Union internationale des télécommunications

**QUESTION 9-1/2**

*Identification des sujets d'étude des Commissions d'études de l'UIT-T et de l'UIT-R qui intéressent particulièrement les pays en développement*


**UIT-D** COMMISSION D'ÉTUDES 2 3e PÉRIODE D'ÉTUDES (2002-2006)

# *Rapport sur les infrastructures nationales de sécurisation du cyberespace*

Union internationale des télécommunications

# LES COMMISSIONS D'ÉTUDES DE L'UIT-D

Les Commissions d'études de l'UIT-D ont été créées aux termes de la Résolution 2 de la Conférence mondiale de développement des télécommunications (CMDT) organisée à Buenos Aires, Argentine, en 1994. Pour la période 2002-2006, la Commission d'études 1 est chargée d'examiner sept Questions dans le domaine des stratégies et politiques de développement des télécommunications. La Commission d'études 2 est, elle, chargée d'étudier onze Questions dans le domaine du développement et de la gestion des services et réseaux de télécommunication. Au cours de cette période, pour permettre de répondre dans les meilleurs délais aux préoccupations des pays en développement, les résultats des études menées à bien au titre de chacune de ces deux Questions sont publiés au fur et à mesure au lieu d'être approuvés par la CMDT.

**Pour tout renseignement**

*Veuillez contacter:*


Mme Fidélia AKPO
Bureau de Développement des Télécommunications (BDT)
UIT
Place des Nations
CH-1211 GENÈVE 20
Suisse
Téléphone: +41 22 730 5439
Fax: +41 22 730 5484
E-mail: fidelia.akpo@itu.int


**Pour commander les publications de l'UIT**

*Les commandes ne sont pas acceptées par téléphone. Veuillez les envoyer par téléfax ou par e-mail.*


UIT
Service des ventes
Place des Nations
CH-1211 GENÈVE 20
Suisse
**Fax: +41 22 730 5194**
**E-mail: sales@itu.int**


**La Librairie électronique de l'UIT: www.itu.int/publications**

Union internationale des télécommunications

***QUESTION 9-1/2***

*Identification des sujets d'étude des Commissions d'études de l'UIT-T et de l'UIT-R qui intéressent particulièrement les pays en développement*

**UIT-D** COMMISSION D'ÉTUDES 2 3e PÉRIODE D'ÉTUDES (2002-2006)

# *Rapport sur les infrastructures nationales de sécurisation du cyberespace*

Union internationale des télécommunications

**DÉNI DE RESPONSABILITÉ**

**Le présent rapport a été préparé par un grand nombre de volontaires provenant de diverses Administrations et entreprises. La mention de telle ou telle entreprise ou tel ou tel produit n'implique aucune approbation ni recommandation de la part de l'UIT.**

# Rapport sur les infrastructures nationales de sécurisation du cyberespace

## TABLE DES MATIÈRES

## Avant-propos

*GALILEE bouleversa la science et la technologie il y a cinq siècles en affirmant que l'histoire de la nature était écrite dans la langue des nombres. Les plus récents progrès technologiques nous font comprendre que l'histoire humaine est, quant à elle, écrite dans la langue de l'information. Zéro et un sont les constituants du futur, deux chiffres qui forment l'alphabet des plus complexes parmi tous les phénomènes, les technologies de l'information et de la communication (TIC).*

Les années 90 ont été marquées par l'exploitation des systèmes de communication, qui ont permis le développement à grande échelle des échanges électroniques, tant dans le domaine industriel et bancaire que dans celui du commerce en ligne et plus récemment dans celui des relations entre les citoyens et les administrations. Si au cours des premières années, l'ouverture et l'interopérabilité des réseaux et des systèmes ainsi que leurs performances ont été privilégiées aux dépens de la sécurité, on a récemment assisté à une prise de conscience des problèmes par les utilisateurs des nouvelles technologies, qui ont entamé des réflexions sur la sécurité des réseaux de l'information et de la communication.

On ne pourra tirer concrètement profit des TIC que si l'on est convaincu que ces technologies et ces réseaux sont fiables et sûrs et ne sont pas utilisés abusivement. La mise en place d'un cadre stable et reconnu de normes et d'accords nationaux compatibles est essentielle pour l'édification de la société de l'information et constitue un pas important vers l'instauration de la confiance. Cette confiance repose aussi sur l'existence d'un cadre réglementaire et juridique permettant notamment de résoudre les problèmes que posent la cybercriminalité, la sécurité des réseaux d'information et de communication, la protection de la sphère privée, les éléments juridiques du commerce électronique et la protection des droits de propriété intellectuelle, autant d'éléments qui devraient être examinés à l'échelle internationale, toutes les parties concernées y participant activement.

Avec l'augmentation du piratage informatique et des virus informatiques, il est nécessaire de prévoir pour les réseaux d'information et de communication des systèmes de sécurité qui soient efficaces. Une collaboration internationale des Etats, du secteur privé et de la société civile est donc requise afin qu'il soit possible de coordonner les mesures adoptées et d'élaborer des dispositions juridiques permettant de protéger et de sécuriser les infrastructures, les systèmes et les services que nous procure graduellement la société mondiale de l'information.

Il convient de noter que dans la Décision 8 (Marrakech, 2002) de la Conférence de plénipotentiaires sont établies des lignes d'action, dont l'une est consacrée à la confidentialité et à la sécurité lors de l'utilisation des technologies nationales de l'information et de la communication (TNIC). Les partenaires publics et privés ne doivent pas hésiter à agir lorsque les conditions de travail locales sont un facteur de risque. La construction d'un cadre sécuritaire est un élément important pour le développement des TNIC. En outre, dans la Résolution 130 (Marrakech, 2002), il a été demandé à l'UIT d'entamer des travaux sur la sécurisation des réseaux de communication et de l'information. D'autres dispositions sur le même sujet sont données à l'Annexe 1 de la Résolution 130 de la PP-02. Par ailleurs, l'Assemblée mondiale de normalisation des télé-communications (AMNT) (Florianópolis, Brésil, octobre 2004) a adopté des résolutions qui concernent précisément les travaux sur la sécurité des réseaux de télécommunication et de l'information. Dans le présent rapport, il est tenu compte de ces importantes décisions. Ce rapport est une contribution du Groupe de travail 9-1/2 de l'UIT-D sur le sujet.

# 1 Introduction

La société de l'information offre de grandes possibilités de promotion du développement durable, de la démocratie, de la transparence, de la responsabilité et de la bonne gouvernance. L'exploitation des nouvelles possibilités offertes par les technologies de l'information et de la communication (TIC), en association avec les médias traditionnels et les mesures appropriées destinées à réduire la fracture numérique, sont les éléments clés de toute stratégie nationale ou internationale qui vise à réaliser les objectifs de développement, fixés par la Déclaration du Millénaire de l'Assemblée générale des Nations Unies.

Parmi les principaux problèmes auxquels sont confrontés les Etats, il faut noter ceux qui concernent la sécurité des informations, la complexité, la capacité et la portée croissantes des technologies de l'information, l'anonymat qu'elles permettent de garder et l'internationalisation des réseaux de communication. Les principales infrastructures d'un pays sont les institutions publiques et privées dans les domaines de l'agriculture, de l'alimentation, de l'eau, de la santé, des services d'urgence gouvernementaux et de défense nationale, de l'information et des télécommunications, de l'énergie, du transport, des services financiers, de la chimie et de la poste. Le **cyberespace** est leur «centre nerveux», le système de contrôle du pays. Ce cyberespace est composé de centaines de milliers de serveurs, d'ordinateurs, de routeurs, de commutateurs interconnectés et de systèmes de transport de l'information (câbles, satellites, voies hertziennes) qui permettent aux principales infrastructures de fonctionner harmonieusement. Le bon fonctionnement du cyberespace est donc essentiel pour l'économie nationale (et internationale) ainsi que pour la sécurité nationale.

