

Le Centre Hospitalier de Polynésie française (CHPF) accueillera mi-2023 un scanner à Tomographie par Émission de Positons, ou TEP-scan. Cet appareil permet de compléter le diagnostic du cancer et d'évaluer l'efficacité des traitements contre le cancer de la prostate, qui touche environ 120 nouveaux cas chaque année en Polynésie française.

L'Institut du Cancer de la Polynésie Française (ICPF) a annoncé par un communiqué l'arrivée prochaine, en mi-2023, du TEP-scan. Cette nouvelle acquisition permettra au CHPF de compléter le diagnostic d'un cancer en repérant les tumeurs et les métastases, et d'évaluer l'efficacité d'un traitement de radiothérapie ou de chimiothérapie.

Actuellement, les patients nécessitant un examen par TEP-scan doivent être obligatoirement évasanés en métropole ou vers la Nouvelle-Zélande.

En 2025, dans le bâtiment du futur Institut du Cancer de Polynésie française, **son utilisation s'étendra à l'ensemble des cancers** grâce au module complémentaire appelé « cyclotron ».

Aussi, un séminaire sur la thématique du TEP et de la radiothérapie interne des cancers de la prostate est coorganisé avec l'ICPF et le CHPF**, ce samedi 5 novembre à l'amphithéâtre du CHPF**. Un événement gratuit et ouvert à tous les professionnels de santé.

Pour l'occasion, deux experts en médecine isotopique ont été conviés, le Dr Roland Hustinx, professeur et médecin au CHU de Liège et le Dr Philippe Robin médecin au CHU de Brest.

DOCUMENT N°10

Lexpol, 23/01/2023

Loi du pays n° 2023-14 du 23 janvier 2023 relative à la prévention des risques d'exposition aux rayonnements ionisants en milieu professionnel

(NOR : TRA22202795LP)
Paru in extenso au journal officiel n°7 NS du 23/01/2023 à la page 862 dans la partie Lois du pays

Version en vigueur au 23/01/2023

Après saisine du Conseil économique, social, environnemental et culturel de la Polynésie française ; L'assemblée de la Polynésie française a adopté ;
Le Président de la Polynésie française promulgue la loi du pays dont la teneur suit :

Article LP. 1er

Pour l'application de la présente loi du pays et des textes pris pour son application, la Polynésie française peut solliciter le soutien, par voie de convention, de l'Autorité de sûreté nucléaire (ASN) et de l'Institut de radioprotection et de sûreté nucléaire (IRSN).

La convention avec l'ASN a notamment pour objet d'organiser les modalités de contrôle des installations et d'apporter son appui dans le domaine du contrôle de la radioprotection des professionnels.

La convention avec l'IRSN a notamment pour objet :

1° D'organiser la centralisation des doses issues de la dosimétrie, reçues par les professionnels au cours de leur vie entière (système SISERI) ;

2° D'organiser la transmission des informations en vue d'alimenter l'inventaire national des sources (Système SIGIS) ;

3° De permettre la mesure d'éventuelles contaminations internes par anthropogammamétrie ;

4° D'organiser les reconstitutions de doses à distance, lorsqu'elles ne peuvent pas être estimées sur place, en particulier en cas de contamination interne ;

5° De faciliter d'éventuelles interventions en Polynésie française en appui des services de sécurité civile en cas d'incident ou d'accident, sur décisions de l'ASN.

Art. LP. 2

Pour celles qui ne sont pas fixées dans la réglementation relative à la protection des personnes et de l'environnement contre les risques liés à l'exposition aux rayonnements ionisants, les termes définis ci-après sont applicables à la présente loi du pays ainsi qu'aux textes pris pour son application :

- "employeur", toute entreprise ou tout service et établissement public de la Polynésie française dont l'activité est susceptible d'exposer le professionnel à un risque dû aux rayonnements ionisants ;
- "professionnel", toute personne susceptible d'être exposée à un risque dû aux rayonnements ionisants dans le cadre de son activité professionnelle, quelle que soit son activité, son statut ou la nature de son contrat de travail.

Art. LP. 3

Sans préjudice des dispositions relatives aux principes généraux de prévention prévues dans le code du travail de la Polynésie française et des dispositions spécifiques prévues par le statut général de la fonction publique de la Polynésie française, les règles de prévention des risques pour la santé et la sécurité des professionnels, y compris les travailleurs indépendants et les employeurs, exposés aux rayonnements ionisants sont fixées dans le respect des principes généraux de radioprotection des personnes énoncés à l'article LP. 2 de la loi du pays relative à la protection des personnes et de l'environnement contre les risques liés à l'exposition aux rayonnements ionisants.

Art. LP. 4

L'employeur désigne un conseiller en radioprotection, spécialement formé, afin de le conseiller sur toutes les questions et mesures à prendre en lien avec la prévention des risques d'exposition aux rayonnements ionisants.

Sur proposition du conseiller en radioprotection au sens de l'alinéa précédent, le professionnel lui transmet les résultats de la dosimétrie.

Art. LP. 5

Ier - Les dispositions du présent titre s'appliquent dès lors que les professionnels, y compris les travailleurs indépendants, sont susceptibles d'être exposés à un risque dû aux rayonnements ionisants d'origine naturelle ou artificielle.

Elles s'appliquent notamment :

1° A la fabrication, à la production, au traitement, à la manipulation, au stockage, à l'utilisation, à l'entreposage, à la détention, au transport de substances radioactives.

Une substance radioactive est une substance qui contient des radionucléides, naturels ou artificiels, dont l'activité ou la concentration justifie un contrôle de radioprotection.

2° A la fabrication et à l'exploitation d'équipements électriques émettant des rayonnements ionisants et contenant des composants fonctionnant sous une différence de potentiel supérieure à 5 kilovolts ;

3° A l'exploitation d'aéronefs en ce qui concerne l'exposition de l'ensemble des personnes embarquées pour le service de l'aéronef en vol.

II - Les dispositions du présent titre ne s'appliquent pas :

1° Aux expositions résultant de l'exposition à un niveau naturel de rayonnements dû :

a) A des radionucléides contenus dans l'organisme humain ;

b) Au rayonnement cosmique régnant au niveau du sol ;

c) Aux radionucléides présents dans la croûte terrestre non perturbée ;

2° Aux expositions subies par les professionnels du fait des examens médicaux auxquels ils sont soumis ;

3° A l'exposition des professionnels autres que les équipages aériens au rayonnement cosmique au cours d'un vol aérien.

Art. LP. 6

Les spécificités des règles de prévention appelées par le présent titre sont déterminées par arrêté pris en conseil des ministres, notamment :

1° Les modalités de l'évaluation des risques et de la mise en œuvre des actions de prévention qui en découlent ; 2° Les conditions d'emploi des professionnels exposés ;

3° Les valeurs limites d'exposition ;

4° Les modalités de surveillance de l'exposition, de suivi dosimétrique et de suivi médical spécifiques ; 5° Les modalités des vérifications de radioprotection ;

6° Les modalités des formations compte tenu des situations particulières d'exposition ;

7° Les conditions d'information des professionnels sur les risques et les mesures prises pour y remédier ;

8° Les prescriptions particulières relatives à certaines professions, à certains modes de travail, à certains risques ;

9° Les éventuelles restrictions ou interdictions concernant les activités, procédés, dispositifs ou substances, dangereux pour les professionnels.

Art. LP. 7

Lors de leur mise en service dans l'établissement, à l'issue de toute modification importante susceptible d' affecter la santé et la sécurité des professionnels, et de façon régulière, en vue de s'assurer qu'ils sont installés conformément aux spécifications prévues et qu'ils peuvent être utilisés en sécurité, l'employeur procède à des vérifications initiales et à des vérifications périodiques, dont les conditions sont fixées par arrêté pris en conseil des ministres.

Art. LP. 8

Lorsque les doses prévisionnelles susceptibles d'être reçues dépassent des niveaux définis par arrêté pris en conseil des ministres, l'employeur met en œuvre une surveillance dosimétrique individuelle appropriée à lecture différée, et le cas échéant mesure l'exposition externe du professionnel au cours d'une opération à l'aide d'un dispositif de mesure en temps réel.

Art. LP. 9.— Sanction administrative

Les infractions aux dispositions de l'article LP. 7 et des arrêtés pris pour leur application sont punies d'une amende administrative, dont le montant maximal ne peut dépasser 178 000 F CFP.

La sanction est prise par le chef de service en charge du travail ou par le Président de la Polynésie française, chacun dans son champ de compétence.

Art. LP. 10.— Sanction pénale

Le fait de ne pas respecter les dispositions de la présente loi du pays et des arrêtés pris pour leur application, à l'exception de l'article LP. 7, est puni des peines prévues pour les contraventions de la cinquième classe et le cas échéant, pour leur récidive.

L'amende est appliquée autant de fois qu'il y a de professionnels concernés par les infractions constatées.

Art. LP. 11

L'article 93-10 de la délibération n° 95-215 AT du 14 décembre 1995 modifiée, portant statut général de la fonction publique de la Polynésie française est ainsi modifié :

1° Après le mot "définies aux", sont insérés les mots : "dispositions suivantes :" ;

2° Il est créé un alinéa 2 commençant par un tiret devant les mots : "livres I à V" et se terminant par les mots : "du même code ;" ;

3° Il est inséré in fine un alinéa 3 ainsi rédigé : "- réglementation relative à la prévention des risques d'exposition aux rayonnements ionisants en milieu professionnel.".

Art. LP. 12

Le titre III du livre IV de la partie IV relatif à la prévention des risques d'exposition aux rayonnements ionisants du code du travail de la Polynésie française ainsi que les articles LP. 4725-3 et LP. 4725-4 sont abrogés.

Le présent acte sera exécuté comme loi du pays.

POLYNESIE FRANÇAISE

MINISTERE
DU TRAVAIL, DE L'EMPLOI,
DE LA FORMATION PROFESSIONNELLE
ET DE LA FONCTION PUBLIQUE,
chargé de la réforme de l'administration,
des relations avec l'Assemblée de Polynésie française
et le Conseil économique, social et culturel

SERVICE DU PERSONNEL
ET DE LA FONCTION PUBLIQUE

CONCOURS EXTERNE POUR LE RECRUTEMENT DE 03 INGENIEURS EN CHEF DE CATEGORIE A RELEVANT DU STATUT DE LA FONCTION PUBLIQUE DE LA POLYNESIE FRANCAISE

UNE NOTE DE SYNTHESE

Mardi 28 février 2006 de 12h30 à 16h30 (4 heures) (Coefficient 5)

Aucun document n'est autorisé, ni même l'usage de la calculatrice.

Le sujet comporte 100 pages.

CONCOURS EXTERNE D'INGENIEURS EN CHEF DE CATEGORIE A

REDACTION D'UNE NOTE DE SYNTHESE

Sujet :

La sécurité des informations par Internet est une préoccupation majeure de l'Etat.
En vous appuyant sur le rapport du député Pierre LASBORDES (document joint de 99 pages) vous rédigerez une note de synthèse de 4 à 6 pages maximum mettant en évidence les menaces qui pèsent sur l'utilisation de cet outil, puis vous comparerez l'organisation des SSI des principaux partenaires étrangers au système français. Enfin, vous justifierez la création et l'autonomie d'une base industrielle et technologique spécialisée en SSI pour gérer les informations.

La sécurité des systèmes d'information

Un enjeu majeur pour la France

Pierre LASBORDES
Député

Le 26 novembre 2005

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, qui m'a apporté compétence et expérience.

M. Roger BALERAS, *ancien Directeur des applications militaires du CEA* ;
M. Jean-Paul GILLYBOEUF, 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 LACARRIERE, *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 Ecole normale supérieure ULM, Directeur du département informatique*
M. Jean-Pierre VUILLERME, *Directeur des services environnement et prévention du groupe Michelin.*

Je tiens à remercier également 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

Le nom 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.

Sommaire détaillé

ANNEXES

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.

Si 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 modifié considérablement 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 toute entière.

Les Etats-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 Etats-Unis dominent le monde, donne à notre nation un avantage unique »[1].

Pour l'Etat 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 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-

[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*

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'Etat 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, en 2001, aux Etats-Unis, un préjudice de 59 milliards de dollars aux mille premières entreprises américaines. L'exemple le plus spectaculaire porte sur la révélation[2], en juin 2005, des agissements d'une entreprise israélienne qui « louait » un cheval de Troie[3] 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 permettant 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'Etat d'une adaptation nouvelle et urgente, dans la logique de l'Etat stratège.

[2] http://solutions.journaldunet.com/0506/050603_espionnage_industriel_israel.shtml

[3] Cheval de Troie : programme qui exécute des instructions sans l'autorisation de l'utilisateur 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.

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.

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.

SYNTHESE

SECURITE DES SYSTEMES 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, le réseau de commandement des forces armées sont des systèmes d'information.

I- 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, 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 vulnérabilités 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'Etat 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.

II- 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[4], la DCSSI[5] 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[6], elle a mis en place un centre opérationnel de la sécurité des systèmes d'information (COSSI), activé en permanence, 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.

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[7], 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

[4] Secrétariat général de la défense nationale

[5] Direction centrale de la sécurité des systèmes d'information

[6] Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques

[7] Centre de formation à la sécurité des systèmes d'information

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[8], 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 cybercriminalité. Dans le cadre de ses missions, 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'OCLCTIC[9] , est une structure à vocation interministérielle placée au sein de Direction de la police judiciaire (DCPJ). Elle lutte contre les auteurs d'infractions liées aux TIC, enquête à la demande de l'autorité judicaire, 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, donnent 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'Etat 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[10] 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 (Etats-Unis, Royaume-Uni, Allemagne, Suède, Corée du Sud et Israël) et aborde les initiatives multilatérales (Union européenne,

[8] Agence pour le Développement de l'Administration Electronique, rattachée au ministre chargé du budget et de la réforme de l'Etat

[9] office central de lutte contre la criminalité liée aux technologies de l'information et de la communication

[10] Haut fonctionnaire de Défense

OCDE, ONU, G8, réseaux de veille et d'alerte). On ne retiendra dans cette synthèse que le cas de l'Allemagne.

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 DCSSI, 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 de 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'Etat 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.

III - Base industrielle et technologique

Les Etats-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 (anti spam, anti-virus,...), 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'Etat et des grands donneurs d'ordres ne sont pas favorables aux PME innovantes. A 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 secteur 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 ministère 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 la compétence et l'expérience particulière de la France (en particulier de ses centres d'évaluation) soient 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 approuvé au préalable.10 produits ont déjà été qualifiés et 7 sont en cours de qualifications. La moitié de ces produits sont développés 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.

IV – SIX RECOMMANDATIONS

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

- Etablir 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 ;
- Etablir 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'Etat 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'Etat** 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'Etat en 2004.

UN IMPERATIF

Refondre l'organisation de la SSI de l'Etat

En complément aux six axes de recommandations, afin d'amener notre pays à un niveau de sécurité et d'autonomie, il faut **renforcer l'action de l'Etat** et ses moyens humains et financiers en matière de SSI, **rationaliser l'organisation** des services de l'Etat 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, qui ne semble plus adaptée aux enjeux actuels.

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 ;

- 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,** seraient 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 principe de gouvernance garantissant la confiance, l'implication des personnels, la transparence et la neutralité** et **évaluée sur ses activités**, notamment de support, de communication et de formation, selon des critères de performance et de qualité.

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, 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 le champs couvert et leur complexité (voir schéma en annexe 4) 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'Etat 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 Galiléo ;
  - 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 radio-électriques, 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 (allègement 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.

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

Analyser et comprendre les menaces et les vulnérabilités nécessitent 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 (principe de la vision de Clausewitz) car il n'y a pas de légitime défense en SSI[11] 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 :

[11] Stanislas de MAUPEOU, article Revue Défense nationale, novembre 2003

- 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 pares-feu protègent uniquement des attaques résiduelles (i.e. qui ne correspondent pas aux services offerts)[12] ;
- 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).

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 aux fins de protéger les ressources et les informations contre tout préjudice et également prévoir le cas de la faillite de la protection.

Pour être mise en œuvre sur un plan opérationnel, cette politique de sécurité s'adosse 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.

1.2 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 5).

[12] 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/) ;

• **L'AFNOR[13] 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, Internet,....

- « 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 LIMITEE**

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 conséquences qu'aurait leur divulgation, leur altération, leur indisponibilité ou 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 LIMITEE.

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'informa tique, 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.

1.3 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 ;

[13] Association française de normalisation.