Conscient de la nécessité d'assurer à tous les pays un accès équitable et adapté aux TIC, il ne faut pas oublier que ces technologies peuvent être utilisées à des fins incompatibles avec les objectifs de maintien de la stabilité et de sécurité internationale et peuvent nuire à l'intégrité des infrastructures étatiques, et à travers celles-ci à la sécurité des Etats. Pour résoudre ces problèmes, il faut agir sur plusieurs fronts et lutter contre la cybercriminalité. Sécuriser le cyberespace est un défi stratégique difficile qui requiert des efforts coordonnés de la part de tous les acteurs de la société de l'information.

a) Il est nécessaire de rendre plus fiable et plus sûre l'utilisation des TIC pour que cette utilisation puisse se généraliser et que la confiance des utilisateurs puisse augmenter. A cette fin, il convient:

   - de protéger la confidentialité des données et les intérêts des consommateurs;
   - de rendre les transactions électroniques et le commerce en ligne plus fiable et d'en instaurer le contrôle;
   - d'élaborer des normes techniques mondiales et régionales susceptibles de faciliter la mise en œuvre et l'utilisation des TIC;
   - d'améliorer la qualité des réseaux mondiaux et régionaux et d'en maintenir l'interconnectivité et l'interopérabilité;
   - de renforcer la coopération internationale pour lutter contre la cybercriminalité;
   - de créer des mécanismes adaptés visant à mieux faire connaître l'importance de la sécurité des réseaux d'information et de communication et des ressources dont dispose la communauté internationale dans ce domaine;
   - d'analyser les menaces (réelles et potentielles) qui pèsent sur la sécurité de ces réseaux, notamment en ce qui concerne le piratage informatique et les virus informatiques sur l'internet, et de réfléchir aux méthodes et aux moyens susceptibles d'y remédier;
   - d'améliorer les échanges d'informations techniques et la coopération internationale dans le domaine de la sécurité des réseaux d'information et de communication.

Dans les sections 2 et 3 sont décrits les moyens mis à la disposition des utilisateurs des TIC pour protéger les réseaux de communication et d'information ainsi que les méthodes utilisées par les «pirates» pour s'attaquer à ces réseaux.

Dans la section 9 intitulée «Centre de contrôle et d'acquisition des données transmises, y compris l'IP» est donné un exemple de système permettant à l'organe de contrôle d'assurer la sécurité et la surveillance des réseaux de communication et d'information.

b) Face au développement sans précédent des TIC, il est nécessaire de prendre de nouvelles mesures pour accroître le respect des droits de l'homme et des libertés fondamentales, en particulier le droit à la liberté d'opinion et d'expression et le droit à la confidentialité des données. Il faut donc:

- mettre en œuvre des dispositions juridiques garantissant l'accès à l'information et le droit du public à cet accès à l'information;
- élaborer un cadre juridique national sur la liberté d'expression;
- appliquer le droit relatif à la communication et à l'information dans le cyberespace.

Ce sujet est traité dans la section 5 «Aspects juridiques» où il est tenu compte des travaux et des études réalisées par l'ONU, l'OCDE, le Conseil de l'Europe, l'Union européenne et les Etats-Unis d'Amérique, ainsi que des rapports y relatifs. Ensuite, dans la section 6 sont décrites les normes ISO actuelles et dans la section 7 sont indiqués les résultats du Sommet mondial sur la société de l'information (SMSI, Genève, décembre 2003) sur la sécurité de l'information.

La section 8 porte sur l'ensemble des travaux réalisés ou en cours à l'UIT.

Un exemple de système de contrôle des données y compris l'internet est donné à la section 9.

La section 10 est consacrée à des études de cas pertinents, en particulier la lutte contre le spam.

# 2 Sécurité et protection des réseaux

La notion de système de gestion et de protection des réseaux de télécommunication (sécurité) a été introduite à l'échelle mondiale au moyen des normes ISO 9000 et ISO 14000 ainsi que du Rapport technique TR 13335 de l'ISO «Management of information, communications technology security». Le système de sécurité des réseaux doit être fondé sur un ensemble d'éléments corrélés ou interactifs (politiques, techniques, procéduriers, humains) permettant:

- une approche de la gestion des risques à définir, impliquant la mise en œuvre et la vérification/maintenance/amélioration continue de la sécurité de l'information au sein d'un organisme. Il y a lieu de tenir compte dans un réseau du fait que toutes les informations et tous les systèmes de traitement de ces informations n'ont pas la même valeur, ne subissent pas les mêmes menaces et ne sont pas également vulnérables. C'est un processus continu où l'on doit prendre en compte et traiter les contraintes évolutives de l'environnement interne et externe.

## 2.1 Concept

Les entreprises réagissent différemment face à la menace que constituent les pirates (hackers); en pratique cela les conduit à mettre en place des infrastructures de sécurité. La politique de sécurité mise en œuvre doit pouvoir être mise à jour et améliorée.

La construction d'une architecture de sécurité englobe plusieurs tâches. Selon la taille et les ressources de l'entreprise, ces tâches seront réalisées par le personnel interne ou par un prestataire. Dans les deux cas, elles sont essentielles.

- Définition de l'objectif du projet: de l'accès simple à l'internet au développement d'un portail que les partenaires pourront utiliser pour consulter les données contenues dans le système d'information.
- Recensement des fonctionnalités souhaitées.
- Recensement des flux engendrés.
- Réalisation de l'adéquation entre les besoins et la politique de sécurité (*une politique de sécurité doit être appliquée*).

- Recensement de l'incidence sur le reste du système d'information: synchronisation avec les différents responsables de domaines fonctionnels.
- Recherche d'outils ou de configurations assurant la sécurisation de l'ensemble des flux: authentification, intégrité, chiffrement, disponibilité, etc.
- Choix d'outils supplémentaires répondant au cahier des charges.
- Définition de l'architecture de sécurité au moyen de l'ensemble des éléments qui la composent.
- Définition du plan d'adressage.
- Mise en place d'une maquette permettant de valider les fonctionnalités et la sécurité de l'ensemble.
- Rédaction des procédures d'exploitation, d'administration et mise en place d'une procédure de défense en cas d'attaque.
- Transfert des compétences aux exploitants et aux administrateurs.
- Création d'un site pilote.
- Réalisation d'un test d'intrusion.
- Modification si besoin est de l'architecture de sécurité ou des procédures.
- Déploiement multisite du système.

## 2.2 Technologies

Les technologies de sécurité permettent aujourd'hui d'installer des équipements de plus en plus performants et robustes. Ces derniers sont souvent proposés sous la forme de «boîtes noires» spécialisées. (routeurs évolués, commutateurs, logiciels).

Le choix des solutions se fait aujourd'hui en fonction du coût, de l'évolution, de l'administration, de la politique de licence et de la compatibilité avec les normes de l'industrie. L'administration est un élément important car, plus l'interfaçage est facile, plus la solution est attractive. En effet, certaines entreprises ne disposent pas d'équipe affectée exclusivement à la sécurité. Ce sont alors les personnes chargées du réseau qui assurent la gestion des éléments de sécurité.

Par ailleurs, le placement d'un pare-feu peut très rapidement avoir une influence sur le choix puisque souvent, dès la mise en place d'un pare-feu, les solutions telles que l'authentification et le chiffrement à l'aide de tunnels VPN gagnent en importance.

Il existe, outre le pare-feu, d'autres techniques qui doivent êtres utilisées conjointement avec les pare-feu afin d'optimiser leurs efficacités en matière de sécurité:

- relais de messagerie;
- logiciels antivirus;
- serveurs mandataires, protocole de transfert hypertexte (HTTP), protocole de transfert de fichiers (FTP), groupe de discussion;
- logiciels d'optimisation de la bande passante;
- systèmes et logiciels de chiffrement;
- système d'analyse des fichiers log;
- système de détection d'attaques et d'intrusion (SDI);
- dispositifs d'authentification des utilisateurs;
- commutateurs web «intelligents»;
- outils de détection des points de vulnérabilité;
- mémoires tampons.

Dans le cas de liaisons hertziennes (Wireless LAN), on a affaire à un réseau dont les connexions et les données qui y transitent ne sont pas vraiment fiables et dont la confidentialité ne peut être assurée sans dispositif de sécurité. On retrouve ici ce que l'on connaît déjà avec l'internet, et les remèdes sont les mêmes, à savoir isolation du système d'information par la création d'une zone démilitarisée (DMZ) spécifique et mise en place de mesures de sécurité dans une couche supérieure (chiffrement, signature, etc.). Le § 2.9 du présent document traite plus spécifiquement de ce sujet.

## 2.3 Routeurs

Un routeur est un ordinateur relié à plusieurs réseaux au moyen d'une interface pour chacun d'eux, dont la fonction consiste à un paquet de données d'un réseau à un autre en fonction de l'adresse de destination contenue dans l'en-tête du paquet. Par défaut, un routeur achemine tous les paquets sans exception, permet l'accès distant (Telnet avec authentification) sur toutes ses interfaces pour la configuration, assure la mise à jour éventuelle des logiciels par le réseau ainsi que le «read and write» à distance au moyen du protocole simple de gestion du réseau (SNMP, *simple network management protocol*).

Avant d'installer le pare-feu (un routeur filtrant dont on peut modifier les décisions de routage avec des règles d'accès), il faut d'abord configurer le routeur situé en amont. Pour cela, on déterminera d'abord comme il convient la capacité de la connexion au réseau public. Le routeur qui y est relié pourra, selon sa configuration, restreindre l'usage de certains des protocoles afin d'éviter un encombrement de la bande passante. Ainsi, que la ligne donne accès à l'internet ou à un site partenaire, seuls les flux déclarés utiles pourront passer, évitant ainsi toute attaque par «inondation» de paquets. Une fois cette étape achevée, on pourra envisager l'installation du pare-feu.

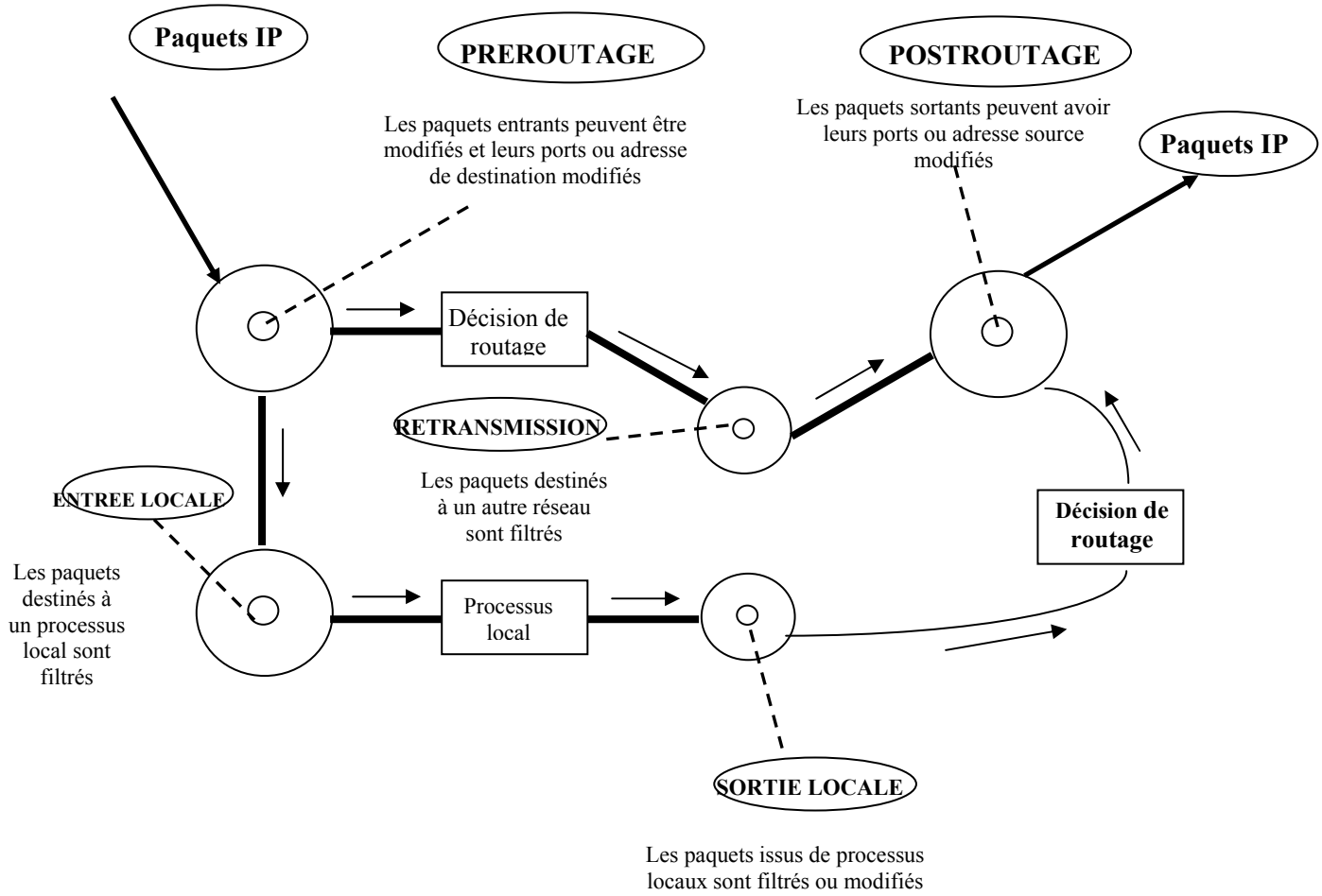
## 2.4 Coupe-feu

Les limites du périmètre de sécurité sont en général déterminées par un ou plusieurs éléments coupe-feu, devant être administrées centralement. Sous le nom générique de pare-feu, on retrouve de nombreux produits logiciels comme matériels assurant toujours la même fonction: isoler de manière sélective le réseau d'entreprise des autres réseaux (blindage contre les pirates, filtrage contre les fureteurs). Par conséquent, établir un périmètre de sécurité consiste à identifier le ou les réseaux de machines et de ressources à protéger. La limite de ce périmètre constitue donc le lieu où toutes les connexions entrantes et sortantes sont contrôlées. L'autorisation de passage d'un paquet à travers un pare-feu est alors définie par des règles telles que:

- l'adresse d'origine ou de destination du paquet;
- le protocole utilisé;
- le port de connexion.

Le coupe-feu est la seule et unique passerelle de communication pour tous les hôtes situés à l'intérieur de la zone protégée. Pour que ce périmètre de sécurité du réseau soit réellement efficace, il faut que toutes les communications entrantes ou sortantes établies transitent par le coupe-feu. Cet élément joue donc un rôle essentiel dans la solution, puisqu'il garantit le périmètre de sécurité. Le pare-feu utilise un mécanisme de filtrage dynamique des paquets. Il comporte un «contrôleur» de sessions et un dispositif qui analyse l'ensemble des couches réseau. Les paquets sont donc analysés au-delà de l'en-tête IP, et ce quel que soit le protocole de transport employé (TCP, UDP, ICMP, RPC). Chaque session est autorisée ou refusée selon des règles de filtrage bien établies. L'événement est enregistré avec un maximum de détails (ports source et de destination, heure, date, numéro de règle concerné, etc.) et conservé dans une base de données.