- **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 aux fins de lui soutirer de l'information via l'« ingénierie sociale »[14] 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 une porte blindée à l'entrée d'une maison, mais en laissant les fenêtres ouvertes.*

1.3.1 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 (ordinateurs accessibles en ligne !! ce qui n'a pas beaucoup de sens). Pensant avoir à faire à un jeu, il choisit le déclenchement de la 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 (Etat, 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 moteur dans des actes délictueux. Il est cependant utile de

[14] 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.

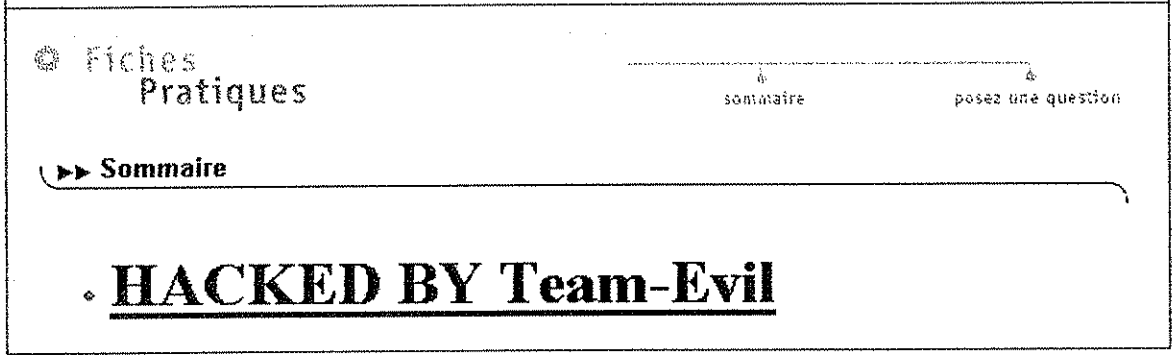
chercher à les comprendre pour mettre en place des stratégies et des tactiques de réponses adaptées.

On distingue traditionnellement 4 types d'attaques qu'ils nous semblent utile ici de rappeler 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[15] : 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 Etat, 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.

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

Profils des attaquants

Sans détailler tous les profils (cf. Annexe 6), on retiendra le plus connu ; les « hackers »[16] 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.

1.3.2 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[17] dans le cadre de la lutte contre le terrorisme »[18]), 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. »

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 ...) ; 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,...) ; les réseaux de communication (téléphone filaire, cellulaires, réseau Internet,...) y compris ceux des forces de police et de la défense.

[16] 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 systèmes d'information seront préférés.

[17] Il est opportun de préciser la distinction faite entre la terminologie française « infrastructures vitales » et anglo-saxonne « *critical infrastructures* »

[18] http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/com/2004/com2004_0702fr01.pdf

L'interdépendance entre certaines de ces infrastructures génère également des facteurs de risques en terme de réaction en chaîne qui doivent conduire l'Etat 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 domaines 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 anti virus ou les pares-feu mais la vigilance de l'utilisateur est primordiale ainsi qu'une véritable politique de mise à jour des applications.

- **L'Etat : une cible de choix**

A titre d'exemple, le Ministère de la Défense Américain (Department of defense) est le plus attaqué au monde, avant Microsoft[19]. Preuve en est aussi le succès des sites gouvernementaux (extension .gov aux Etats-Unis, .gouv.fr en France) sur les pages référençant les défigurations, « considérées spéciales»[20].

Si la défiguration d'un site peut sembler banale et sans conséquence autre que l'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.

[19] Source auditions

[20] Défigurations spéciales : http://www.zone-h.com/en/defacements/special

- **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[21] 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 toutes 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.

1.3.3 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).

[21] http://solutions.journaldunet.com/0506/050603_espionnage_industriel_israel.shtml

Liaisons transatlantiques
Le réseau TAT-1422, assure une partie du transit Internet entre l'Europe et les Etats-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.

- **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 de l'art actuel, 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.

1.3.4 Les vecteurs d'attaques sont multiples et témoignent d'une complexité croissante

1.3.4.1 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...), **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.

[22] A propos de TAT-14 : https://www.tat-14.com/tat14/

La miniaturisation des moyens de stockage, comme les clés USB[23], 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,...) **ont accès aux locaux**.

1.3.4.2 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 leurs vulnérabilités les rendent 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 la confidentialité, par écoute des émissions radioélectriques du réseau.

La menace TEMPEST[24] :

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.

[23] Une faille de sécurité concernant l'utilisation des clefs USB a été mis 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 consulter toutes les données. Cette faille est propre à la technologie USB et non au système d'exploitation, ce qui signifie que tous les systèmes sont potentiellement vulnérables.

[24] 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

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 Ile-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...

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.

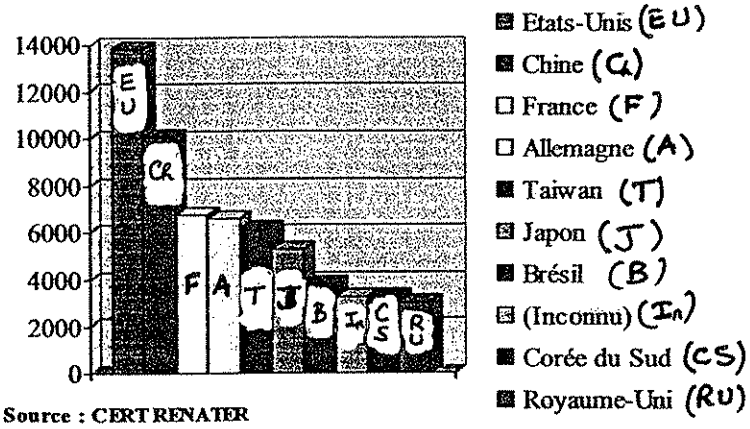
Considérant, par exemple, l'intérêt que pourrait trouver un concurrent à lire à distance l'ensemble du flux logistique de distribution d'un industriel, et dans la mesure où ce type de technologie est envisagé pour transmettre des données personnelles (sur des passeports par exemple) l'emploi de la technologie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

1.3.4.3 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'information sur le système ou réseau ciblé. A 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.



Source : CERT RENATER

Provenance des « scans »

Au mois d'octobre 2005, 104219 sources distinctes ont sondé des machines sur le réseau RENATER[25].

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

[25] RENATER : Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche

- **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.

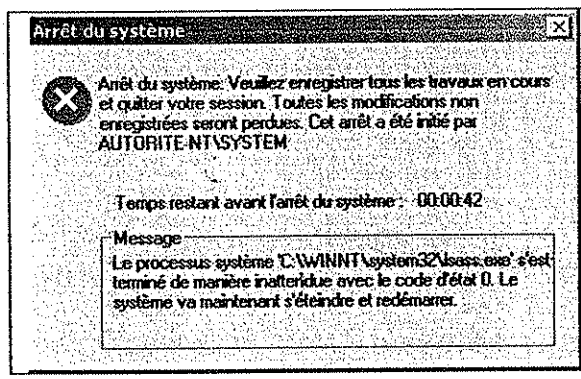
- **L'altération et la destruction :** il peut s'agir d'altérer ou de détruire des données stockées sur le système, ou bien le système lui-même, avec des finalités diverses. Au-delà des implications financières et industrielles évidentes, le but poursuivi peut être la dégradation des mécanismes de protection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

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 tous premiers vers sont apparus en 1982. On retiendra la déferlante médiatique d'**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 $. 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**[26].



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**[27].

Se propageant entre PC sous Windows sans firewall grâce aux connexions réseau, il a longuement fait parler de lui en mai 2004.

[26] Source auditions

[27] http://www.sophos.fr/virusinfo/analyses/w32sassera.html

- **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.

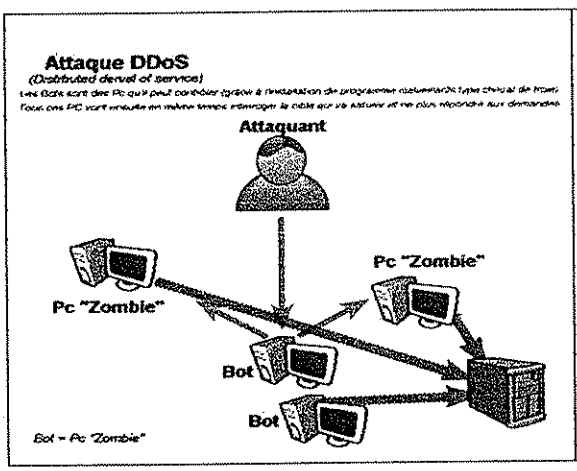
  A titre d'exemple, dans un grand groupe[28] , 5% des courriels échangés en 2004 ont été interceptés et éradiqués. Mais il faut aussi et surtout tenir compte de tout ce qui ne se détecte pas à cause de mise à jour non effectuée ou de vulnérabilité encore inconnue. Les anti virus agissent par définition a posteriori. C'est précisément pour cela que la protection contre les virus ne peut et ne doit pas se limiter à un anti virus 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[29] 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. Ils peuvent provoquer des redémarrages intempestifs ou empêcher le téléchargement de correctifs tout en bloquant l'accès à certains sites Internet.

  Les attaquants dont la motivation est souvent financière, pour ne pas être détectés et préserver leur anonymat, ont de plus en plus tendance à mettre en place un réseau de machines devant rester invisible leur permettant, le moment venu, de relayer de manière massive à partir des machines infectées l'attaque désirée : des Spam, 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[30].



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

En 2002, pendant une heure, les treize serveurs de noms racine (dont 10 aux Etats-Unis), qui permettent directement ou indirectement, à tous les navigateurs de trouver les pages web demandées, à tous les emails 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.

[28] Sources auditions
[29] Source Sophos et Clusif
[30] Rapport "Internet Security Threat Report" de la société Symantec

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

- **Un Spam** est un courrier électronique d'exemplaires identiques, envoyé en nombre, de façon automatique et non sollicité[31].
  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. A titre d'exemple un grand groupe français[32] dans lequel 500 000 mails sont échangés chaque jour, en rejette 60 000, dont 31 000 Spam 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 Etats-Unis)[33]. 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,...). 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.

1.3.4.4 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.

1.3.4.5 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.

1.4 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

[31] 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).

[32] Source auditions

[33] Rapport "Internet Security Threat Report" de la société Symantec

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.

1.4.1 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 (patch) ; 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 7).

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** [34]

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,[35] 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[36].

- **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 de vol de données de l'entreprise alors que des mesures simples concernant

[34] 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).

[35] Source auditions

[36] Source auditions

l'utilisation de ces périphériques et leur traçabilité permettra de réduire sensiblement le niveau de risque.

D'après une enquête IDC[37], 71% des sondés jugent très préoccupante l'utilisation en privé d'équipements mobiles en particulier par les dirigeants.

1.4.2 Les organisations sources de vulnérabilités

L'utilisation des failles inhérentes à l'organisation d'une entité est également un moyen d'accéder à ses 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 %).

Une 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 de savoir-faire en matière d'administration de systèmes définitive ;

- **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.**

[37] Livre blanc IDC France – Internet Secutiy System (ISS) sur la sécurité des systèmes d'information – 100 entretiens auprès d'entreprises et d'administrations françaises – avril 2005

l'utilisation de ces périphériques et leur traçabilité permettra de réduire sensiblement le niveau de risque.

D'après une enquête IDC[37], 71% des sondés jugent très préoccupante l'utilisation en privé d'équipements mobiles en particulier par les dirigeants.

1.4.2 Les organisations sources de vulnérabilités

L'utilisation des failles inhérentes à l'organisation d'une entité est également un moyen d'accéder à ses 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 %).

Une 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 de savoir-faire en matière d'administration de systèmes définitive ;
- **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.**

[37] Livre blanc IDC France – Internet Secutiy System (ISS) sur la sécurité des systèmes d'information – 100 entretiens auprès d'entreprises et d'administrations françaises – avril 2005

1.4.3 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.

1.4.4 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.

1.5 Des enjeux futurs en matière de SSI

1.5.1 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 »[38].

[38] Source auditions

1.5.2 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.

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.**[39]

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.

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

Un enjeu de souveraineté nationale : l'Etat 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'Etat, des infrastructures vitales, et des entreprises sensibles.

En effet, l'Etat 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".

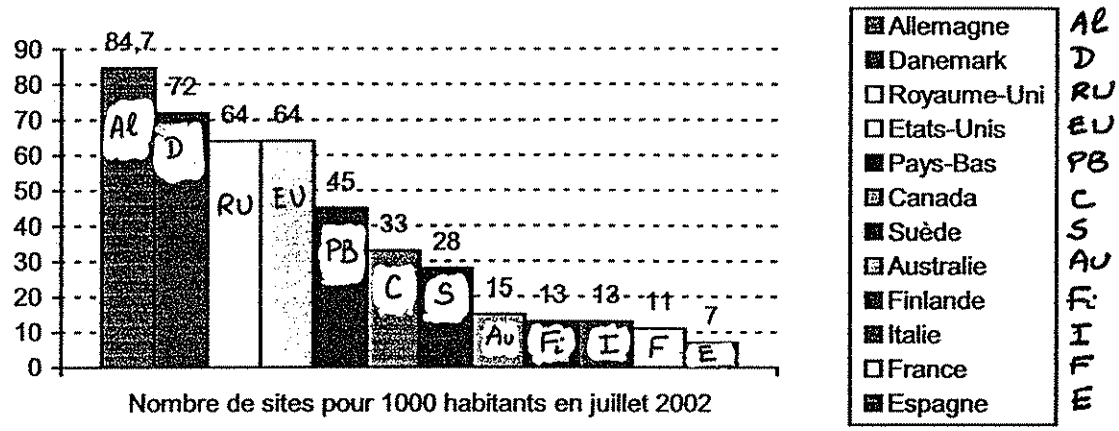
Les champs d'actions de la SSI et de l'Intelligence économique, se recoupent pour partie, car ils font la synthèse de l'économie de la connaissance, et donc de l'information. Pour être efficace, une politique volontariste d'Intelligence économique doit notamment s'appuyer sur des systèmes d'information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

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 Etats-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.

[39] Source auditions

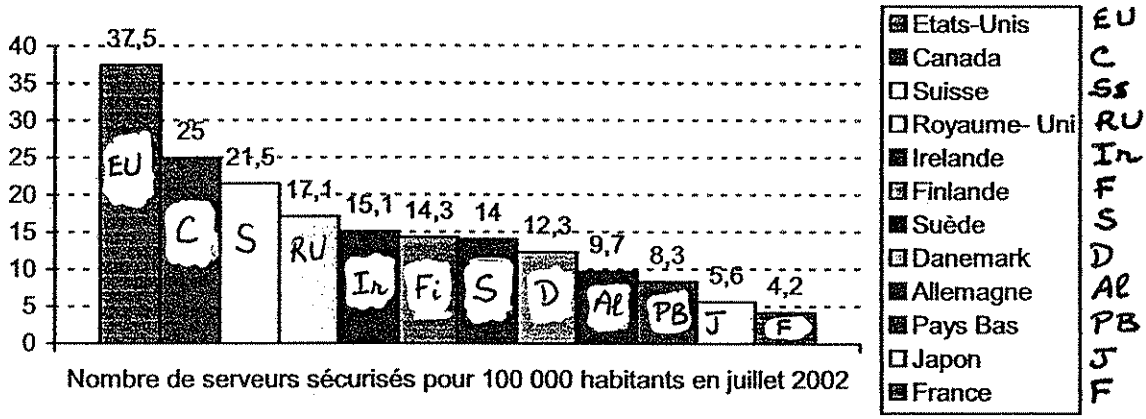
Un enjeu économique : un environnement sécurisé est nécessaire afin d'accompagner le rattrapage français dans l'usage des TIC par les citoyens et les entreprises françaises indispensable pour la croissance française.
Selon le tableau de bord du commerce électronique de décembre 2004[40] malgré un taux 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.



Nombre de serveurs sécurisés pour 100 000 habitants en juillet 2002

D'autres statistiques dans cette étude, relatives 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 Etats-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.

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

Dans un contexte de mondialisation croissante de l'économie et de concurrence soutenue, les entreprises françaises, mais aussi l'Etat, 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.

2 Les réponses organisationnelles et techniques

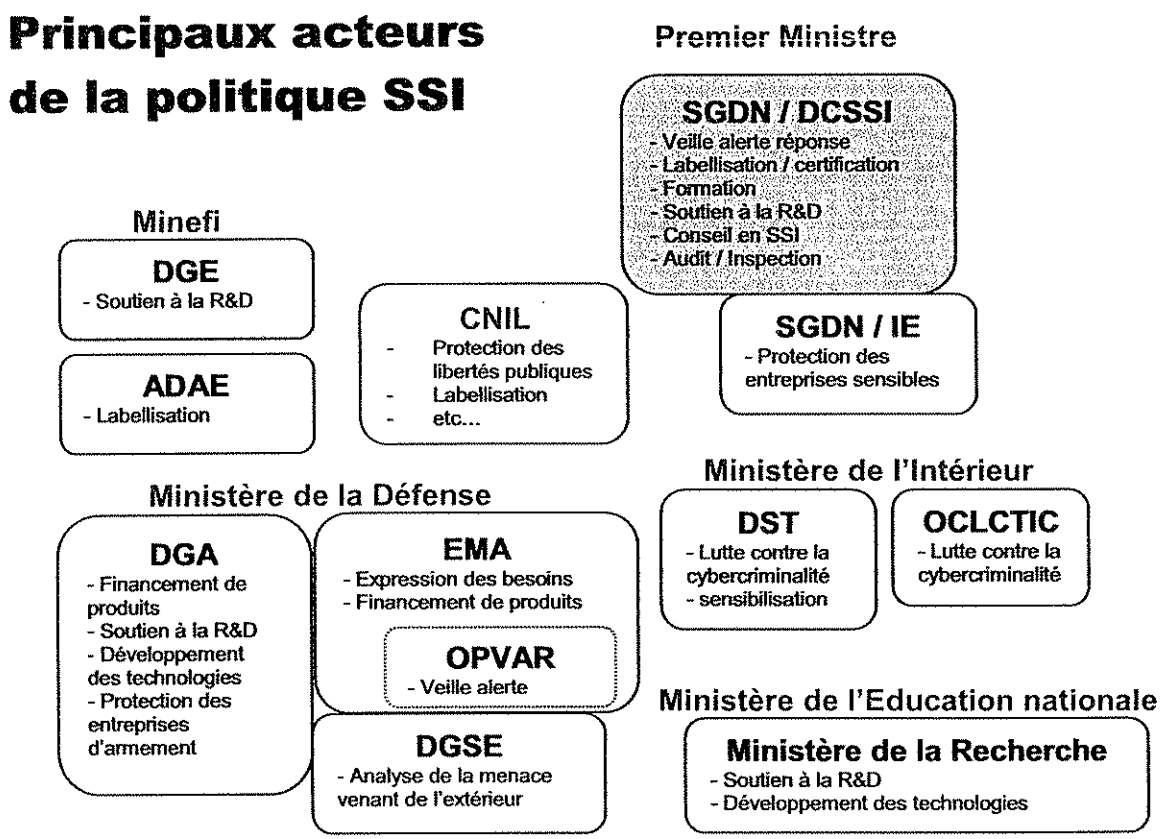
2.1 Comment l'Etat est-il organisé pour assurer la SSI ?

La sécurité est l'affaire de tous, mais l'Etat 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'Etat 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.

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

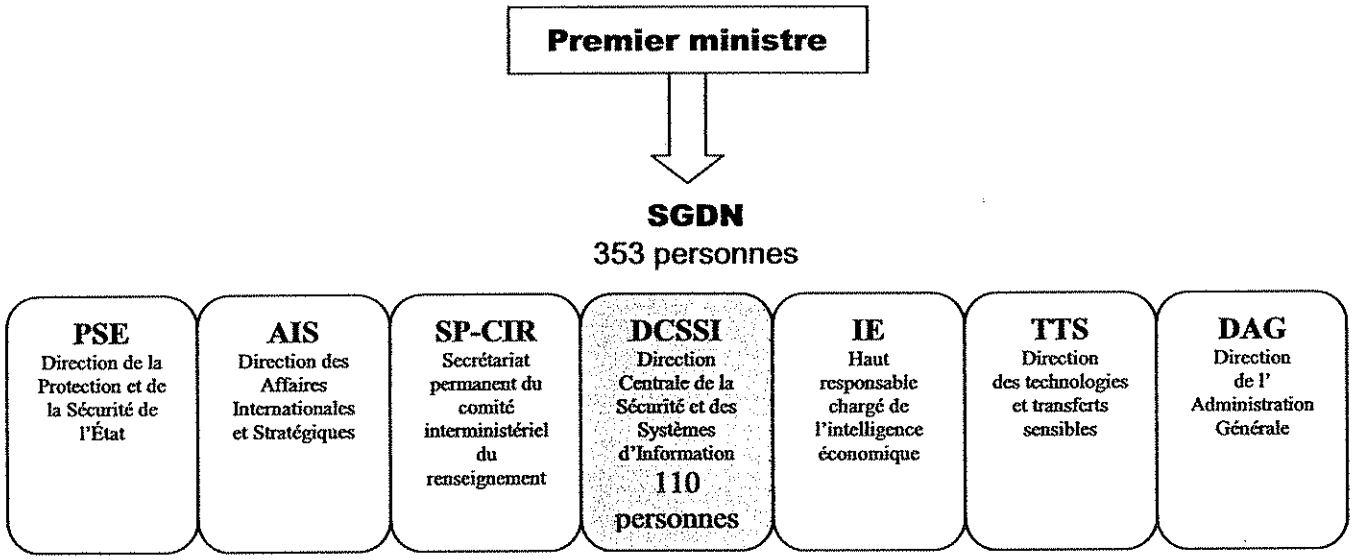
La réglementation en sécurité des systèmes d'information (SSI) n'existe pas sous la forme d'un code législatif ou réglementaire. La SSI n'est d'ailleurs pas même définie d'un point de vue juridique. En fait, le domaine de la SSI fait référence à une multitude de textes de niveaux juridiques très divers 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 9)

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



2.1.2.1 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[41] *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**[42] (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.

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.

[41] Décret n°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).

[42] Le décret 2001-69342 précise les missions de 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)**[43], 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 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 24h/24 7j/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[44] (centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques). Chacune de ces unités regroupe une dizaine de personnes. Les ministères et les opérateurs d'infrastructures vitales sont invités à signaler au COSSI les attaques dont ils sont victimes.

[43] Le décret n°2001-69443 précise le rôle de la CISSI

[44] 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).

- 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'Etat, 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)[45], 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. A titre d'exemples le CFSSI propose plusieurs degrés de stages[46] de haut niveau de spécialisation ou de simple sensibilisation, d'une durée d'une journée, ou après deux années de formation tel que le Brevet d'études supérieures de la sécurité des systèmes d'information (BESSSI). En 2004, pas moins de 898 stagiaires avaient suivi l'une ou l'autre des formations[47].
  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.

2.1.2.2 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.

[45] Décret 87-354 du 25 mai 1987
[46] cfssi@sgdn.pm.gouv.fr et www.formations.ssi.gouv.fr
[47] Source auditions

2.1.2.2.1 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)[48] 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)[49], 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[50].

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 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

[48] Cf. infra 2.1.2.3
[49] Voir glossaire
[50] Bientôt DGSIC

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 : la Direction générale de la sécurité extérieure

La DGSE a pour mission d'évaluer la menace provenant de l'étranger qui pèse sur les systèmes d'information.

2.1.2.2.2 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 : la Direction de la surveillance du territoire

Dans le cadre de ses missions de lutte contre l'espionnage, de la lutte anti-terroriste 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 créée 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 judicaire, 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 Ile 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'ADAE (Agence pour le Développement de l'Administration Electronique), 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'Etat.
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, aux 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'Etat.

2.1.2.2.3 Les conséquences de la multiplication des acteurs publics

La multiplication des acteurs publics dont les missions se chevauchent et les textes fondateurs peu précis, donnent **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'Etat 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 par exemple 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 ?

2.1.2.3 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.

A 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'Etat, 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)**

A 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.**

2.1.3 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[51], soit à recourir à l'externalisation[52].

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[53].

- 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 a « mettre en place une organisation conjointe de développement de produits de sécurité», présentée par le PRSSI, est à recommander.

2.2 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'Education 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 ;

[51] 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.
[52] Parfois retenue par certains ministères, le recours à l'externalisation doit être conditionné à un encadrement plus strict.
[53] 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.

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

L'Etat 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'Etat, 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'Etat 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.

2.4 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 Etats-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.

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

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

L'E*xecutive order* 12333 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 Etat.

La NSA a une double mission : protéger les systèmes d'information des Etats-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 13228 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'informations 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.

2.4.1.2 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'Etat, est l'homologue de la DCSSI. Au Royaume Uni, le NISCC[54], 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[55], chargé de recueillir des alertes et de signaler des incidents (mais sans capacité d'intervention) et des ISAC[56], 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,

[54] National Infrastructure Security Co-ordination Centre
[55] Warning, Advice and Reporting Point
[56] Information Sharing and Analysis Center

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[57] 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) pour une délivrance des premiers passeports à l'automne 2006. Par ailleurs, un nouveau programme de recherche (IADP[58]) a été mis en place afin d'optimiser les efforts dans le domaine SSI, en partenariat avec l'industrie.

2.4.1.3 Allemagne : une politique produit forte très tournée vers les utilisateurs

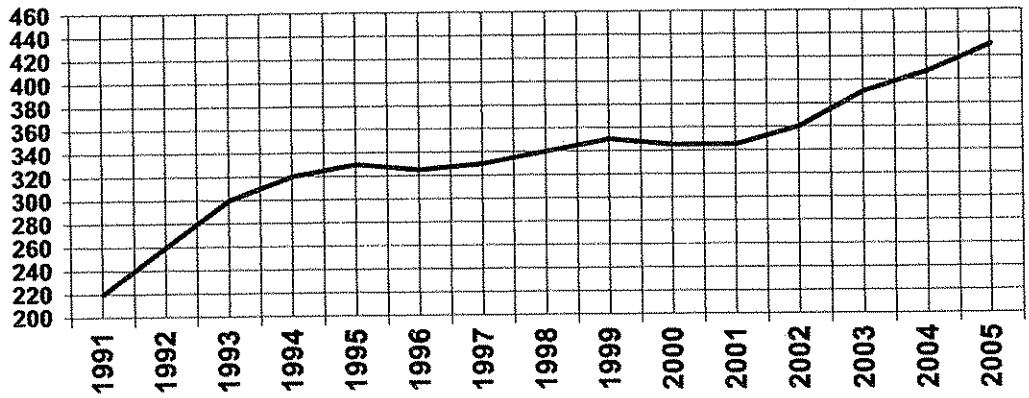
L'Allemagne a adopté en juillet dernier, un plan national pour la protection des infrastructures d'information (NPSI)[59] qui comporte trois objectifs principaux :

- 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.

Evolution 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** :

[57] General Information Assurance Products and Services Initiative – www.gipsi.gov.uk .
[58] Information Assurance Devleopment Programme.
[59] http://www.bmi.bund.de/nn_148134/Internet/Content/Nachrichten/Pressemitteilungen/2005/08/Information__Infrastructure__en.html .

- **Informer le pays**
  - o 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 ;
  - o en participant à des campagnes de sensibilisation des PME en 2004 (Sécurité de l'Internet pour les PME) ;
  - o 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 :**
  - o 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 ;
  - o 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 ;
  - o 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 ;
  - o 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 Etats-Unis, la Suisse, la Suède et la Finlande ;
  - o le BSI conseille également les Länder sur le plan technique.

- **Analyser les risques, évaluer et tester :**
  - o le BSI assure la certification des produits et services de SSI (38 en 2004) ainsi que l'attribution de licences pour des applications classifiées ;
  - o il a une action particulière sur les procédures biométriques et des applications mobiles ;
  - o 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.

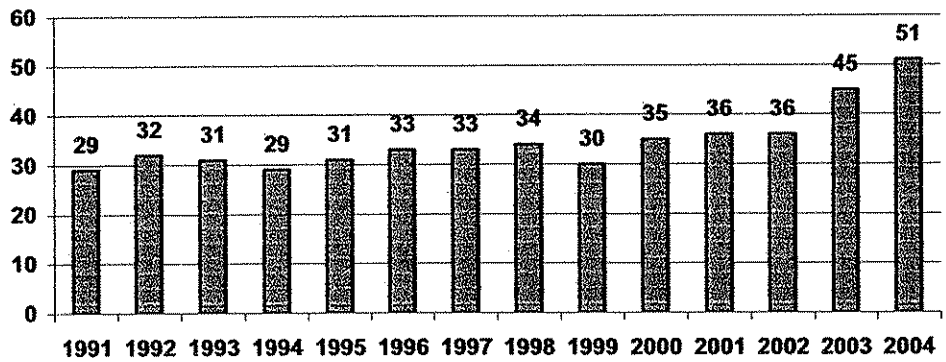
- **Assurer des fonctions opérationnelles :**
  - o assurer la fonction de CERT allemand (Computer Emergency Response Team) ;
  - o coordination technique du réseau d'information Berlin-Bonn ;

- 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.

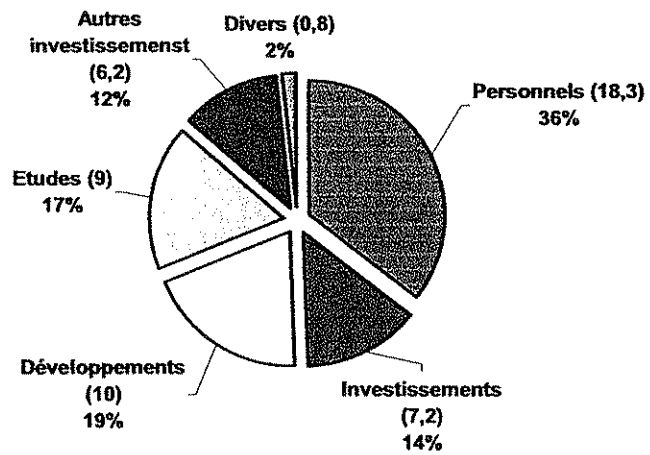
Pour assurer l'ensemble de ces missions, le BSI dispose d'un budget significatif de **51 millions d'euros** en augmentation régulière depuis 2002.

BUDGET en millions d'euros du BSI



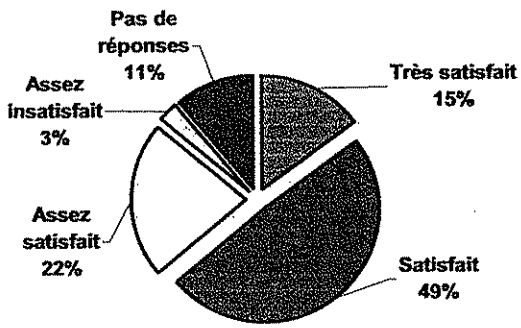
La répartition de ce budget, montre une action forte sur les développements, 10 M€, soit 19% du budget et les études pour 9 M€ soit 17% du budget que l'on ne retrouve pas en France.

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



2.4.1.4 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[60] pour les aspects organisationnels et l'IST[61] (appelé à remplacer le FRA[62]) 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.**

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

A 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

[60] Swedish Emergency Management Agency.
[61] Institute for Signals Intelligence and Technical Infosec.
[62] National Defence Radio Establishment.

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 6ème Bureau (domestic affairs) s'était vu adjoindre le Cyber Crime Group dont le personnel pourrait rejoindre le NCSC.

2.4.1.6 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'Etat 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).

2.4.1.7 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'Etat, 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)[63]. 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 Etats membres, et de coopérer de ce fait 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 Etats 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'Etat [...] ou aux activités de l'Etat 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)[64], de la deuxième commission sur le développement d'une

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

[64] Résolutions n° 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.

culture globale de la cybersécurité[65] et de la troisième commission sur la lutte contre l'utilisation criminelle des technologies de l'information[66]. 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 Etats-Unis et la Russie sur la prise en compte de l'utilisation des TIC à des 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[67] 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[68]), 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 Etats 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[69] 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 Etats-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

[65] Résolutions n° 57/239 du 20 décembre 2002 et 58/199 du 23 décembre 2003.
[66] Résolutions n°55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001.
[67] Union internationale des télécommunications.
[68] Working party in information security and privacy.
[69] www.oecd.org/sti/cultureofsecurity .

en œuvre des « bonnes pratiques » dans le domaine de l'alerte et de la veille informatique (CERT) ; la 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[70] et à l'échelle européenne au sein de la TF-CSIRT[71] 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, (Etats-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 Etats 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).

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

2.5.1 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 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[72] qui met en évidence les principaux sinistres chez les grandes et moyennes entreprises on notera que:

[70] Forum of Incident Response and Security Teams.