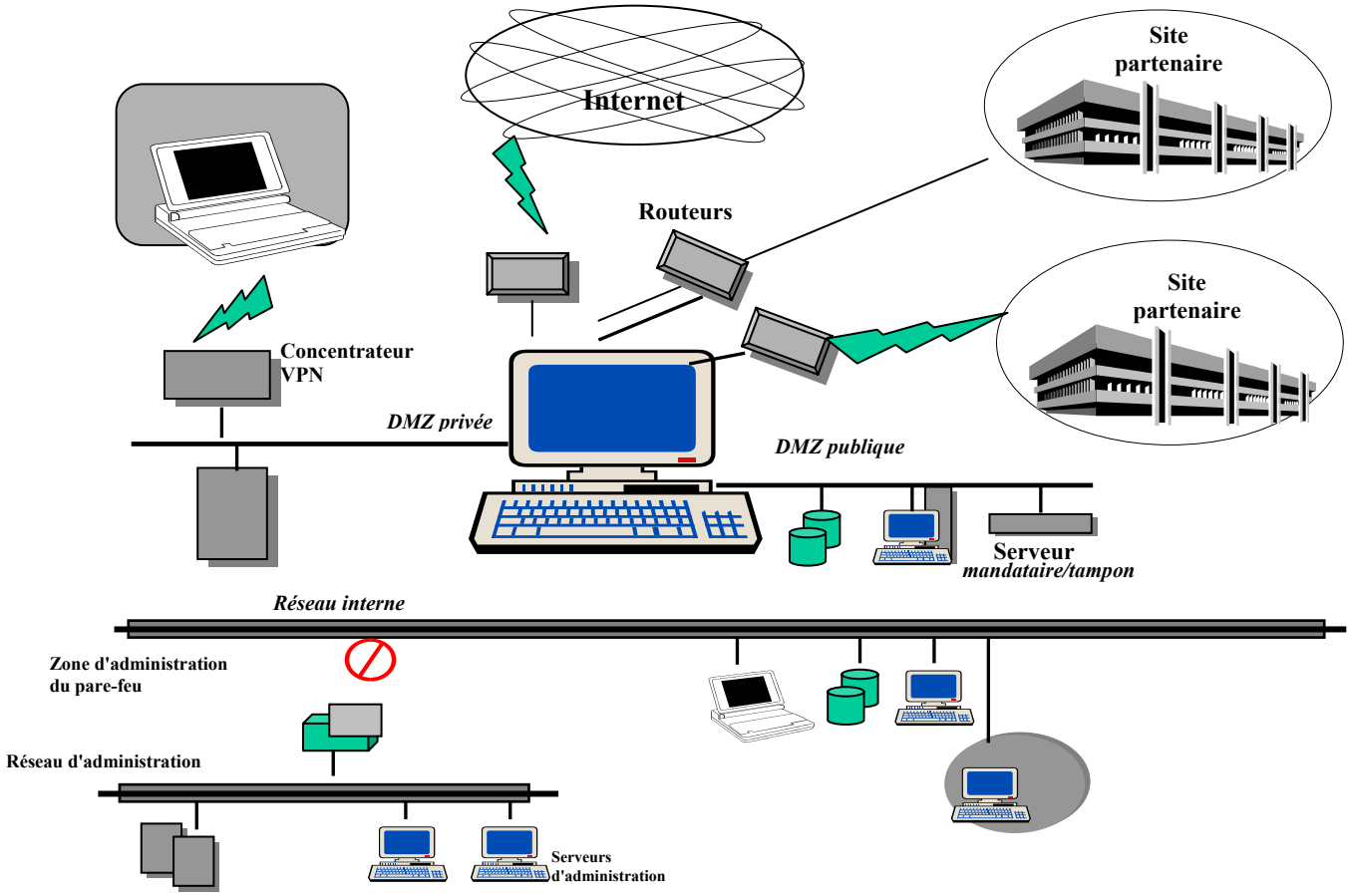
**Figure 1 – Schéma de principe d'un pare-feu**




Il faut veiller à la mise en place de zones démilitarisées (DMZ) ou de sous-réseaux. Ces zones servent le plus souvent à héberger des équipements plus ou moins sensibles ou ayant un rôle bien précis dans la topologie de sécurité déployée. Elles agissent donc comme des «compartiments» totalement ou partiellement étanches. Les différentes parties du réseau protégé, qui utilisent des plans d'adressage déterminés selon les besoins de fonctionnement, sont subdivisées comme suit: le réseau «fournisseur d'accès» assurant le raccordement à l'internet, nommé réseau extérieur; la ou les zones dites démilitarisées, une ou plusieurs DMZ étant publiques, tandis qu'une DMZ est privée et le réseau interne. Les flux de communication doivent donc être examinés en détail jusqu'au niveau des données admises dans le périmètre. Cette fonction est souvent assurée par des éléments «périphériques» – clés qui garantissent un examen approfondi et permettent de lever le doute sur la nature malveillante du paquet. En conséquence, la fonction du coupe-feu est complétée par celle des serveurs et des équipements servant à contrôler ou à alerter en cas de situation anormale. Un pare-feu non accompagné d'équipements complémentaires peut donc rendre un réseau vulnérable, car il ne peut analyser et examiner les paquets jusqu'au niveau des données elles-mêmes.

Le pare-feu est le centre du réseau en étoile, c'est-à-dire l'interface vers le réseau interne, vers l'extérieur (réseau, réseau public, ou autre sous-réseau), vers les zones démilitarisées (DMZ) et vers des sous-réseaux particuliers. La zone DMZ accepte les connexions débutant au niveau du réseau interne ou de l'internet pour les services en question uniquement alors que le service interne est inaccessible depuis l'extérieur ou depuis cette zone démilitarisée. Un exemple de connexion d'un pare-feu (firewall) est donné ci-après.

**Figure 2 – Exemple de connexion d'un pare-feu**




Pour résumer, la mise en œuvre d'un pare-feu débutera obligatoirement par sa configuration. Dans un premier temps, ce pare-feu sera réglé pour ne rien laisser passer, et cela quel que soit le sens (entrée, sortie du réseau ou accès vers et depuis la DMZ). En fonction des besoins, on ajoutera au fur et à mesure des règles autorisant l'accès, afin que ne soient établies que les connexions autorisées dans le cadre de la politique de sécurité.

Un autre point à considérer lors de la mise en route de la porte coupe-feu est celui qui concerne l'adressage du périmètre de sécurité, devant être confidentiel. A cet effet, le mécanisme de traduction des adresses sera activé et démarré sur le(s) pare-feu et routeurs, afin de masquer complètement les adresses du réseau interne. Cette traduction sera de type statique ou dynamique selon les besoins. On notera que, vis-à-vis de l'extérieur, toutes les communications IP utilisent dans ce cas la même adresse, ou un nombre d'adresses très restreint. Cela est plus efficace mais aussi – et surtout – cela permet de n'autoriser que cette ou ces adresses IP en tant qu'adresses de sortie via le routeur d'accès à l'internet.

Ainsi, dans le cas de deux sous-réseaux DMZ (dans une zone DMZ publique et une zone DMZ privée par exemple) et d'une interface vers le réseau interne, chacun des sous-réseaux sera obligatoirement inclus dans une plage d'adresses unique. Les serveurs situés dans la DMZ publique doivent être accessibles depuis l'extérieur (internet). Dans ce cas, ils pourront recevoir soit directement une adresse publique, susceptible d'être acheminée, soit une adresse interne, non susceptible d'être acheminée sur l'internet. S'il s'agit d'une adresse interne, non susceptible d'être acheminée, les serveurs web dans une DMZ ne seront pas directement

accessibles à partir de l'internet. Pour atteindre les données, les internautes doivent aller jusqu'au pare-feu qui hébergera sur son interface externe l'adresse publique du serveur cible. Sa fonction est de traduire cette adresse en une adresse interne du serveur web, rendant ainsi l'accès possible. Dans ce schéma, le pare-feu tient le rôle de chef d'orchestre qui peut empêcher tout accès direct vers ledit équipement. C'est le principe de la traduction d'adresses.

Dans le cas d'un grand réseau, pour lequel la perte d'une connexion vers l'extérieur serait grave, on prévoira une certaine redondance des équipements (utilisation parallèle de deux pare-feu dont l'un est désigné comme primaire et l'autre comme secondaire).

Il est également possible d'installer des pare-feu, au moins deux, en aval des commutateurs web. Ces commutateurs assurent une répartition de la charge générée par le trafic au point d'accès. On peut ainsi constituer des groupes de pare-feu. Le groupe sera autonome et rendra transparentes aux autres machines la configuration et la répartition de l'activité entre ses membres.

Bien sûr, ces groupes de pare-feu seront toujours administrés centralement. Une politique de sécurité a en effet une dimension «globale» pour le réseau et l'entreprise; c'est souvent la même pour tous les points d'accès. Si plusieurs sites géographiques d'un même réseau d'entreprise sont connectés à l'internet, il sera plus efficace et plus sûr d'assurer une administration synchronisée en ce qui concerne les adjonctions, modifications et révocations des règles de sécurité. Par ailleurs, les alertes seront dirigées vers une ou plusieurs consoles centrales.

**Règles de sécurité pour les coupe-feu**

L'emploi en forte augmentation des ordinateurs dans les télécommunications internationales a amené les délits informatiques dans son sillage. Au cours des dernières années, les délits informatiques ont littéralement explosé, comme le confirment plusieurs enquêtes sur les plans international et national. Dans la plupart des pays, on ne connaît pas le nombre exact d'effractions informatiques ou d'incidents mettant en jeu la sécurité, en particulier ceux qui sont liés aux télécommunications internationales.

La plupart des organismes ou des sociétés de télécommunication ne sont pas spécialement équipés pour faire face aux incidents en matière de sécurité, qui se produisent dans les réseaux d'information et de communication (ICN, *information and communication network*) (même s'ils disposent d'un état-major général de crise chargé de la prise en charge des crises de tous types). La définition des incidents de sécurité est donnée dans la norme ISO 17799. Lorsqu'un tel incident se produit dans un réseau ICN, il est traité comme il convient, c'est-à-dire la personne qui le détecte prend la responsabilité de le traiter au mieux qu'elle peut. Dans certains organismes, on a tendance à oublier et à dissimuler les incidents de sécurité dans les réseaux ICN, ceux-ci pouvant nuire à la production, à la disponibilité et aux recettes.