[71] Task Force to promote the collaboration between Computer Security Incident Response Teams.

[72] 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%)

- **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[73].

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

D'après une étude de l'institut américain en sécurité informatique CSI[74], 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 pas de données statistiques précises qui permettent d'avoir une vision précise du phénomène.

[73] Source Minefi

[74] CSI/FBI Computer Crime and Security Survey – 2005 – Enquête auprès de 700 entreprises et organisations publiques américaines

- **Des protections insuffisantes, en particulier dans les PME** (Etude 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.

2.5.2 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 oeuvre d'une 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[75], 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 ;

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

- mettre en œuvre un plan de sauvegarde ;
- gérer et maintenir les politiques de sécurité.

- **A 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 Etats ;
- 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.

2.5.3 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[76], 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 : Etude 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.

[76] 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

- **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**.

- **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 la SSI efficace par rapports aux besoins 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[77] 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).

[77] Source auditions

- **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[78]. 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 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**[79]. La motivation à investir dans la SSI varie de manière considérable selon la taille de l'entreprise.

[78] Source auditions

[79] Source auditions

2.5.4 Des modèles organisationnels diversifiés pour parer aux menaces et risques informatiques

2.5.4.1 Quelques exemples d'organisations[80]

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 ;
  - 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 H24 7/7 ;
  - 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 11 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

[80] Source auditions

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.

2.5.4.2 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[81] (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[82] 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[83], 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[84] 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[85], 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 2006.

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[86].

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

[81] Managed Security Service Provider
[82] CSO Entreprise & Sécurité de l'Information – Enquête auprès de 144 entreprises de plus de 200 salariés
[83] 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
[84] Source L'Agefi
[85] Source Syntec et 01 Informatique
[86] Source L'Agefi

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 :

- 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 oeuvre. A cet effet, les récents travaux conduits par l'AFNOR, le CIGREF et le SYNTEC sur ce thème sont à signaler.

2.5.5 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 Etats-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.[87]

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

2.5.6 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...

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.

[87] Source auditions

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 24h/24h et 7j/7j 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.

2.5.7 Les entreprises attendent de l'Etat 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'Etat ont des difficultés à **identifier rapidement le bon interlocuteur**[88] parmi les nombreux services de l'Etat.

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'Etat 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

[88] Source auditions

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.

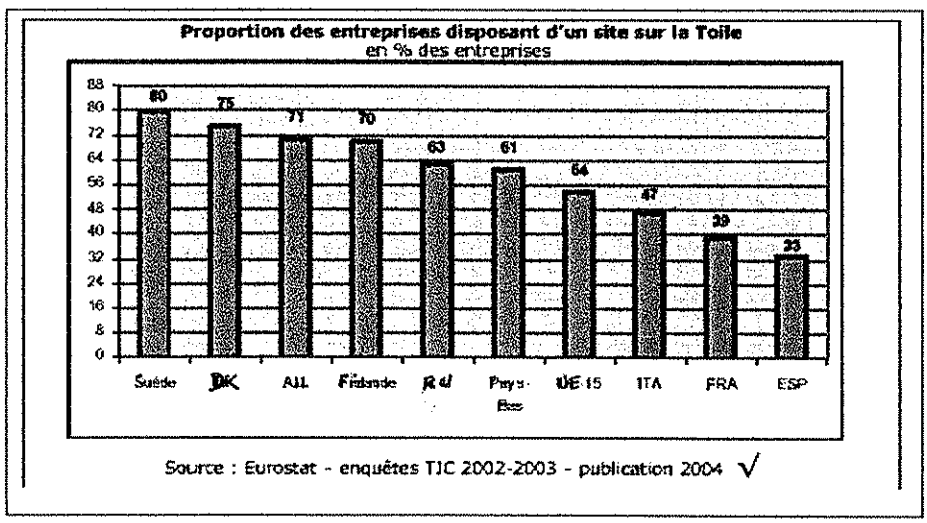
Les entreprises intervenant à l'international **souhaitent** disposer d'un support efficace des services de l'Etat pour les accompagner face aux risques spécifiques de l'international : veille, alertes, informations sur les menaces, conseils (juridiques, procédures, méthodologie, outils et solutions, 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 Etats** devient problématique pour la politique de sécurité de grands groupes[89].

2.5.8 Les problématiques spécifiques des PME face à la SSI

2.5.8.1 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'Economie Numérique 2004[90], 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.



[89] Source auditions

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

- **Les PME françaises sont elles-même 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.

Ces données sont confirmées par cette même étude de la Mission pour l'Economie 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.**

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

La part manufacturière est plus importante qu'aux Etats-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 Economie Numérique.

2.5.8.2 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[91], workflow[92],...

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[93] 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'Etat en matière de politique « qualité », à travers les

[91] Stockage de données

[92] Outils informatiques de gestion de flux de travail des entreprises qui permet d'optimiser leurs processus métiers clés.

[93] Source Le Monde Informatique

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.
Ainsi, l'AFNOR[94] 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**

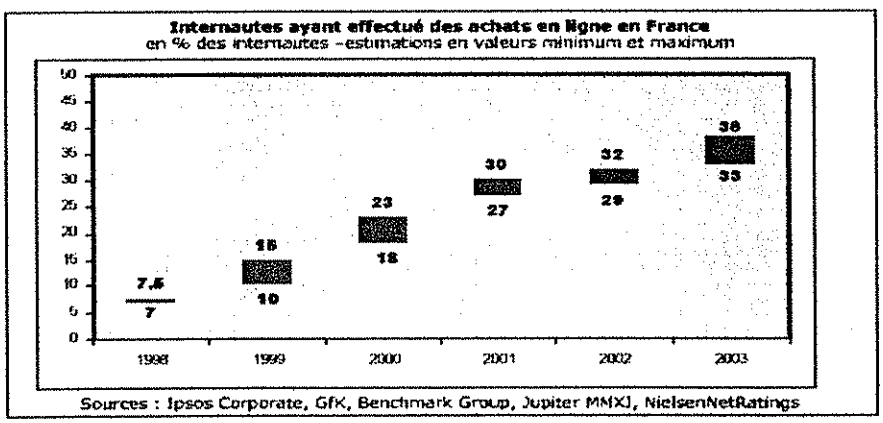
Les tendances du marché et surtout les positionnements pris par de nombreux acteurs informatiques le démontrent, **les PME apparaissent comme un futur marché en croissance en matière d'infogérance et de services de sécurité informatique** afin de compenser leurs déficiences internes qui les obligent 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[95]. 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.

2.6 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. A 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 oeuvre.



[94] Source auditions
[95] Source 01 Informatique

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[96]. Ce type d'action est à amplifier.

2.7 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'Etat 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'Etat 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 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?

[96] Source Délégation aux usages de l'Internet

3 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'informations 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.

3.1 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[97]. Ils ne sont pas habituellement inclus dans le marché de la SSI ;

[97] Digital Right Management (gestion des droits numériques) : protection des contenus vidéos et audios, notamment soumis à des droits d'auteur, diffusés sur Internet

- 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 multi niveaux.

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.

3.1.1 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[98] 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 Etat relèvent d'exigences de souveraineté et de sécurité des biens et des personnes.

Pour répondre à ces besoins, les attentes concernent des **produits logiciels** (anti-virus, pares-feu,...), 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:

[98] La sécurité des systèmes d'information dans les entreprises françaises en 2004, vision comparée de la France et du monde ; Ernst&Young , décembre 2004

- *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 (anti spam, anti-virus,...), 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).

3.1.2 Le marché de la sécurité est en forte croissance

Selon l'enquête IDC Sécurité 2005[99], 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 2004 et 2003). 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% ;
- les appliances (boîtiers physiques intégrant de une à plusieurs fonctionnalités : pare-feu/VPN, anti-virus, anti-spam, prévention et détection d'intrusion,...(Cf. Annexe 12 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, le marché des produits logiciels de sécurité en 2003 les plus attractifs 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[100] 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 Md$ au niveau mondial en 2007.

[99] 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

[100] Source Les Echos / Eurosmart

3.1.3 Caractéristiques de quelques marchés logiciels et matériels de SSI

Selon IDC 2005[101]

Segment	Croissance du marché/an (2004-2009)	Marché national (M€) en 2004	Principaux acteurs	Présence française	Produit logiciel libre public	Criticité des produits
Logiciels : Anti–virus, Anti-spam et Spyware (segment SCM[102])	16%	157	Symantec, Network Associates (MC Afee), Trend, Sophos ...	Non	Oui, ClamAV	Non
Pares – feu / VPN (appliances)	2%	47	Check Point, Cisco,...	PME	Oui, netfilter, IP filter	Oui
Pares-feu (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)[103]	13%	88	IBM, Computer Associates, Verisign,...	GE[104] et PME		Oui

Des données complémentaires sont fournies en annexe 12 sur les différents logiciels et matériels de SSI : anti-virus, coupe-feu, détection d'intrusion, administration sûre, authentification renforcée, VPN, sécurité messagerie, chiffrement de fichiers, mémoires de masse et téléphone chiffrant.

3.1.4 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.

[101] 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

[102] Secure Content Management – Cf. annexe 12

[103] 3A pour Authentification, Autorisation et Administration - ou management des identités et de l'accès – Cf. annexe 12

[104] GE: Grande Entreprise

Le classement IDC 2003[105], 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[106]), Check point (Israël-EU), Network Associates (EU), IBM (EU), Trend micro (EU), Sophos (RU[107]), 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**[108]

	Télécoms	Banque / Finance	TV	Gouvernement / Santé	Transport	Sécurité
Volumes en millions d'unités	1220	330	65	60	25	15
% de croissance	+ 16%	+ 18%	+ 18%	+ 33%	+ 67%	+ 25%

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.

3.1.5 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 une taux de croissance moyenne de 18,2% par an sur la période 2004/2009.

[105] IDC 2003, Western European security software forecast and competitive vendors shares, 2003-2008
[106] EU : Etats-Unis
[107] Royaume-Uni
[108] Source Les Echos / Eurosmart

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 Etats-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 24h 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 3 – 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[109]) 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 multi clients 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.

[109] 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.

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

3.1.6.1 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 dés organisations (restriction des droits d'un utilisateur sur sa propre machine).

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

3.1.7 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 coupes-feu. A 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'Etat, 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.

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

3.2.1 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 leader 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'Etat.

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'Etat :

- 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 23M€ entre 2001 et 2004 ont été consacrés au thème SSI[110].

- 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.

A 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.

[110] Source Ministère de la Recherche

Enfin, on peut noter la montée en puissance des pôles de compétitivité dont certains intègrent les questions de SSI notamment en Ile de France (System@tic), en PACA (solutions de communications sécurisées) et Rhône-Alpes (Minatec) ou de transactions électroniques sécurisées en Basse-Normandie.

En ce qui concerne la Commission européenne :

Le 6è 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[111]. De plus la Commission a lancé une action préparatoire, en vue du 7ème PCRD, dotée d'un budget prévisionnel de 65 millions d'euros pour la période 2004 – 2006, concernant la recherche de sécurité :

- 6è 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[112] ;
- 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 ;
- 7è 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[113] 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'Etat dans de telles actions est nécessaire; mais la volonté et les financements semblent encore incertains.

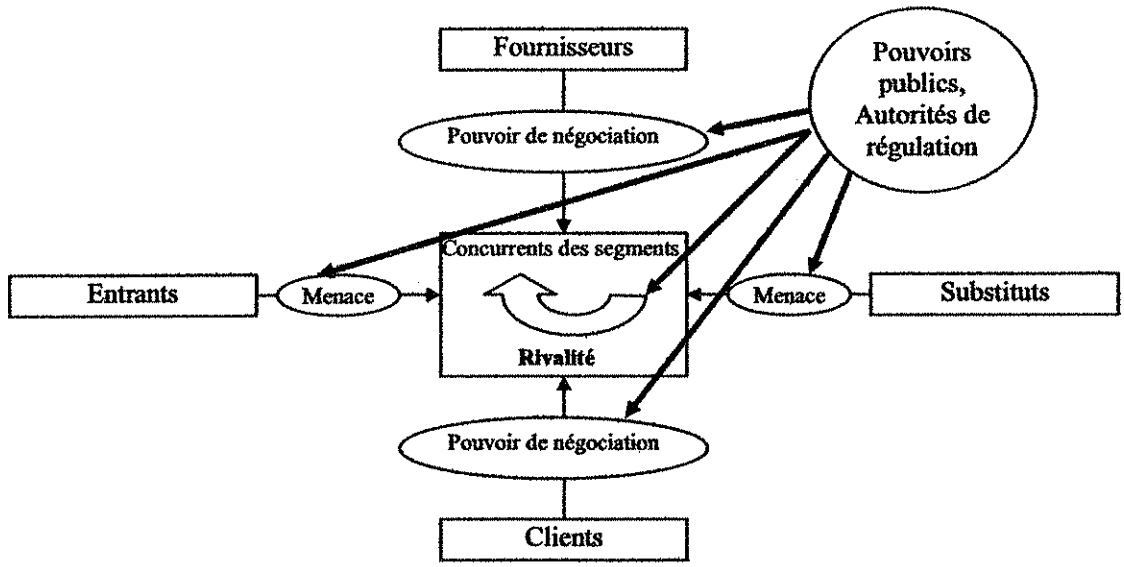
3.2.2 La situation des PME fournisseurs de produits et services SSI est très critique

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.

[111] Source Commission européenne
[112] Source Commission européenne
[113] Source auditions

3.2.2.1 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'Etat 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'Etat **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'Etat 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[114] 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. A ce niveau d'activité, elles devraient pouvoir générer suffisamment de cash flow pour continuer à innover et financer leur R&D.

L'Etat 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**.

- **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.

[114] Source auditions

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'Etat 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.**

3.2.2.2 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 Etats-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 Etats et aux grands donneurs d'ordres européens sans barrières spécifiques **doit être un objectif de l'Etat** 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 Etats-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.

3.2.2.3 Les politiques d'achat de l'Etat 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'Etat, 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[115] 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'Etat 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.

A 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. A cela s'ajoute 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.

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

3.2.2.4 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[116] et la transmission / cession [117].

Certes, les mesures gouvernementales ont été nombreuses ces dernières années :

- développement des FCPI[118] et d'Alternext ;

[115] Plan de Renforcement de la Sécurité des Systèmes d'Information de l'Etat (2004-2007) du 10 mars 2004

[116] 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.

[117] 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

- 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[119] ;
- 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.

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 Etats-Unis est différente : la taille du marché intérieur et les sources de financement disponibles leur permettent de se dispenser de financement 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,** serait 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 Economique 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

[118] Fonds Communs de Placement dans l'Innovation
[119] Leveraged By Out : opération d'acquisition d'une entreprises financée par un fort recours à l'endettement

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**[120] :

- en 2003, le financement de la R&D en TIC était de 90 $ par habitant en France, contre 220-240 $ aux Etats-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 Etats-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 Etats-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).

Ainsi, le financement de la R&D par les grandes entreprises françaises et européennes étant proportionnellement plus faible que celui des entreprises concurrentes aux Etats-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[121] ;
- 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[122],...) ;
- 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 Etats-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.

A 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

[120] Source : Futuris et Conseil Stratégique des Technologies de l'Information -Groupement Français de l'Industrie de l'Information octobre 2003.
[121] Doublement de 5 à 10% de la part en volume des dépenses de recherche prises en compte
[122] Programme d'Etudes Amont

particulières pour favoriser le recrutement de compétences par des PME, notamment en marketing des technologies[123], 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 ;
- 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)[124] ;
- 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...

3.2.3 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.

3.3 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.