Souvent, lorsqu'un incident de sécurité est détecté dans un réseau ICN, la personne qui le détecte ne sait pas à qui elle doit en faire part, de sorte que l'administrateur du système ou du réseau est amené, pour se débarrasser simplement du problème, à adopter une solution de rechange ou à effectuer une rapide réparation. L'autorité nécessaire ne lui a pas été conférée, et il ne dispose ni du temps ni de l'expérience qui lui permettraient de réparer le système pour qu'un tel incident ne se reproduise plus. Pour ces raisons principalement, il vaut mieux disposer d'une équipe ou d'un groupe formé qui soit en mesure de prendre en charge, rapidement et correctement, les incidents de sécurité. En outre, il s'agit souvent de domaines aussi divers que le domaine des relations multimédia, le domaine juridique, celui de l'application des lois, des parts de marché, ou le domaine financier.

Lors de la signalisation ou de la prise en charge d'un incident, l'emploi de différentes taxinomies peut conduire à des erreurs d'interprétation. Cela peut, à son tour, impliquer qu'un incident de sécurité dans un réseau ICN ne reçoive ni l'attention appropriée ni la prise en charge prompte qui sont nécessaires pour y mettre fin, pour le contenir et pour éviter qu'il ne se reproduise. Les conséquences qui peuvent en découler pour l'organisme touché (la victime) peuvent être sérieuses.

Afin d'être en mesure de prendre en charge et de signaler correctement un incident, il est nécessaire de comprendre comment il est détecté, pris en charge et résolu. En déterminant la configuration des incidents (à savoir les incidents physiques, administratifs ou organisationnels et logiques), il est possible d'obtenir une image globale de la structure et du flux d'un incident. Une terminologie uniforme est fondamentale pour une compréhension commune des mots et des termes.

La Recommandation UIT-T E.409 donne un aperçu de la question et en décrit le cadre, permettant de disposer de lignes directrices en matière de planification de l'organisation en cas d'un incident et de prise en charge de l'incident de sécurité, et décrivant le flux et la prise en charge de l'incident.

Agissant comme des gardiens, les pare-feu surveillent les réseaux et examinent le trafic entre lesdits réseaux et l'internet. Tout trafic non sollicité ou suspect est systématiquement bloqué. Les pare-feu peuvent également être configurés pour sécuriser un réseau en fonction d'un ou de plusieurs autres réseaux.

Les cinq règles de sécurité à respecter lors de l'implantation des coupe-feu sont les suivantes:

*1) Identifier les zones de confiance*

La toute première étape, dans la sécurisation d'un réseau, consiste à définir les zones de confiance (*trust zones*) présentes. Dans sa forme la plus simple, la sécurité du réseau traite des zones de confiance.

*2) Mettre à jour les règles*

Il est très important que tous les pare-feu puissent bénéficier d'une mise à jour des règles de sécurité. La seule façon de vérifier si le pare-feu respecte véritablement la politique de sécurité acceptée, consiste à s'en assurer en conjonction avec un système de détection d'intrusion (*intrusion detection system*) (voir le § 2.6), ou à vérifier manuellement, au moyen d'un test intrusif ou d'un examen du pare-feu par une tierce partie.

*3) Examiner le trafic*

Lorsqu'il a été décidé d'appliquer une politique de sécurité au moyen de pare-feu, il est important de consigner les alertes dans un journal d'exploitation (log). L'une des principales fonctions de gestion d'un pare-feu consiste à consigner le trafic qui circule en son sein. La consignation ne sert à rien si les fichiers des journaux d'exploitation ne sont pas examinés régulièrement. Ce point doit donc faire partie des règles intégrées dans la politique de sécurité.

*4) Surveiller la stabilité*

Un pare-feu est un composant de l'infrastructure des réseaux, et doit à ce titre être administré en tant que tel. En d'autres termes, il faut surveiller sa durée maximale de fonctionnement. En effet, s'il n'est pas stable, les utilisateurs chercheront des moyens de le contourner, pour éviter un incident, ce qui conduira inévitablement à une diminution importante du niveau de sécurité. Cette règle doit également faire partie de la politique de sécurité.

*5) Documenter la politique de sécurité*

La politique de sécurité d'un pare-feu doit toujours être documentée, afin de fournir un élément de référence aux administrateurs et aux utilisateurs du pare-feu.

Si la politique de sécurité est effectivement documentée, les utilisateurs pourront travailler normalement, tout en se conformant à la politique de sécurité officielle, sinon ils auront tendance à réagir au cas par cas.

**Importance des pare-feu (exemple)**

En août 2003, la vulnérabilité des utilisateurs des systèmes à large bande connectés à l'internet a été mise en évidence lors de la propagation du ver «MSBlast». Ce programme-ver s'introduit dans les ordinateurs en profitant d'une faille du système d'exploitation; il recherche les portes d'entrée qui sont restées ouvertes ou les ordinateurs qui sont connectés à l'internet. S'il en trouve, «MSBLast» établit une connexion et se télécharge à l'intérieur de l'ordinateur; là, à partir de ce nouvel hôte, le ver explore à nouveau l'internet à la

recherche d'autres portes d'entrée ouvertes dans d'autres ordinateurs, sur tout l'internet. La particularité de ce ver est qu'il agit sans intervention de la part des utilisateurs; les connexions internet à large bande permanentes sont donc de par leur nature plus vulnérables, même si en fait tous les types de connexion peuvent êtres touchés.

C'est ainsi qu'en quelques jours seulement, «MSBLast» a infecté 180 000 ordinateurs dans le monde entier; ceux qui étaient protégés par des pare-feu n'ont pas été touchés, les pare-feu ayant aidé à minimiser les attaques. Cet exemple souligne toute l'importance que revêtent les mesures de sécurité telles que les pare-feu, lorsqu'on utilise une connexion à large bande. Bien sûr, un utilisateur à large bande peut attendre de recevoir une bonne leçon pour apprendre, c'est-à-dire attendre d'être victime d'un virus pour se protéger, mais les pouvoirs publics et les ISP ont un important rôle pédagogique à jouer et peuvent prendre certaines mesures concrètes, par exemple en normalisant les programmes de sécurité préinstallés.

(http://www.msnbc.com/news/951168.asp?cp1=1)

## 2.5 Antivirus

Il existe deux sortes d'antivirus dont les techniques sont différentes mais complémentaires:

### 2.5.1 Scanners

L'antivirus compare les fichiers avec sa table de signatures, qui renferme l'identité de chaque famille de virus. Cette technique est efficace pour les virus connus à condition que la table soit à jour. Mais elle ne permet pas de se protéger contre des virus inconnus ou anciens dont le code a été modifié.