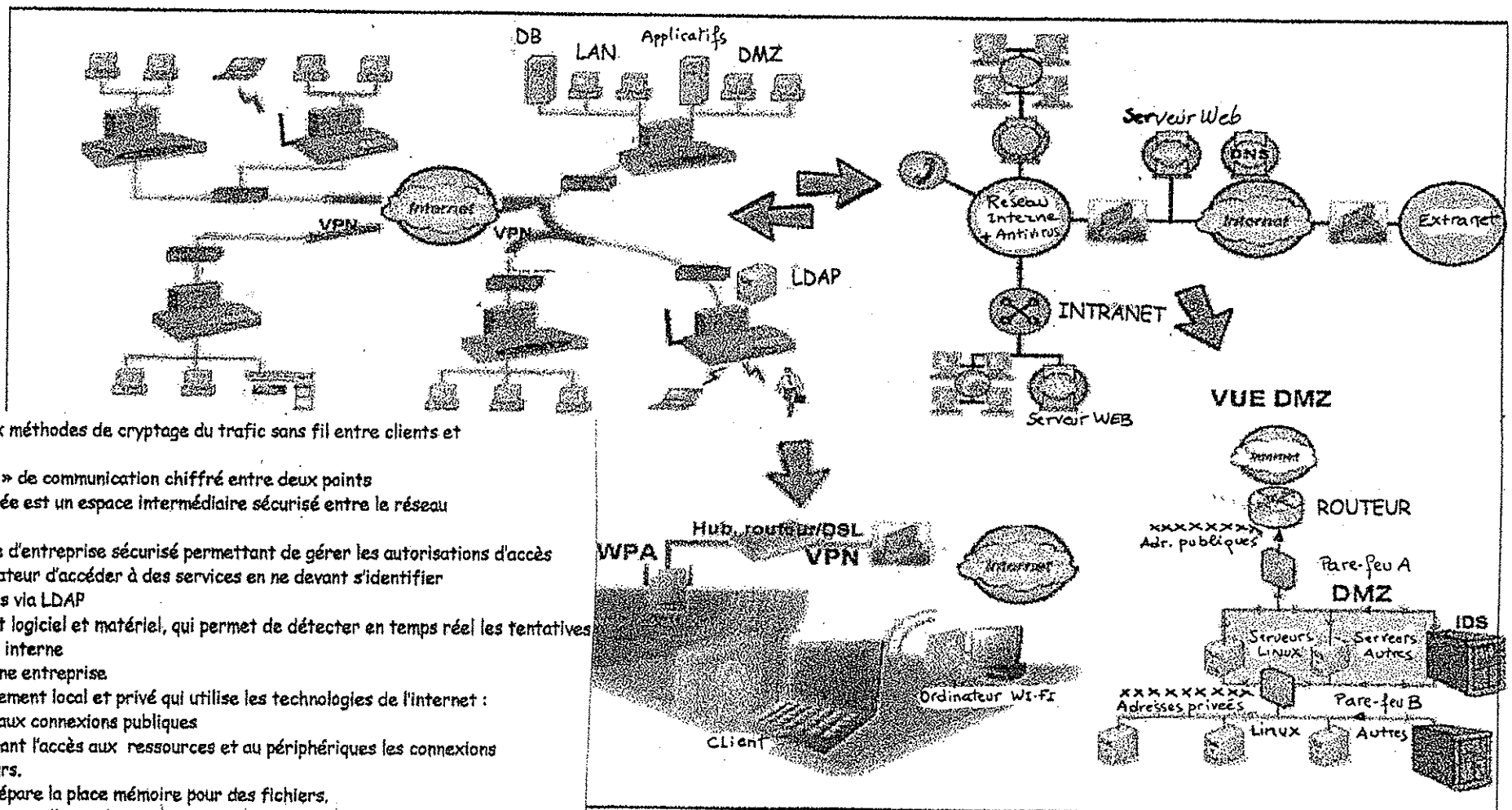
[123] Source auditions
[124] Source auditions

ANNEXE 1

Organismes

- ADAE : Agence pour le Développement de l'Administration Electronique ;
- BRCI : Brigade Centrale de la Répression de la Criminalité Informatique ;
- CCSDN : Commission Consultative du Secret de la Défense Nationale ;
- CEMA : Chef d'Etat Major des Armées ;
- CEMAA : Chef d'Etat Major de l'Armée de l'Air ;
- CEMAT : Chef d'Etat Major de l'Armée de Terre ;
- CMM : Chef d'Etat Major de la Marine ;
- CERT-RENATER : centre d'alerte et de réponse aux attaques informatiques dédié aux membres de la communauté GIP-RENATER – REseau 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'Evaluation 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 Etudes 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 Etudes 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.

- Schéma de principe des systèmes d'information



WEP ET WPA sont deux méthodes de cryptage du trafic sans fil entre clients et ports d'accès sans fil

Un VPN est un « tunnel » de communication chiffré entre deux points

DMZ ou zone démilitarisée 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 q'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 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 au périphériques les connexions des différents utilisateurs.

Un serveur de fichier prépare la place mémoire pour des fichiers,

Un serveur d'impressions et exécute les sorties sur imprimantes du réseau

Un serveur d'application rend disponible sur son disque dur des programmes « partagés »

CNS : permet d'effectuer la corrélation entre les adresses et le nom du domaine associé

ANNEXE 3

– 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 englobe 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 matérialisé 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, quelque soit 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, à 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 (*), de leur fournir un vade-mecum pour les aider dans cette mission et d'actualiser régulièrement ce document.

(*) 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 4

– 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. Evaluer 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 5

ANNEXE 12. – Exemples de chartes d'utilisateurs dans les entreprises et l'Etat[139]

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'Etat.

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 ;
  - 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,...) ;

[139] Sources auditions

- 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 affectée ;

- 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.

- ...

POLYNESIE FRANÇAISE

MINISTERE
DU TRAVAIL, DE L'EMPLOI,
DE LA FORMATION PROFESSIONNELLE
ET DE LA FONCTION PUBLIQUE,
chargé de la réforme de l'administration,
des relations avec l'Assemblée de Polynésie française
et le Conseil économique, social et culturel

SERVICE DU PERSONNEL
ET DE LA FONCTION PUBLIQUE

CONCOURS EXTERNE POUR LE RECRUTEMENT DE 03 INGENIEURS EN CHEF DE CATEGORIE A RELEVANT DU STATUT DE LA FONCTION PUBLIQUE DE LA POLYNESIE FRANCAISE

UNE NOTE DE SYNTHESE

Mardi 28 février 2006 de 12h30 à 16h30 (4 heures) (Coefficient 5)

Aucun document n'est autorisé, ni même l'usage de la calculatrice.

Le sujet comporte 100 pages.

CONCOURS EXTERNE D'INGENIEURS EN CHEF DE CATEGORIE A

REDACTION D'UNE NOTE DE SYNTHESE

Sujet :

La sécurité des informations par Internet est une préoccupation majeure de l'Etat.
En vous appuyant sur le rapport du député Pierre LASBORDES (document joint de 99 pages) vous rédigerez une note de synthèse de 4 à 6 pages maximum mettant en évidence les menaces qui pèsent sur l'utilisation de cet outil, puis vous comparerez l'organisation des SSI des principaux partenaires étrangers au système français. Enfin, vous justifierez la création et l'autonomie d'une base industrielle et technologique spécialisée en SSI pour gérer les informations.

La sécurité des systèmes d'information

Un enjeu majeur pour la France

Pierre LASBORDES
Député

Le 26 novembre 2005

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, qui m'a apporté compétence et expérience.

M. Roger BALERAS, *ancien Directeur des applications militaires du CEA* ;
M. Jean-Paul GILLYBOEUF, 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 LACARRIERE, *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 Ecole normale supérieure ULM, Directeur du département informatique*
M. Jean-Pierre VUILLERME, *Directeur des services environnement et prévention du groupe Michelin.*

Je tiens à remercier également 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

Le nom 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.

Sommaire détaillé

ANNEXES

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.

Si 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 modifié considérablement 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 toute entière.

Les Etats-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 Etats-Unis dominent le monde, donne à notre nation un avantage unique »[1].

Pour l'Etat 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 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-

[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*

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'Etat 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, en 2001, aux Etats-Unis, un préjudice de 59 milliards de dollars aux mille premières entreprises américaines. L'exemple le plus spectaculaire porte sur la révélation[2], en juin 2005, des agissements d'une entreprise israélienne qui « louait » un cheval de Troie[3] 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 permettant 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'Etat d'une adaptation nouvelle et urgente, dans la logique de l'Etat stratège.

[2] http://solutions.journaldunet.com/0506/050603_espionnage_industriel_israel.shtml

[3] Cheval de Troie : programme qui exécute des instructions sans l'autorisation de l'utilisateur 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.

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.

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.

SYNTHESE

SECURITE DES SYSTEMES 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, le réseau de commandement des forces armées sont des systèmes d'information.

I- 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, 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 vulnérabilités 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'Etat 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.

II- 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[4], la DCSSI[5] 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[6], elle a mis en place un centre opérationnel de la sécurité des systèmes d'information (COSSI), activé en permanence, 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.

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[7], 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

[4] Secrétariat général de la défense nationale

[5] Direction centrale de la sécurité des systèmes d'information

[6] Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques

[7] Centre de formation à la sécurité des systèmes d'information

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[8], 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 cybercriminalité. Dans le cadre de ses missions, 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'OCLCTIC[9] , est une structure à vocation interministérielle placée au sein de Direction de la police judiciaire (DCPJ). Elle lutte contre les auteurs d'infractions liées aux TIC, enquête à la demande de l'autorité judicaire, 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, donnent 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'Etat 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[10] 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 (Etats-Unis, Royaume-Uni, Allemagne, Suède, Corée du Sud et Israël) et aborde les initiatives multilatérales (Union européenne,

[8] Agence pour le Développement de l'Administration Electronique, rattachée au ministre chargé du budget et de la réforme de l'Etat

[9] office central de lutte contre la criminalité liée aux technologies de l'information et de la communication

[10] Haut fonctionnaire de Défense

OCDE, ONU, G8, réseaux de veille et d'alerte). On ne retiendra dans cette synthèse que le cas de l'Allemagne.

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 DCSSI, 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 de 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'Etat 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.

III - Base industrielle et technologique

Les Etats-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 (anti spam, anti-virus,...), 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'Etat et des grands donneurs d'ordres ne sont pas favorables aux PME innovantes. A 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 secteur 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 ministère 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 la compétence et l'expérience particulière de la France (en particulier de ses centres d'évaluation) soient 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 approuvé au préalable.10 produits ont déjà été qualifiés et 7 sont en cours de qualifications. La moitié de ces produits sont développés 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.

IV – SIX RECOMMANDATIONS

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

- Etablir 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 ;
- Etablir 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'Etat 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'Etat** 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'Etat en 2004.

UN IMPERATIF

Refondre l'organisation de la SSI de l'Etat

En complément aux six axes de recommandations, afin d'amener notre pays à un niveau de sécurité et d'autonomie, il faut **renforcer l'action de l'Etat** et ses moyens humains et financiers en matière de SSI, **rationaliser l'organisation** des services de l'Etat 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, qui ne semble plus adaptée aux enjeux actuels.

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 ;

- 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,** seraient 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 principe de gouvernance garantissant la confiance, l'implication des personnels, la transparence et la neutralité** et **évaluée sur ses activités**, notamment de support, de communication et de formation, selon des critères de performance et de qualité.

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, 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 le champs couvert et leur complexité (voir schéma en annexe 4) 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'Etat 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 Galiléo ;
  - 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 radio-électriques, 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 (allègement 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.

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

Analyser et comprendre les menaces et les vulnérabilités nécessitent 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 (principe de la vision de Clausewitz) car il n'y a pas de légitime défense en SSI[11] 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 :

[11] Stanislas de MAUPEOU, article Revue Défense nationale, novembre 2003

- 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 pares-feu protègent uniquement des attaques résiduelles (i.e. qui ne correspondent pas aux services offerts)[12] ;
- 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).

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 aux fins de protéger les ressources et les informations contre tout préjudice et également prévoir le cas de la faillite de la protection.

Pour être mise en œuvre sur un plan opérationnel, cette politique de sécurité s'adosse 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.

1.2 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 5).

[12] 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/) ;

• **L'AFNOR[13] 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, Internet,....

- « 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 LIMITEE**

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 conséquences qu'aurait leur divulgation, leur altération, leur indisponibilité ou 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 LIMITEE.

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'informa tique, 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.

1.3 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 ;

[13] Association française de normalisation.

- **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 aux fins de lui soutirer de l'information via l'« ingénierie sociale »[14] 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 une porte blindée à l'entrée d'une maison, mais en laissant les fenêtres ouvertes.*

1.3.1 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 (ordinateurs accessibles en ligne !! ce qui n'a pas beaucoup de sens). Pensant avoir à faire à un jeu, il choisit le déclenchement de la 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 (Etat, 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 moteur dans des actes délictueux. Il est cependant utile de

[14] 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.

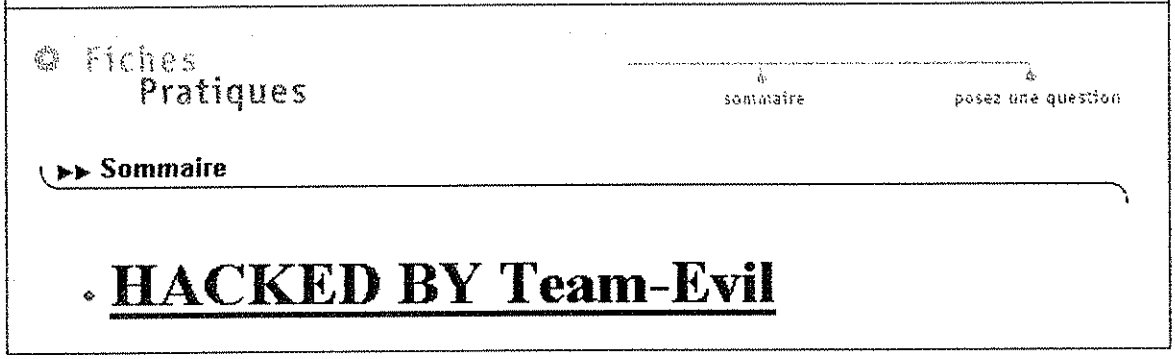
chercher à les comprendre pour mettre en place des stratégies et des tactiques de réponses adaptées.

On distingue traditionnellement 4 types d'attaques qu'ils nous semblent utile ici de rappeler 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[15] : 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 Etat, 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.

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

Profils des attaquants

Sans détailler tous les profils (cf. Annexe 6), on retiendra le plus connu ; les « hackers »[16] 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.

1.3.2 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[17] dans le cadre de la lutte contre le terrorisme »[18]), 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. »

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 ...) ; 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,...) ; les réseaux de communication (téléphone filaire, cellulaires, réseau Internet,...) y compris ceux des forces de police et de la défense.

[16] 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 systèmes d'information seront préférés.

[17] Il est opportun de préciser la distinction faite entre la terminologie française « infrastructures vitales » et anglo-saxonne « *critical infrastructures* »

[18] http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/com/2004/com2004_0702fr01.pdf

L'interdépendance entre certaines de ces infrastructures génère également des facteurs de risques en terme de réaction en chaîne qui doivent conduire l'Etat 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 domaines 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 anti virus ou les pares-feu mais la vigilance de l'utilisateur est primordiale ainsi qu'une véritable politique de mise à jour des applications.

- **L'Etat : une cible de choix**

A titre d'exemple, le Ministère de la Défense Américain (Department of defense) est le plus attaqué au monde, avant Microsoft[19]. Preuve en est aussi le succès des sites gouvernementaux (extension .gov aux Etats-Unis, .gouv.fr en France) sur les pages référençant les défigurations, « considérées spéciales»[20].

Si la défiguration d'un site peut sembler banale et sans conséquence autre que l'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.

[19] Source auditions

[20] Défigurations spéciales : http://www.zone-h.com/en/defacements/special

- **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[21] 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 toutes 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.

1.3.3 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).

[21] http://solutions.journaldunet.com/0506/050603_espionnage_industriel_israel.shtml

Liaisons transatlantiques
Le réseau TAT-1422, assure une partie du transit Internet entre l'Europe et les Etats-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.

- **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 de l'art actuel, 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.

1.3.4 Les vecteurs d'attaques sont multiples et témoignent d'une complexité croissante

1.3.4.1 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...), **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.

[22] A propos de TAT-14 : https://www.tat-14.com/tat14/

La miniaturisation des moyens de stockage, comme les clés USB[23], 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,...) **ont accès aux locaux**.

1.3.4.2 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 leurs vulnérabilités les rendent 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 la confidentialité, par écoute des émissions radioélectriques du réseau.

La menace TEMPEST[24] :

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.

[23] Une faille de sécurité concernant l'utilisation des clefs USB a été mis 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 consulter toutes les données. Cette faille est propre à la technologie USB et non au système d'exploitation, ce qui signifie que tous les systèmes sont potentiellement vulnérables.

[24] 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

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 Ile-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...

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.