### 2.5.2 Antivirus génériques

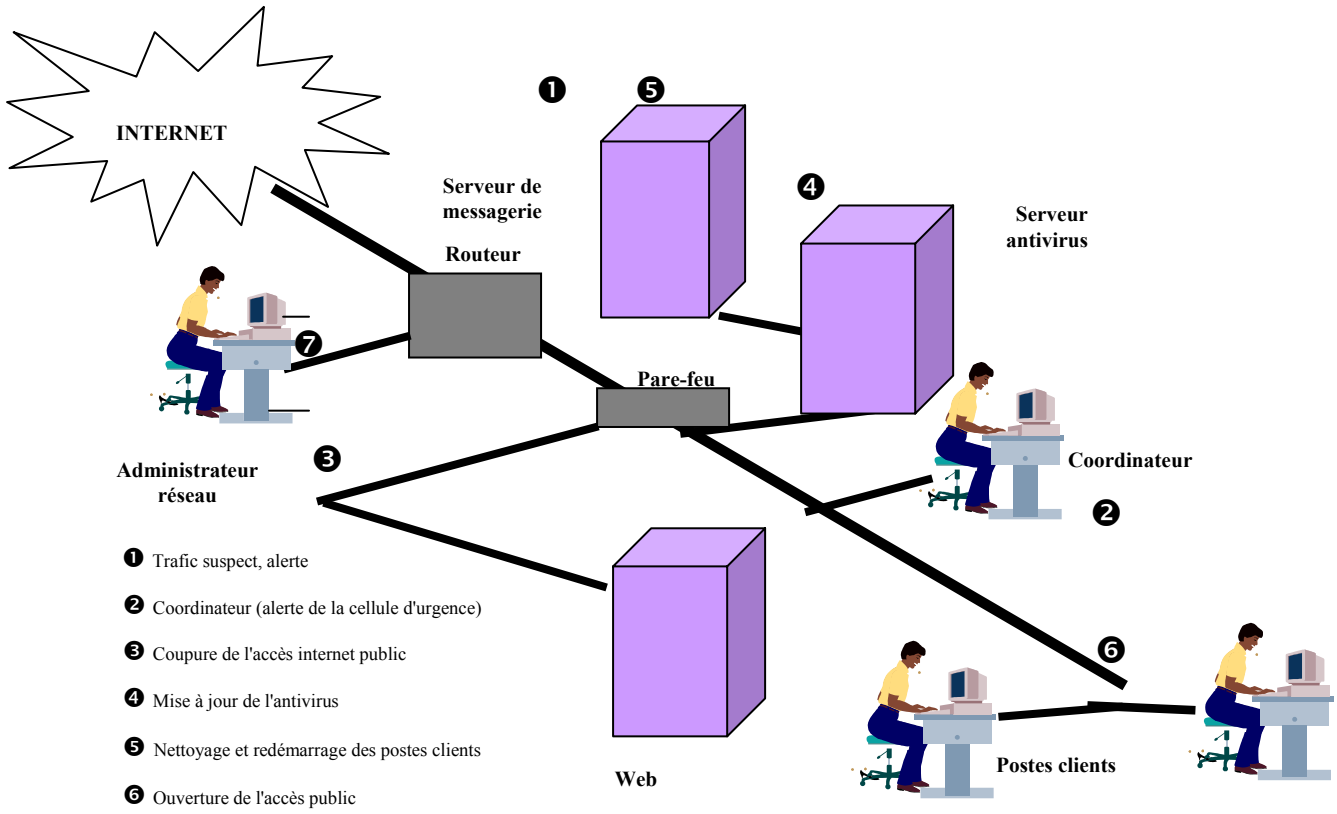
Ils font appel, dans le cadre d'une politique de sécurité, à plusieurs techniques de détection: la technique heuristique (recherche des structures suspectes dans un programme), la vérification de l'intégrité des fichiers (détection des modifications), l'analyse des comportements (prise sur le fait du virus) et la simulation du virus dans une machine virtuelle. Ces méthodes sont les seules qui permettent d'intercepter un virus inconnu. Mais elles génèrent de nombreuses fausses alertes et une charge accrue pour le système. C'est pourquoi elles sont souvent associées à une table de signatures, le moteur heuristique se limitant alors à essayer d'intercepter les virus inconnus les plus visibles.

Face aux virus, la politique de sécurité de l'entreprise doit se concentrer sur deux fonctions clés: i) l'administration du système et ii) la coordination de la sécurité en matière de virus. La première fonction effectue tous les réglages des serveurs et des postes de travail, qui permettent de rendre les applications aussi étanches que possible aux infections. La seconde fonction est chargée de la mise à jour régulière du parc d'antivirus. Elle doit aussi être à l'affût des alertes informatives sur les virus afin de les transmettre aux utilisateurs. Communiquer aux utilisateurs les sujets des messages électroniques qui véhiculent des virus constitue déjà une précaution efficace. Par ailleurs, le coordinateur a la responsabilité de mettre en place un plan de réponse rapide aux attaques. L'utilisateur final peut devoir être séparé du réseau tandis que les applications touchées peuvent devoir être fermées.

A l'instar des éditeurs d'antivirus, l'entreprise doit avoir son propre centre de réponse rapide. Toutes les personnes directement impliquées font partie de la cellule d'urgence. Le rôle de chacune d'elles est défini après une simulation d'attaque virale. La rapidité d'exécution du plan de réponse est la première condition de son succès.

Il est donné ci-après un exemple de plan d'actions antiviral.

**Figure 3 – Plan d'action antiviral**




## 2.6 Systèmes de détection des intrusions

Les systèmes de détection d'intrusions (SDI) sont devenus une des premières préoccupations des entreprises et des opérateurs. Bien des experts se sont concertés pour donner une définition satisfaisante du terme «intrusion», mais cela n'est pas aussi simple qu'il y paraît. En effet, passer au scanner un port peut-il être considéré comme une intrusion? Et que dire des attaques par déni de service (DoS) qui, d'un point de vue purement technique, ne visent pas à pénétrer dans un système d'information, mais simplement à le saturer?

Nous définirons donc l'intrusion comme une activité inhabituelle au sein du système d'information. Cette définition inclut notamment: le passage au scanner d'un port, les attaques directes ou indirectes contre un composant du système d'information, les attaques virales, les attaques par déni de service et les abus quant à l'utilisation de la bande passante. Les systèmes SDI devraient être intégrés dans la politique de sécurité.

### 2.6.1 Catégories des systèmes de détection

#### 2.6.1.1 Systèmes de détection des intrusions fondés sur le réseau (NIDS)

Les NIDS sont probablement les systèmes les plus connus. Il s'agit de composants qui se comportent comme un renifleur, capturant et décodant toutes les trames transitant par le segment sur lequel il est connecté. Mais, à la différence d'un renifleur, cette sonde analyse les paquets IP (Protocole Internet) dans leur intégralité, afin de repérer les signatures d'attaques connues, ou les anomalies dans les en-têtes des paquets.

#### 2.6.1.2 Systèmes de détection des intrusions fondés sur l'hôte (HIDS)

Les HIDS sont les compléments naturels des NIDS. Il s'agit d'agents logiciels que l'on installe sur les machines à protéger et dont le rôle est triple:

- détection d'attaques contre des applications installées sur le système protégé;
- vérification de l'intégrité des fichiers sensibles;
- corrélation des fichiers journaux, en provenance d'applications ou d'équipements tiers, tels les routeurs, les coupe-feu, ou les commutateurs.

#### 2.6.1.3 Leurres

Inspiré des stratégies militaires, le leurre est sans doute un composant moins connu. Bon nombre de techniques d'attaques utilisent des mécanismes préalables de reconnaissance (empreintes) pour déterminer la nature des systèmes d'exploitation et des applications cibles. Par exemple, «nmap» est un scanner de ports relativement populaire, qui permet également de prendre l'empreinte d'un système.

Afin d'empêcher l'emploi de telles méthodes de reconnaissance, les leurres brouillent les scanners en simulant un système virtuel, et en générant de fausses réponses, pour induire l'intrus en erreur.

Les leurres les plus couramment utilisés sont les suivants:

1) Back Officer Friendly

Le programme gratuit Back Officer Friendly, ou BOF (www.nfr.com/products/bof), permet de simuler sur une machine Windows des services comme http (*hyper text transfer protocol*), ftp (*file transfer protocol)*, telnet et mail et le logiciel back office.

Lorsque le leurre est actif, la moindre requête lancée sur le réseau à destination de l'un des services ouverts sur la machine suffit à générer chez l'utilisateur une alarme de type «POP UP» (fenêtre contextuelle). Back Officer Friendly est un leurre simple qui permet à une personne peu habituée au concept de le mettre en pratique très simplement.

2) Specter

Specter (www.specter.com) est un leurre similaire, qui possède la fonctionnalité supplémentaire consistant à enregistrer le trafic avec l'attaquant, ou à activer des réponses automatiques à destination de l'attaquant.

Cette fonctionnalité additionnelle le rend plus furtif que le BOF.

3) Deception Toolkit

Deception Toolkit, ou DTK (www.all.net/dtk) est historiquement l'une des premières réalisations de leurre.

Cet outil, dont les sources sont disponibles sur l'internet, permet de simuler différents services qui comportent des vulnérabilités connues.

4) ManTrap

ManTrap (www.recourse.com/product/ManTrap) est un produit qui permet de simuler plusieurs sous-systèmes d'exploitation, au-dessus du système d'exploitation de base de la machine. L'attaquant voit le leurre comme étant composé de plusieurs serveurs équipés de systèmes d'exploitation différents. L'outil permet d'enregistrer très précisément toute l'activité du leurre.

Le principal inconvénient de ce type d'outils réside dans le fait qu'ils possèdent une signature qui pourrait les trahir, face à un attaquant expérimenté. Parce qu'un leurre ne doit pas se distinguer de son environnement, les meilleurs leurres sont ceux qui ressemblent à s'y méprendre à l'un des serveurs qui les environnent (mais en éloignant les données sensibles et en supprimant les interactions avec les autres serveurs).