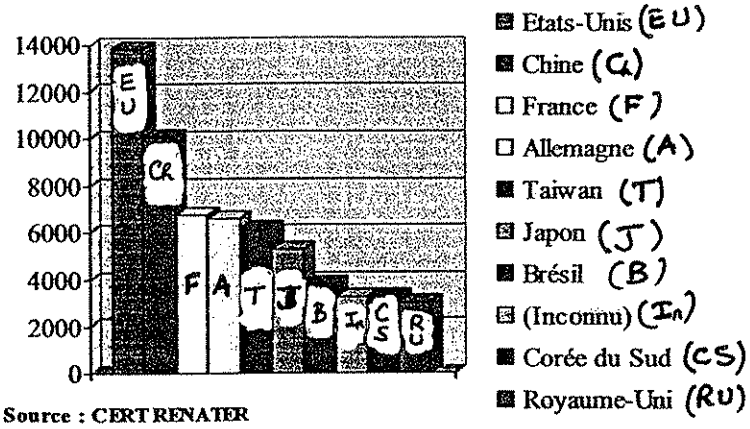
Considérant, par exemple, l'intérêt que pourrait trouver un concurrent à lire à distance l'ensemble du flux logistique de distribution d'un industriel, et dans la mesure où ce type de technologie est envisagé pour transmettre des données personnelles (sur des passeports par exemple) l'emploi de la technologie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

1.3.4.3 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'information sur le système ou réseau ciblé. A 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.



Source : CERT RENATER

Provenance des « scans »

Au mois d'octobre 2005, 104219 sources distinctes ont sondé des machines sur le réseau RENATER[25].

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

[25] RENATER : Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche

- **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.

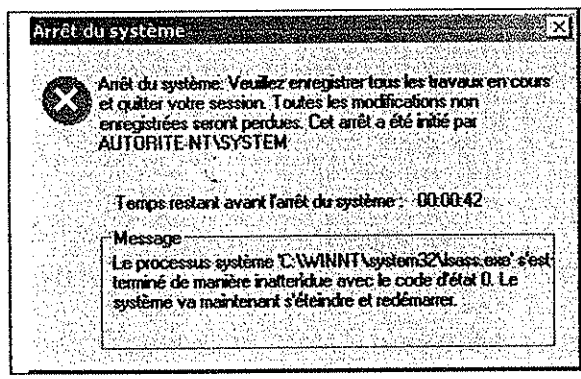
- **L'altération et la destruction :** il peut s'agir d'altérer ou de détruire des données stockées sur le système, ou bien le système lui-même, avec des finalités diverses. Au-delà des implications financières et industrielles évidentes, le but poursuivi peut être la dégradation des mécanismes de protection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

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 tous premiers vers sont apparus en 1982. On retiendra la déferlante médiatique d'**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 $. 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**[26].



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**[27].

Se propageant entre PC sous Windows sans firewall grâce aux connexions réseau, il a longuement fait parler de lui en mai 2004.

[26] Source auditions

[27] http://www.sophos.fr/virusinfo/analyses/w32sassera.html

- **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.

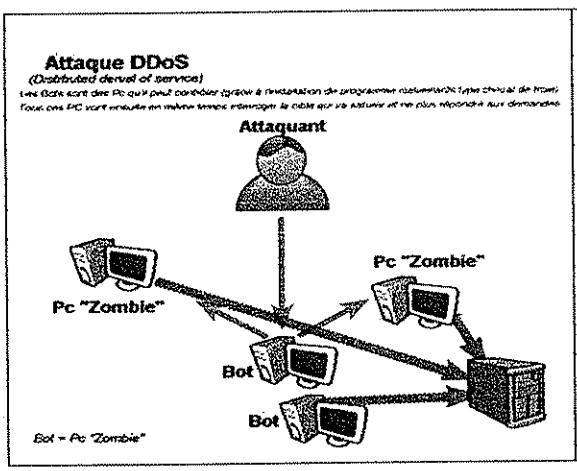
  A titre d'exemple, dans un grand groupe[28] , 5% des courriels échangés en 2004 ont été interceptés et éradiqués. Mais il faut aussi et surtout tenir compte de tout ce qui ne se détecte pas à cause de mise à jour non effectuée ou de vulnérabilité encore inconnue. Les anti virus agissent par définition a posteriori. C'est précisément pour cela que la protection contre les virus ne peut et ne doit pas se limiter à un anti virus 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[29] 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. Ils peuvent provoquer des redémarrages intempestifs ou empêcher le téléchargement de correctifs tout en bloquant l'accès à certains sites Internet.

  Les attaquants dont la motivation est souvent financière, pour ne pas être détectés et préserver leur anonymat, ont de plus en plus tendance à mettre en place un réseau de machines devant rester invisible leur permettant, le moment venu, de relayer de manière massive à partir des machines infectées l'attaque désirée : des Spam, 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[30].



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

En 2002, pendant une heure, les treize serveurs de noms racine (dont 10 aux Etats-Unis), qui permettent directement ou indirectement, à tous les navigateurs de trouver les pages web demandées, à tous les emails 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.

[28] Sources auditions
[29] Source Sophos et Clusif
[30] Rapport "Internet Security Threat Report" de la société Symantec

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

- **Un Spam** est un courrier électronique d'exemplaires identiques, envoyé en nombre, de façon automatique et non sollicité[31].
  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. A titre d'exemple un grand groupe français[32] dans lequel 500 000 mails sont échangés chaque jour, en rejette 60 000, dont 31 000 Spam 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 Etats-Unis)[33]. 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,...). 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.

1.3.4.4 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.

1.3.4.5 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.

1.4 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

[31] 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).

[32] Source auditions

[33] Rapport "Internet Security Threat Report" de la société Symantec

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.

1.4.1 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 (patch) ; 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 7).

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** [34]

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,[35] 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[36].

- **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 de vol de données de l'entreprise alors que des mesures simples concernant

[34] 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).

[35] Source auditions

[36] Source auditions

l'utilisation de ces périphériques et leur traçabilité permettra de réduire sensiblement le niveau de risque.

D'après une enquête IDC[37], 71% des sondés jugent très préoccupante l'utilisation en privé d'équipements mobiles en particulier par les dirigeants.

1.4.2 Les organisations sources de vulnérabilités

L'utilisation des failles inhérentes à l'organisation d'une entité est également un moyen d'accéder à ses 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 %).

Une 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 de savoir-faire en matière d'administration de systèmes définitive ;

- **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.**

[37] Livre blanc IDC France – Internet Secutiy System (ISS) sur la sécurité des systèmes d'information – 100 entretiens auprès d'entreprises et d'administrations françaises – avril 2005

l'utilisation de ces périphériques et leur traçabilité permettra de réduire sensiblement le niveau de risque.

D'après une enquête IDC[37], 71% des sondés jugent très préoccupante l'utilisation en privé d'équipements mobiles en particulier par les dirigeants.

1.4.2 Les organisations sources de vulnérabilités

L'utilisation des failles inhérentes à l'organisation d'une entité est également un moyen d'accéder à ses 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 %).

Une 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 de savoir-faire en matière d'administration de systèmes définitive ;
- **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.**

[37] Livre blanc IDC France – Internet Secutiy System (ISS) sur la sécurité des systèmes d'information – 100 entretiens auprès d'entreprises et d'administrations françaises – avril 2005

1.4.3 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.

1.4.4 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.

1.5 Des enjeux futurs en matière de SSI

1.5.1 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 »[38].

[38] Source auditions

1.5.2 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.

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.**[39]

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.

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

Un enjeu de souveraineté nationale : l'Etat 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'Etat, des infrastructures vitales, et des entreprises sensibles.

En effet, l'Etat 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".

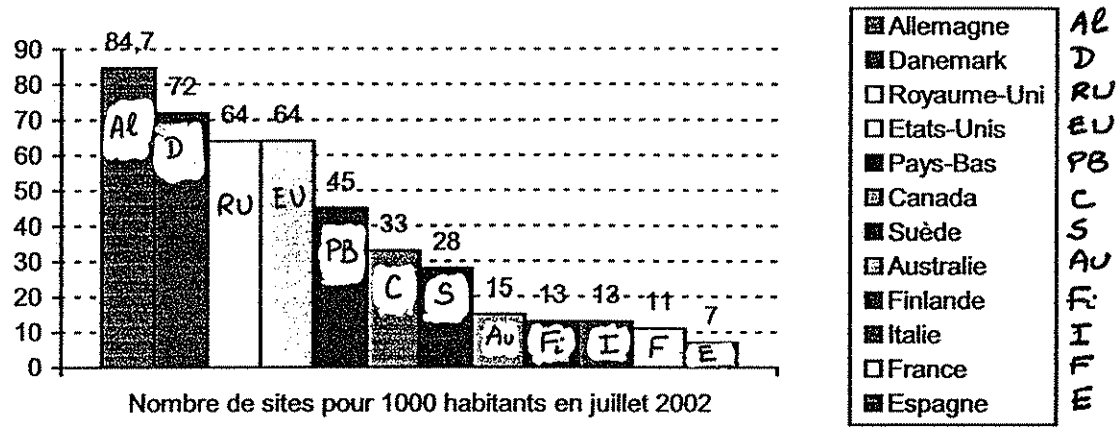
Les champs d'actions de la SSI et de l'Intelligence économique, se recoupent pour partie, car ils font la synthèse de l'économie de la connaissance, et donc de l'information. Pour être efficace, une politique volontariste d'Intelligence économique doit notamment s'appuyer sur des systèmes d'information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

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 Etats-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.

[39] Source auditions

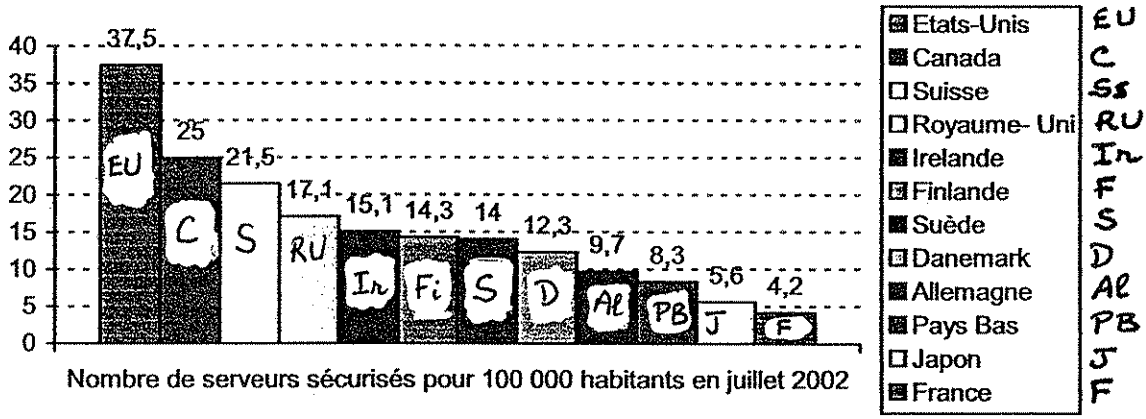
Un enjeu économique : un environnement sécurisé est nécessaire afin d'accompagner le rattrapage français dans l'usage des TIC par les citoyens et les entreprises françaises indispensable pour la croissance française.
Selon le tableau de bord du commerce électronique de décembre 2004[40] malgré un taux 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.



Nombre de serveurs sécurisés pour 100 000 habitants en juillet 2002

D'autres statistiques dans cette étude, relatives 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 Etats-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.

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

Dans un contexte de mondialisation croissante de l'économie et de concurrence soutenue, les entreprises françaises, mais aussi l'Etat, 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.

2 Les réponses organisationnelles et techniques

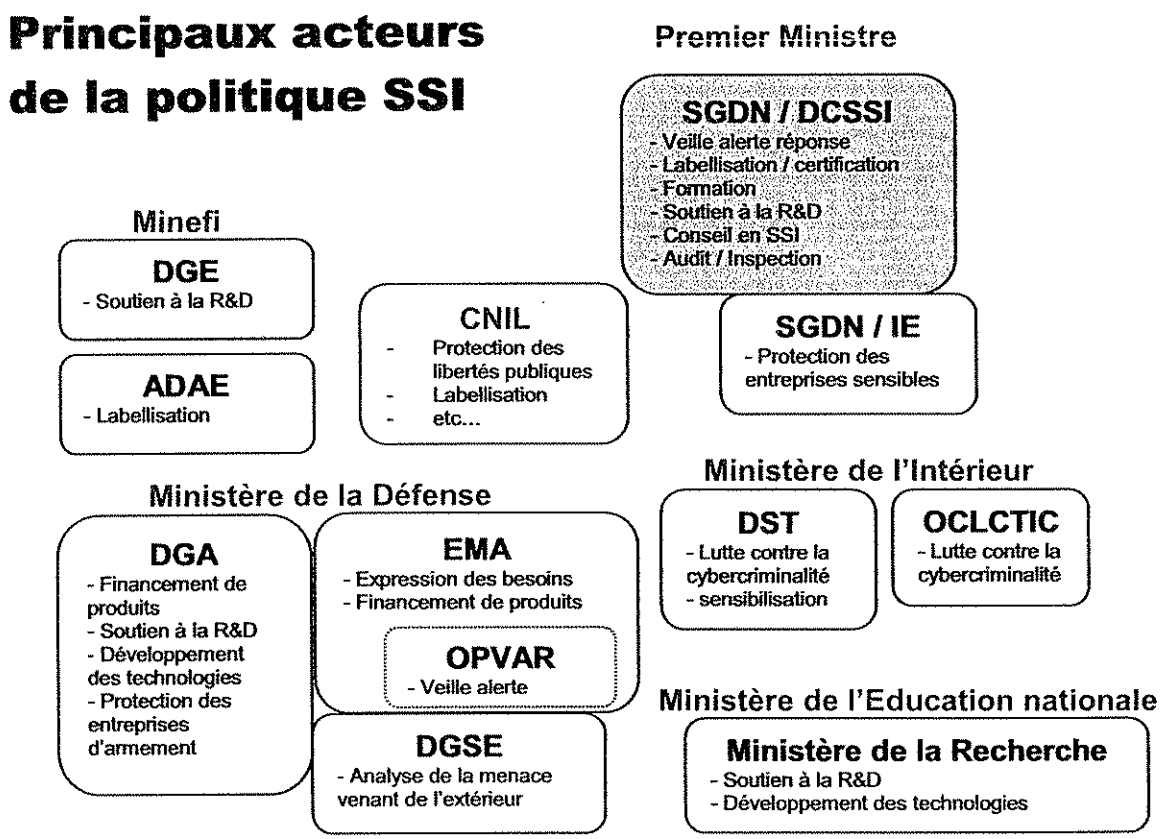
2.1 Comment l'Etat est-il organisé pour assurer la SSI ?

La sécurité est l'affaire de tous, mais l'Etat 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'Etat 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.

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

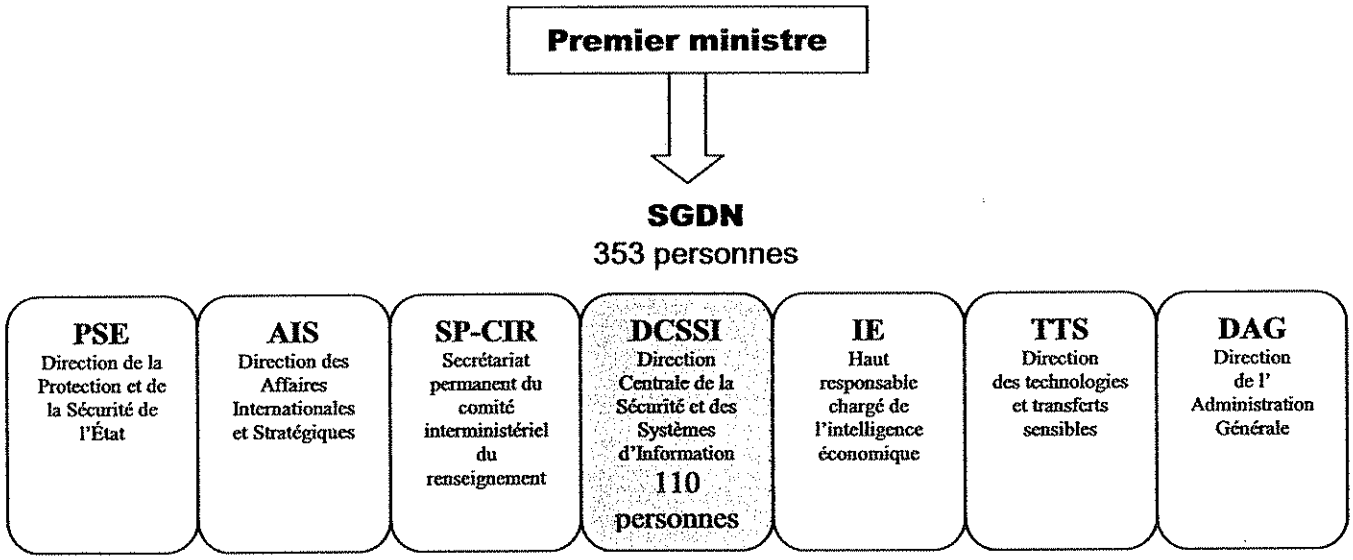
La réglementation en sécurité des systèmes d'information (SSI) n'existe pas sous la forme d'un code législatif ou réglementaire. La SSI n'est d'ailleurs pas même définie d'un point de vue juridique. En fait, le domaine de la SSI fait référence à une multitude de textes de niveaux juridiques très divers 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 9)

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



2.1.2.1 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[41] *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**[42] (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.