Un leurre est un moyen de sécurité, qui vient s'ajouter aux éléments déjà installés. Ce n'est que lorsqu'une entreprise dispose d'un système de sécurité sophistiqué qu'elle peut se permettre d'ajouter ce nouvel outil dans son architecture réseau. Un leurre ne doit en effet être utilisé qu'en complément de systèmes tels que les pare-feu, les sondes de détection d'intrusion, l'examen régulier des fichiers d'enregistrement, la surveillance permanente de l'activité du réseau et des systèmes de serveurs, etc.

### 2.6.2 Techniques de détection

Diverses techniques sont couramment utilisées pour détecter une intrusion, certaines s'appliquant à l'en-tête d'un datagramme, d'autres aux données utiles.

#### 2.6.2.1 Analyse des signatures

La plupart des attaques utilisent des chaînes de caractères bien connues, que l'on peut identifier dans le champ de données: ces chaînes sont les signatures des intrusions. L'analyse des signatures consiste donc, tout simplement, à détecter ces chaînes en les comparant à une librairie de signatures d'attaques connues et à donner l'alerte en cas de correspondance.

#### 2.6.2.2 Analyse des en-têtes

Les techniques de reconnaissance des systèmes ne sont généralement pas liées à des chaînes de caractères spécifiques et sont donc non détectables par l'analyse des signatures. Des intrusions de ce type exploitent en général les divers paramètres des en-têtes IP. Elle se chargent notamment de:

- balayer les ports;
- utiliser le champ «TTL» pour déterminer la présence d'équipements de type pare-feu ou routeurs;
- utiliser les champs liés aux options TCP et IP;
- s'emparer des fanions TCP.

Certaines attaques par déni de service sont très simples à mettre en œuvre et profitent d'une mauvaise utilisation des paramètres d'en-tête. On peut citer, par exemple, l'attaque «land», qui consiste à utiliser la même adresse IP pour la destination et pour la source (en détournant cette dernière). La plupart des équipements de communication ne contrôlent pas les adresses source, et quand la cible reçoit une telle requête, elle se renvoie les paquets à elle-même jusqu'à saturation de la pile IP, qui entraîne bien souvent le blocage du système. Il est donc essentiel de compléter l'analyse des signatures par une analyse des divers paramètres d'en-tête, afin de détecter ce type d'intrusions.

#### 2.6.2.3 Analyse comportementale

L'analyse comportementale représente sans doute l'avancée la plus intéressante en matière de détection des intrusions. Elle vise à modéliser les comportements des utilisateurs, afin de déterminer des «profils types» et de donner l'alerte lorsqu'un flux hors gabarit est détecté. A titre d'exemple, prenons un employé d'une agence de voyages qui soumet régulièrement des demandes auprès du siège d'une compagnie aérienne pour réserver

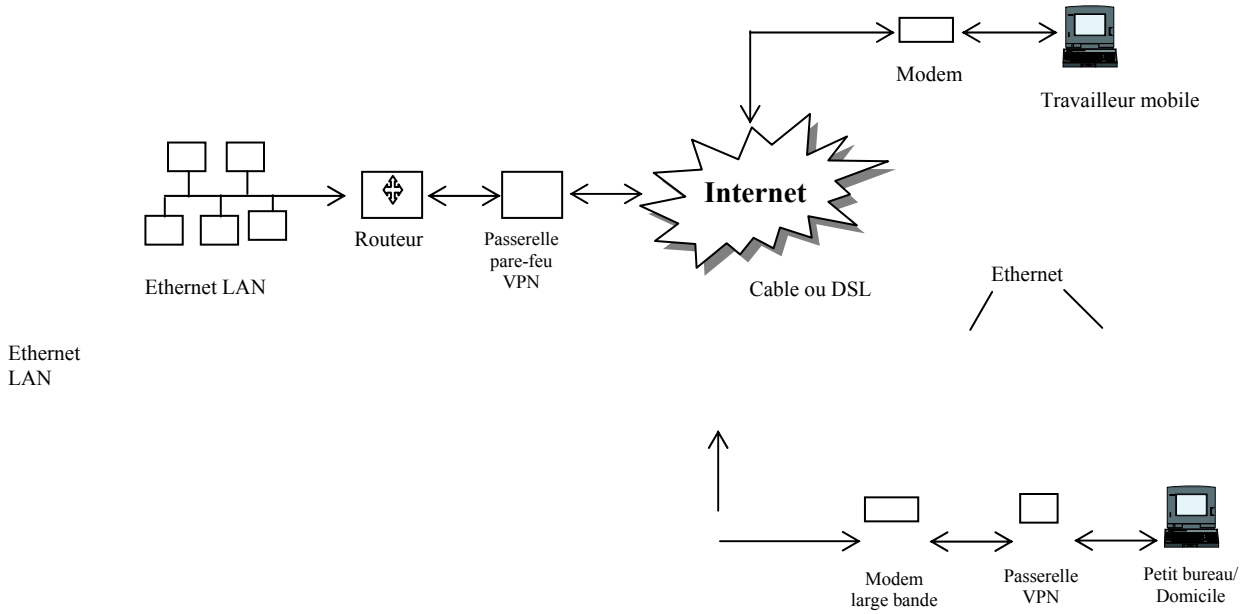
des billets d'avion. Il s'agit en général d'échanges transactionnels constitués de séquences de trames relativement courtes. Si au cours de la surveillance des flux on détecte des trames de longueur proche de l'unité maximale de transfert (MTU), une longueur inhabituelle dans ce cas, le moteur de l'analyse comportementale va donner l'alerte.

Il est à noter que ce type d'analyse fait appel à des moteurs d'inférence et à des techniques d'intelligence artificielle.

## 2.7 Réseau privé virtuel et infrastructure à clé publique

Le principe fondamental du réseau privé virtuel (VPN) est de partager en termes de sécurité des secrets pour pouvoir créer des liens sécurisés entre différents équipements, voire entre des postes clients et des équipements. Cette gestion des clés partagées constitue, par conséquent, un problème dès qu'il s'agit d'administrer un grand nombre d'équipements ou encore des équipements hétérogènes (émanant de plusieurs fournisseurs).

**Figure 4 – Exemple d'architecture VPN**




La nouvelle génération de VPN possède les caractéristiques suivantes:

- des communications meilleures et plus sécurisées sur l'internet, puisque les VPN assurent la sécurité au moyen de l'authentification et du chiffrement;
- la sécurité du courrier électronique (actuellement, un domaine très peu sécurisé);
- une efficacité améliorée et de meilleures communications avec les filiales de l'entreprise, les tierces parties et les utilisateurs distants qui se connectent au système.

Dans un VPN à secrets partagés (par exemple, un réseau d'ambassades), si l'un des équipements est compromis, l'ensemble des secrets et donc le VPN dans son ensemble sont compromis.

Pour éviter cela, il faut choisir une architecture utilisant une clé publique et une clé privée (voir la section 8). L'infrastructure à clé publique (PKI) intervient alors utilement, en ce sens qu'elle permet d'administrer les clés tant privées que publiques.

La fonction PKI ne permet pas de gérer les liens VPN, mais permet de fournir les clés d'authentification d'un équipement à l'autre, sur la base d'un annuaire (LDAP, *lightweight directory access protocol*, X. 509), commun à l'ensemble de l'entreprise et accessible à tous les utilisateurs, qui permette l'authentification stricte des équipements entre eux ou entre clients et équipements.

Toutefois, tout comme dans le monde réel, où nous ne possédons qu'une seule identité qui peut prendre des formes différentes, telles qu'un certificat de naissance, un passeport ou un permis de conduire, dans le monde virtuel, il faut peut-être envisager plus d'une infrastructure de sécurité, chacune donnant aux utilisateurs et aux applications des formes d'identité différentes, tout en coexistant et se complétant mutuellement. Les réseaux VPN devraient s'appliquer à une identité donnée qui a pu être authentifiée.

Des technologies telles que la PKI et l'infrastructure Kerberos (KI) peuvent fonctionner ensemble et donner de meilleurs résultats. La KI est née avec le projet Athena du MIT (*Massachusetts Institute of Technology*); Microsoft a pris la décision en 1999 d'utiliser, dans son système d'exploitation Windows 2000, la version 5 de Kerberos, en remplacement du protocole propriétaire d'authentification NTLM.