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.

[41] Décret n°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).

[42] Le décret 2001-69342 précise les missions de 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)**[43], 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 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 24h/24 7j/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[44] (centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques). Chacune de ces unités regroupe une dizaine de personnes. Les ministères et les opérateurs d'infrastructures vitales sont invités à signaler au COSSI les attaques dont ils sont victimes.

[43] Le décret n°2001-69443 précise le rôle de la CISSI

[44] 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).

- 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'Etat, 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)[45], 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. A titre d'exemples le CFSSI propose plusieurs degrés de stages[46] de haut niveau de spécialisation ou de simple sensibilisation, d'une durée d'une journée, ou après deux années de formation tel que le Brevet d'études supérieures de la sécurité des systèmes d'information (BESSSI). En 2004, pas moins de 898 stagiaires avaient suivi l'une ou l'autre des formations[47].
  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.

2.1.2.2 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.

[45] Décret 87-354 du 25 mai 1987
[46] cfssi@sgdn.pm.gouv.fr et www.formations.ssi.gouv.fr
[47] Source auditions

2.1.2.2.1 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)[48] 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)[49], 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[50].

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 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

[48] Cf. infra 2.1.2.3
[49] Voir glossaire
[50] Bientôt DGSIC

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 : la Direction générale de la sécurité extérieure

La DGSE a pour mission d'évaluer la menace provenant de l'étranger qui pèse sur les systèmes d'information.

2.1.2.2.2 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 : la Direction de la surveillance du territoire

Dans le cadre de ses missions de lutte contre l'espionnage, de la lutte anti-terroriste 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 créée 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 judicaire, 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 Ile 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'ADAE (Agence pour le Développement de l'Administration Electronique), 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'Etat.
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, aux 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'Etat.

2.1.2.2.3 Les conséquences de la multiplication des acteurs publics

La multiplication des acteurs publics dont les missions se chevauchent et les textes fondateurs peu précis, donnent **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'Etat 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 par exemple 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 ?

2.1.2.3 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.

A 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'Etat, 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)**

A 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.**

2.1.3 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[51], soit à recourir à l'externalisation[52].

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[53].

- 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 a « mettre en place une organisation conjointe de développement de produits de sécurité», présentée par le PRSSI, est à recommander.

2.2 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'Education 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 ;

[51] 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.
[52] Parfois retenue par certains ministères, le recours à l'externalisation doit être conditionné à un encadrement plus strict.
[53] 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.

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

L'Etat 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'Etat, 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'Etat 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.

2.4 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 Etats-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.

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

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

L'E*xecutive order* 12333 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 Etat.

La NSA a une double mission : protéger les systèmes d'information des Etats-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 13228 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'informations 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.

2.4.1.2 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'Etat, est l'homologue de la DCSSI. Au Royaume Uni, le NISCC[54], 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[55], chargé de recueillir des alertes et de signaler des incidents (mais sans capacité d'intervention) et des ISAC[56], 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,

[54] National Infrastructure Security Co-ordination Centre
[55] Warning, Advice and Reporting Point
[56] Information Sharing and Analysis Center

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[57] 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) pour une délivrance des premiers passeports à l'automne 2006. Par ailleurs, un nouveau programme de recherche (IADP[58]) a été mis en place afin d'optimiser les efforts dans le domaine SSI, en partenariat avec l'industrie.

2.4.1.3 Allemagne : une politique produit forte très tournée vers les utilisateurs

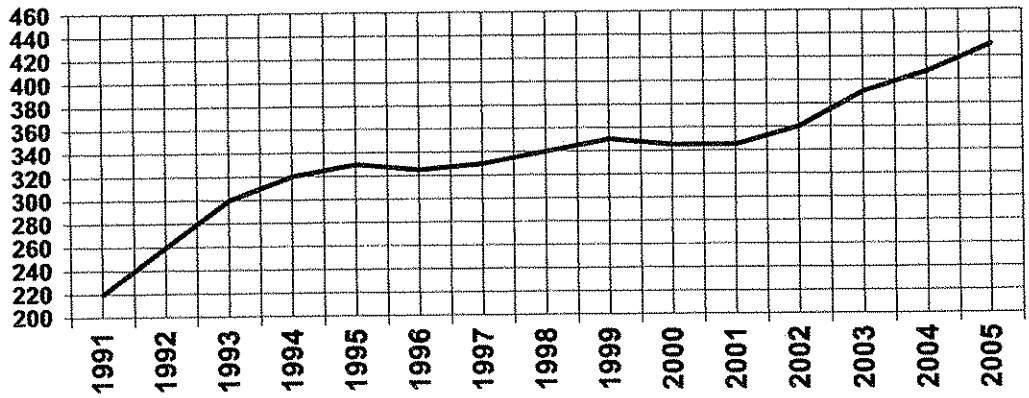
L'Allemagne a adopté en juillet dernier, un plan national pour la protection des infrastructures d'information (NPSI)[59] qui comporte trois objectifs principaux :

- 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.

Evolution 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** :

[57] General Information Assurance Products and Services Initiative – www.gipsi.gov.uk .
[58] Information Assurance Devleopment Programme.
[59] http://www.bmi.bund.de/nn_148134/Internet/Content/Nachrichten/Pressemitteilungen/2005/08/Information__Infrastructure__en.html .

- **Informer le pays**
  - o 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 ;
  - o en participant à des campagnes de sensibilisation des PME en 2004 (Sécurité de l'Internet pour les PME) ;
  - o 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 :**
  - o 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 ;
  - o 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 ;
  - o 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 ;
  - o 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 Etats-Unis, la Suisse, la Suède et la Finlande ;
  - o le BSI conseille également les Länder sur le plan technique.

- **Analyser les risques, évaluer et tester :**
  - o le BSI assure la certification des produits et services de SSI (38 en 2004) ainsi que l'attribution de licences pour des applications classifiées ;
  - o il a une action particulière sur les procédures biométriques et des applications mobiles ;
  - o 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.

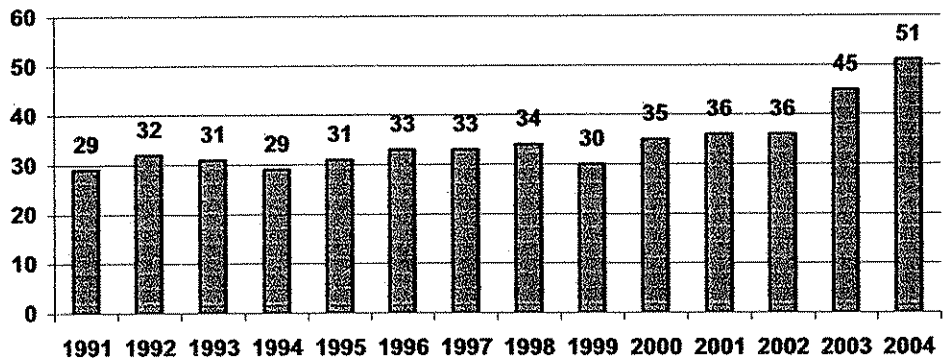
- **Assurer des fonctions opérationnelles :**
  - o assurer la fonction de CERT allemand (Computer Emergency Response Team) ;
  - o coordination technique du réseau d'information Berlin-Bonn ;

- 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.

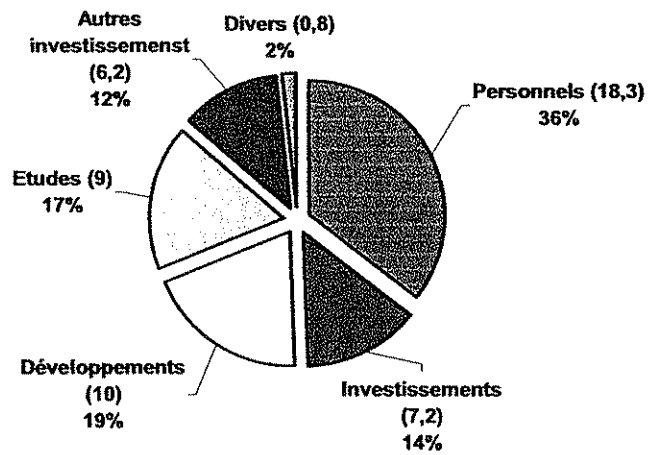
Pour assurer l'ensemble de ces missions, le BSI dispose d'un budget significatif de **51 millions d'euros** en augmentation régulière depuis 2002.

BUDGET en millions d'euros du BSI



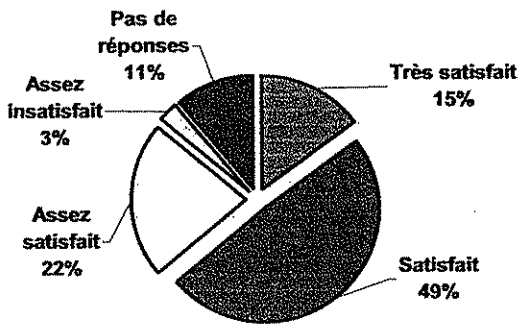
La répartition de ce budget, montre une action forte sur les développements, 10 M€, soit 19% du budget et les études pour 9 M€ soit 17% du budget que l'on ne retrouve pas en France.

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



2.4.1.4 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[60] pour les aspects organisationnels et l'IST[61] (appelé à remplacer le FRA[62]) 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.**

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

A 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

[60] Swedish Emergency Management Agency.
[61] Institute for Signals Intelligence and Technical Infosec.
[62] National Defence Radio Establishment.

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 6ème Bureau (domestic affairs) s'était vu adjoindre le Cyber Crime Group dont le personnel pourrait rejoindre le NCSC.

2.4.1.6 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'Etat 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).

2.4.1.7 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'Etat, 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)[63]. 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 Etats membres, et de coopérer de ce fait 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 Etats 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'Etat [...] ou aux activités de l'Etat 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)[64], de la deuxième commission sur le développement d'une

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

[64] Résolutions n° 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.

culture globale de la cybersécurité[65] et de la troisième commission sur la lutte contre l'utilisation criminelle des technologies de l'information[66]. 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 Etats-Unis et la Russie sur la prise en compte de l'utilisation des TIC à des 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[67] 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[68]), 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 Etats 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[69] 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 Etats-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

[65] Résolutions n° 57/239 du 20 décembre 2002 et 58/199 du 23 décembre 2003.
[66] Résolutions n°55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001.
[67] Union internationale des télécommunications.
[68] Working party in information security and privacy.
[69] www.oecd.org/sti/cultureofsecurity .

en œuvre des « bonnes pratiques » dans le domaine de l'alerte et de la veille informatique (CERT) ; la 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[70] et à l'échelle européenne au sein de la TF-CSIRT[71] 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, (Etats-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 Etats 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).

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

2.5.1 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 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[72] qui met en évidence les principaux sinistres chez les grandes et moyennes entreprises on notera que:

[70] Forum of Incident Response and Security Teams.

[71] Task Force to promote the collaboration between Computer Security Incident Response Teams.

[72] 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%)

- **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[73].

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

D'après une étude de l'institut américain en sécurité informatique CSI[74], 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 pas de données statistiques précises qui permettent d'avoir une vision précise du phénomène.

[73] Source Minefi

[74] CSI/FBI Computer Crime and Security Survey – 2005 – Enquête auprès de 700 entreprises et organisations publiques américaines

- **Des protections insuffisantes, en particulier dans les PME** (Etude 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.

2.5.2 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 oeuvre d'une 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[75], 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 ;

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

- mettre en œuvre un plan de sauvegarde ;
- gérer et maintenir les politiques de sécurité.

- **A 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 Etats ;
- 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.

2.5.3 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[76], 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 : Etude 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.

[76] 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

- **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**.

- **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 la SSI efficace par rapports aux besoins 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[77] 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).

[77] Source auditions

- **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[78]. 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 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**[79]. La motivation à investir dans la SSI varie de manière considérable selon la taille de l'entreprise.

[78] Source auditions

[79] Source auditions

2.5.4 Des modèles organisationnels diversifiés pour parer aux menaces et risques informatiques

2.5.4.1 Quelques exemples d'organisations[80]

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 ;
  - 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 H24 7/7 ;
  - 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 11 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

[80] Source auditions

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.

2.5.4.2 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[81] (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[82] 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[83], 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[84] 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[85], 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 2006.

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[86].

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

[81] Managed Security Service Provider
[82] CSO Entreprise & Sécurité de l'Information – Enquête auprès de 144 entreprises de plus de 200 salariés
[83] 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
[84] Source L'Agefi
[85] Source Syntec et 01 Informatique
[86] Source L'Agefi

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 :

- 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 oeuvre. A cet effet, les récents travaux conduits par l'AFNOR, le CIGREF et le SYNTEC sur ce thème sont à signaler.

2.5.5 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 Etats-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.[87]

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

2.5.6 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...

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.

[87] Source auditions

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 24h/24h et 7j/7j 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.

2.5.7 Les entreprises attendent de l'Etat 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'Etat ont des difficultés à **identifier rapidement le bon interlocuteur**[88] parmi les nombreux services de l'Etat.

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'Etat 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

[88] Source auditions

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.

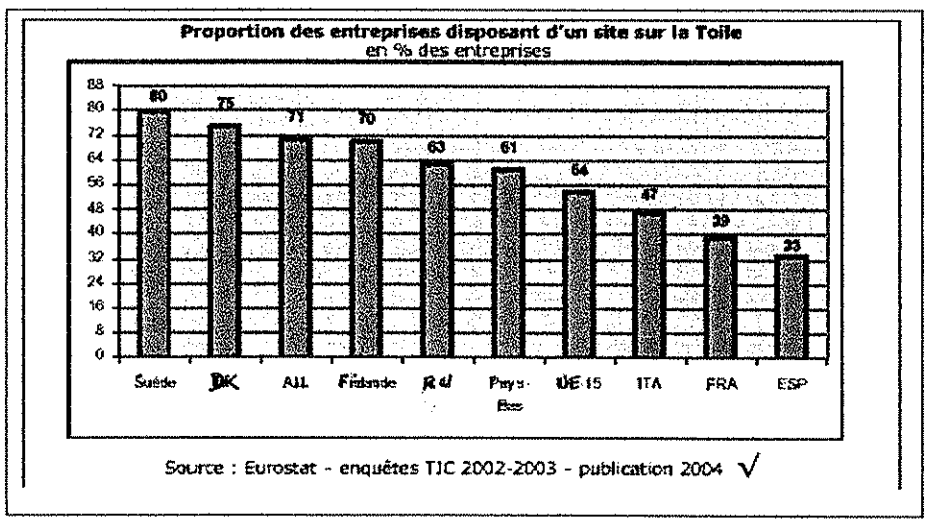
Les entreprises intervenant à l'international **souhaitent** disposer d'un support efficace des services de l'Etat pour les accompagner face aux risques spécifiques de l'international : veille, alertes, informations sur les menaces, conseils (juridiques, procédures, méthodologie, outils et solutions, 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 Etats** devient problématique pour la politique de sécurité de grands groupes[89].

2.5.8 Les problématiques spécifiques des PME face à la SSI

2.5.8.1 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'Economie Numérique 2004[90], 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.



[89] Source auditions

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

- **Les PME françaises sont elles-même 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.

Ces données sont confirmées par cette même étude de la Mission pour l'Economie 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.**

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

La part manufacturière est plus importante qu'aux Etats-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 Economie Numérique.

2.5.8.2 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[91], workflow[92],...

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[93] 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'Etat en matière de politique « qualité », à travers les

[91] Stockage de données

[92] Outils informatiques de gestion de flux de travail des entreprises qui permet d'optimiser leurs processus métiers clés.

[93] Source Le Monde Informatique

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.
Ainsi, l'AFNOR[94] 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**

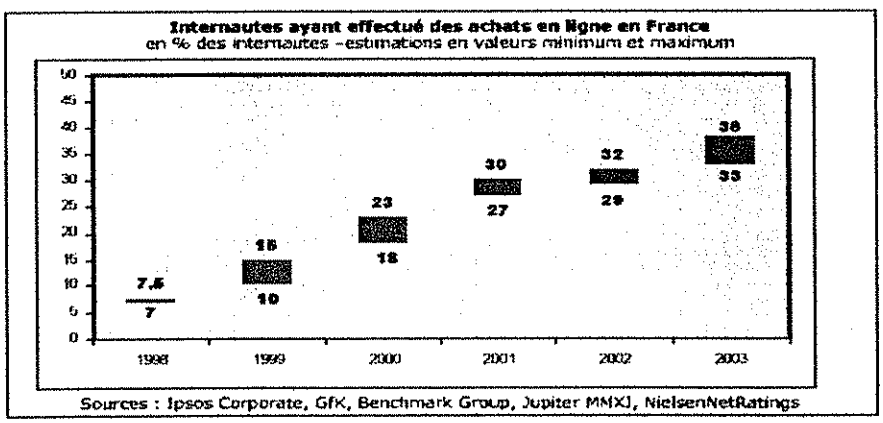
Les tendances du marché et surtout les positionnements pris par de nombreux acteurs informatiques le démontrent, **les PME apparaissent comme un futur marché en croissance en matière d'infogérance et de services de sécurité informatique** afin de compenser leurs déficiences internes qui les obligent 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[95]. 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.

2.6 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. A 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 oeuvre.



[94] Source auditions
[95] Source 01 Informatique

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[96]. Ce type d'action est à amplifier.

2.7 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'Etat 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'Etat 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 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?

[96] Source Délégation aux usages de l'Internet

3 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'informations 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.

3.1 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[97]. Ils ne sont pas habituellement inclus dans le marché de la SSI ;

[97] Digital Right Management (gestion des droits numériques) : protection des contenus vidéos et audios, notamment soumis à des droits d'auteur, diffusés sur Internet

- 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 multi niveaux.

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.

3.1.1 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[98] 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 Etat relèvent d'exigences de souveraineté et de sécurité des biens et des personnes.

Pour répondre à ces besoins, les attentes concernent des **produits logiciels** (anti-virus, pares-feu,...), 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:

[98] La sécurité des systèmes d'information dans les entreprises françaises en 2004, vision comparée de la France et du monde ; Ernst&Young , décembre 2004

- *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 (anti spam, anti-virus,...), 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).

3.1.2 Le marché de la sécurité est en forte croissance

Selon l'enquête IDC Sécurité 2005[99], 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 2004 et 2003). 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% ;
- les appliances (boîtiers physiques intégrant de une à plusieurs fonctionnalités : pare-feu/VPN, anti-virus, anti-spam, prévention et détection d'intrusion,...(Cf. Annexe 12 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, le marché des produits logiciels de sécurité en 2003 les plus attractifs 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[100] 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 Md$ au niveau mondial en 2007.

[99] 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

[100] Source Les Echos / Eurosmart

3.1.3 Caractéristiques de quelques marchés logiciels et matériels de SSI

Selon IDC 2005[101]

Segment	Croissance du marché/an (2004-2009)	Marché national (M€) en 2004	Principaux acteurs	Présence française	Produit logiciel libre public	Criticité des produits
Logiciels : Anti–virus, Anti-spam et Spyware (segment SCM[102])	16%	157	Symantec, Network Associates (MC Afee), Trend, Sophos ...	Non	Oui, ClamAV	Non
Pares – feu / VPN (appliances)	2%	47	Check Point, Cisco,...	PME	Oui, netfilter, IP filter	Oui
Pares-feu (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)[103]	13%	88	IBM, Computer Associates, Verisign,...	GE[104] et PME		Oui

Des données complémentaires sont fournies en annexe 12 sur les différents logiciels et matériels de SSI : anti-virus, coupe-feu, détection d'intrusion, administration sûre, authentification renforcée, VPN, sécurité messagerie, chiffrement de fichiers, mémoires de masse et téléphone chiffrant.

3.1.4 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.

[101] 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

[102] Secure Content Management – Cf. annexe 12

[103] 3A pour Authentification, Autorisation et Administration - ou management des identités et de l'accès – Cf. annexe 12

[104] GE: Grande Entreprise

Le classement IDC 2003[105], 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[106]), Check point (Israël-EU), Network Associates (EU), IBM (EU), Trend micro (EU), Sophos (RU[107]), 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**[108]

	Télécoms	Banque / Finance	TV	Gouvernement / Santé	Transport	Sécurité
Volumes en millions d'unités	1220	330	65	60	25	15
% de croissance	+ 16%	+ 18%	+ 18%	+ 33%	+ 67%	+ 25%

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.

3.1.5 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 une taux de croissance moyenne de 18,2% par an sur la période 2004/2009.

[105] IDC 2003, Western European security software forecast and competitive vendors shares, 2003-2008
[106] EU : Etats-Unis
[107] Royaume-Uni
[108] Source Les Echos / Eurosmart

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 Etats-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 24h 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 3 – 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[109]) 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 multi clients 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.

[109] 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.

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

3.1.6.1 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 dés organisations (restriction des droits d'un utilisateur sur sa propre machine).

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

3.1.7 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 coupes-feu. A 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'Etat, 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.

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

3.2.1 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 leader 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'Etat.

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'Etat :

- 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 23M€ entre 2001 et 2004 ont été consacrés au thème SSI[110].

- 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.

A 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.

[110] Source Ministère de la Recherche

Enfin, on peut noter la montée en puissance des pôles de compétitivité dont certains intègrent les questions de SSI notamment en Ile de France (System@tic), en PACA (solutions de communications sécurisées) et Rhône-Alpes (Minatec) ou de transactions électroniques sécurisées en Basse-Normandie.

En ce qui concerne la Commission européenne :

Le 6è 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[111]. De plus la Commission a lancé une action préparatoire, en vue du 7ème PCRD, dotée d'un budget prévisionnel de 65 millions d'euros pour la période 2004 – 2006, concernant la recherche de sécurité :

- 6è 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[112] ;
- 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 ;
- 7è 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[113] 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'Etat dans de telles actions est nécessaire; mais la volonté et les financements semblent encore incertains.

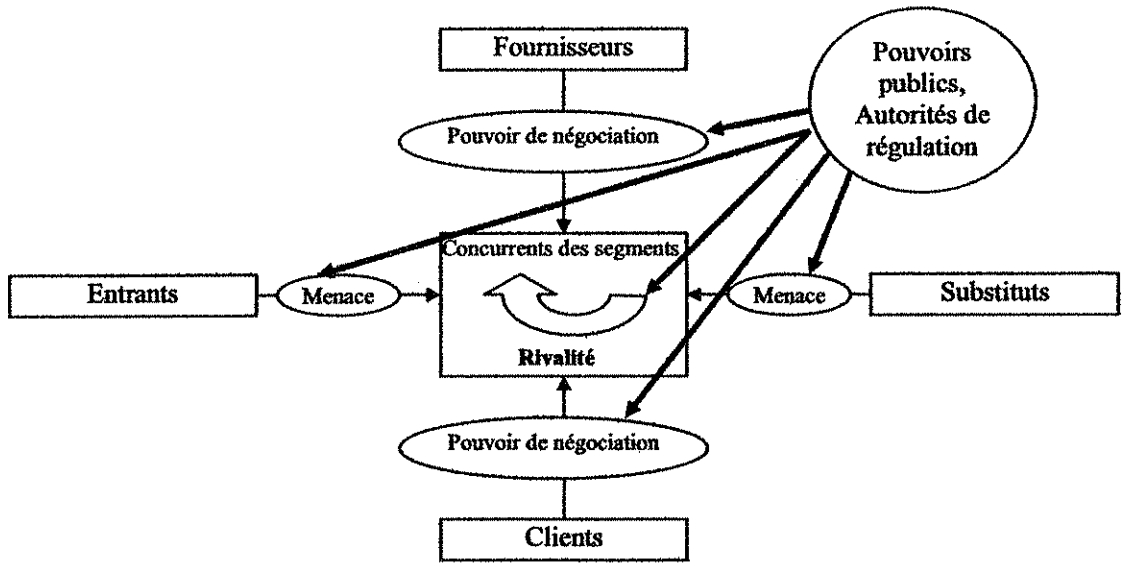
3.2.2 La situation des PME fournisseurs de produits et services SSI est très critique

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.

[111] Source Commission européenne
[112] Source Commission européenne
[113] Source auditions

3.2.2.1 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'Etat 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'Etat **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'Etat 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[114] 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. A ce niveau d'activité, elles devraient pouvoir générer suffisamment de cash flow pour continuer à innover et financer leur R&D.

L'Etat 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**.

- **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.

[114] Source auditions

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'Etat 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.**

3.2.2.2 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 Etats-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 Etats et aux grands donneurs d'ordres européens sans barrières spécifiques **doit être un objectif de l'Etat** 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 Etats-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.

3.2.2.3 Les politiques d'achat de l'Etat 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'Etat, 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[115] 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'Etat 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.

A 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. A cela s'ajoute 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.

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

3.2.2.4 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[116] et la transmission / cession [117].

Certes, les mesures gouvernementales ont été nombreuses ces dernières années :

- développement des FCPI[118] et d'Alternext ;

[115] Plan de Renforcement de la Sécurité des Systèmes d'Information de l'Etat (2004-2007) du 10 mars 2004

[116] 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.

[117] 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

- 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[119] ;
- 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.

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 Etats-Unis est différente : la taille du marché intérieur et les sources de financement disponibles leur permettent de se dispenser de financement 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,** serait 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 Economique 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

[118] Fonds Communs de Placement dans l'Innovation
[119] Leveraged By Out : opération d'acquisition d'une entreprises financée par un fort recours à l'endettement

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**[120] :

- en 2003, le financement de la R&D en TIC était de 90 $ par habitant en France, contre 220-240 $ aux Etats-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 Etats-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 Etats-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).

Ainsi, le financement de la R&D par les grandes entreprises françaises et européennes étant proportionnellement plus faible que celui des entreprises concurrentes aux Etats-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[121] ;
- 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[122],...) ;
- 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 Etats-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.

A 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

[120] Source : Futuris et Conseil Stratégique des Technologies de l'Information -Groupement Français de l'Industrie de l'Information octobre 2003.
[121] Doublement de 5 à 10% de la part en volume des dépenses de recherche prises en compte
[122] Programme d'Etudes Amont

particulières pour favoriser le recrutement de compétences par des PME, notamment en marketing des technologies[123], 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 ;
- 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)[124] ;
- 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...

3.2.3 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.

3.3 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.

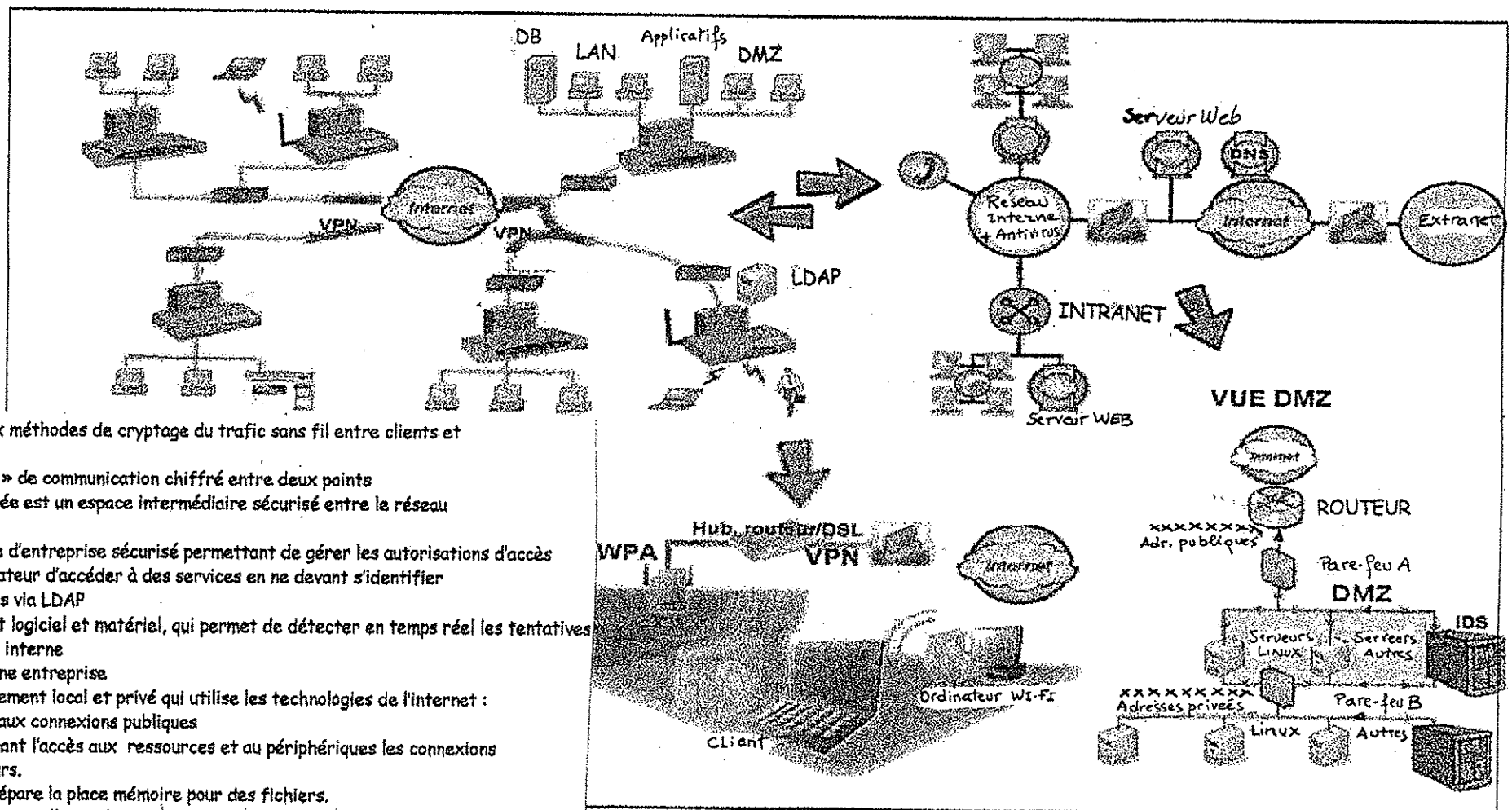
[123] Source auditions
[124] Source auditions

ANNEXE 1

Organismes

- ADAE : Agence pour le Développement de l'Administration Electronique ;
- BRCI : Brigade Centrale de la Répression de la Criminalité Informatique ;
- CCSDN : Commission Consultative du Secret de la Défense Nationale ;
- CEMA : Chef d'Etat Major des Armées ;
- CEMAA : Chef d'Etat Major de l'Armée de l'Air ;
- CEMAT : Chef d'Etat Major de l'Armée de Terre ;
- CMM : Chef d'Etat Major de la Marine ;
- CERT-RENATER : centre d'alerte et de réponse aux attaques informatiques dédié aux membres de la communauté GIP-RENATER – REseau 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'Evaluation 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 Etudes 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 Etudes 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.

- Schéma de principe des systèmes d'information



WEP ET WPA sont deux méthodes de cryptage du trafic sans fil entre clients et ports d'accès sans fil

Un VPN est un « tunnel » de communication chiffré entre deux points

DMZ ou zone démilitarisée 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 q'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 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 au périphériques les connexions des différents utilisateurs.

Un serveur de fichier prépare la place mémoire pour des fichiers,

Un serveur d'impressions et exécute les sorties sur imprimantes du réseau

Un serveur d'application rend disponible sur son disque dur des programmes « partagés »

CNS : permet d'effectuer la corrélation entre les adresses et le nom du domaine associé

ANNEXE 3

– 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 englobe 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 matérialisé 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, quelque soit 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, à 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 (*), de leur fournir un vade-mecum pour les aider dans cette mission et d'actualiser régulièrement ce document.

(*) 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 4

– 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. Evaluer 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 5

ANNEXE 12. – Exemples de chartes d'utilisateurs dans les entreprises et l'Etat[139]

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'Etat.

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 ;
  - 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,...) ;

[139] Sources auditions

- 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 affectée ;

- 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.

- ...