Dans une PKI, la nécessité pour l'utilisateur ou pour l'application de stocker des clés ou des informations confidentielles rend fréquemment plus complexe l'ensemble de l'architecture de la solution. Une solution courante (aucune alternative n'offrant le même niveau de sécurité) consiste à utiliser des cartes à puce, des lecteurs de cartes et des appareils de stockage des clés cryptographiques sur les serveurs.

La plupart des systèmes existants qui utilisent le protocole Kerberos n'exigent pas que l'utilisateur doive conserver une carte physique ou un équipement matériel comportant des informations privées. Ainsi, l'utilisation de Kerberos n'est normalement pas recommandée pour des applications dans lesquelles la non-répudiation ou la signature numérique est requise. Il est, pour cette raison, plus souvent utilisé pour authentifier une application ou un utilisateur, ainsi que pour assurer les services de confidentialité dans un réseau.

Toutefois, du point de vue de la sécurité, les informations privées doivent être traitées avec le même niveau de sécurité que les PKI sur le terminal de l'utilisateur. Par conséquent, il serait souhaitable que le système Kerberos passe par la sécurisation du stockage de l'information privée (par exemple, en utilisant un dispositif sûr tel que la carte à puce) sur le terminal de l'utilisateur. En outre, comme le serveur Kerberos (nommé KDC, centre de distribution des clés) partage les informations privées avec tous les terminaux utilisateurs dans la plupart des systèmes Kerberos, le système Kerberos est souvent utilisé dans un réseau privé.

L'introduction du protocole PKINIT dans le jeu des normes Kerberos permet à l'authentification PKI d'être employée dans un environnement Kerberos. La nature complémentaire des deux infrastructures peut ainsi être pleinement exploitée, puisqu'elles fonctionneront ensemble efficacement si la situation l'exige.

## 2.8 Cryptographie

La sécurité informatique débute souvent par la mise en place d'un logiciel antivirus assurant la protection des données et des systèmes, d'un pare-feu assurant la protection des réseaux et d'un système d'authentification assurant la protection des ressources.

L'introduction du commerce en ligne, de l'administration publique en ligne, etc., nécessite une protection renforcée afin de créer un espace sûr dans des réseaux vastes et hétérogènes. Cela implique l'utilisation de techniques de chiffrement, d'authentification, de tamponnage, d'accusé de réception et d'horodatage. Il s'agit de rendre un réseau homogène, d'appliquer des méthodologies communes émises par une autorité de confiance, d'utiliser des protocoles normalisés.

La cryptographie est la science qui fait appel aux mathématiques pour le chiffrement et le déchiffrement des données. Elle permet la sécurisation des informations confidentielles pour leur stockage ou pour leur transmission vers des réseaux ouverts tels que l'internet.

Le premier type de chiffrement est le chiffrement par clé secrète (ou clé symétrique). Une seule clé est utilisée pour le chiffrement et le déchiffrement. Un expéditeur et un destinataire, souhaitant communiquer de manière sécurisée, doivent convenir d'une clé et ne pas la divulguer. La transmission de la clé ne doit donc pas utiliser le même canal que celui du message protégé.

Les problèmes de distribution des clés sont résolus par la cryptographie à clé publique (ou clé asymétrique). Ce procédé nécessite une paire de clés: une clé publique et une clé privée. Tout ce qui est chiffré avec une des clés ne peut être déchiffré que par l'autre clé. On ne peut pas déduire une des clés à partir de la connaissance de l'autre clé. La cryptographie à clé publique présente l'avantage de permettre l'échange de messages de manière sécurisée, sans mise en œuvre préalable d'un dispositif particulier. L'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. Les communications impliquent uniquement l'utilisation de clés publiques, sans qu'une clé privée ne soit transmise ou partagée.

La combinaison de ces deux types de cryptographie, qui doit être utilisée avec précaution de manière que l'utilisateur n'ait pas une vision erronée de la sécurité, permet une sécurisation optimale. Soit un agent souhaitant envoyer un message chiffré:

1) il crée un couple de clés publique/privée;

2) il conserve la clé privée et envoie sa clé publique à ses destinataires;

3) il chiffre ses messages avec sa clé privée, qu'il est le seul à détenir;

4) les destinataires déchiffrent les messages avec la clé publique;

5) en retour, ils chiffrent leurs messages avec la clé publique de l'agent en question;

6) celui-ci reçoit les messages et les déchiffre avec sa clé privée.

La partie la plus vulnérable est l'utilisateur final.

Un autre avantage de la cryptographie asymétrique est qu'elle permet l'utilisation d'une nouvelle fonctionnalité, la signature électronique. Celle-ci permet au destinataire de vérifier son authenticité et son origine et de s'assurer qu'elle est intacte. Les signatures numériques garantissent donc l'authentification et l'intégrité des données: le message est haché et le résultat est chiffré avec la clé privée. Elles assurent également la fonctionnalité de non-répudiation, afin d'éviter que l'expéditeur dise qu'il n'a pas envoyé les informations.

Lorsque le destinataire reçoit le message et la signature (voir la Figure 5):

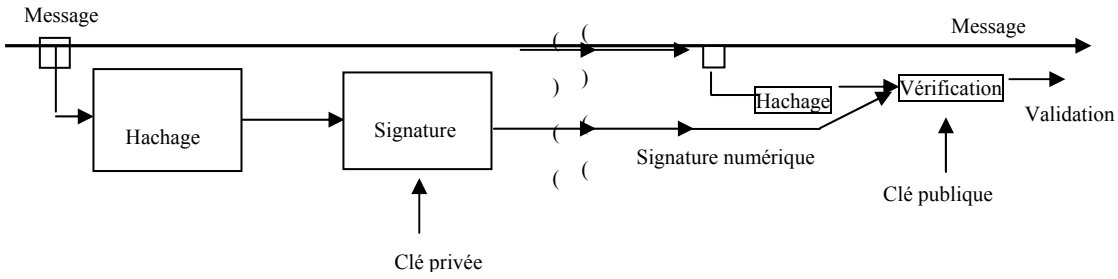
1) le message est haché. Le hachage est un algorithme mathématique opaque, qui ne permet pas de retrouver le message à partir de la condensation;

2) la signature est déchiffrée avec la clé publique;

3) les deux condensations sont comparées.

Il se peut qu'une personne mal intentionnée transmette sa clé publique en se faisant passer pour quelqu'un d'autre. Il est donc nécessaire de faire le lien entre une clé et son utilisateur; les certificats électroniques permettent de répondre à ce besoin. Un certificat électronique est un fichier qui permet de confirmer le lien entre un individu et sa clé publique. Il faut donc souvent établir des systèmes de sécurité, de stockage et d'échanges. Ceux-ci peuvent se présenter sous la forme de référentiels de stockage (serveurs de certificats) ou de systèmes structurés (PKI) qui assurent les fonctions de stockage et de gestion (émission, révocation, récupération, stockage) des certificats.

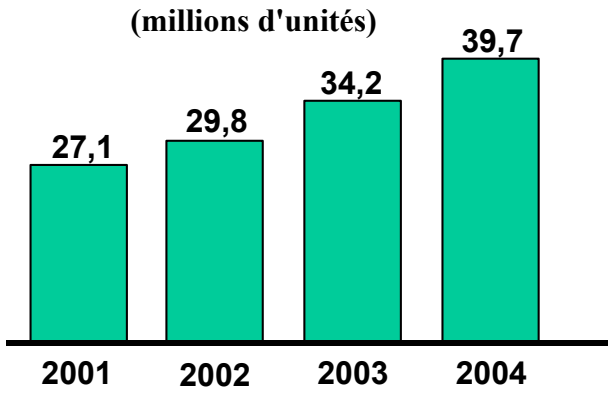
**Figure 5 – Principe général de la signature électronique**




## 2.9 Réseaux locaux hertziens

Selon les informations disponibles, l'industrie mondiale des réseaux locaux hertziens (WLAN) devrait connaître une croissance moyenne annuelle de 30% jusqu'en 2006. Le revenu estimé en 2002 s'élève à 1,97 milliard EUR (www.telecoms.com). Cette croissance est liée à l'usage intensif des ordinateurs portables tant au niveau des entreprises que du grand public: la répartition des ventes d'ordinateurs par type en 2002 est de 76,7% pour les ordinateurs fixes et de 23,3% pour les ordinateurs portables.

**Figure 6 – Ventes mondiales d'ordinateurs portables**




(Source: Gartner Dataquest)

Les administrateurs des réseaux hertziens sont très sensibilisés en ce qui concerne les risques encourus en raison de la non-maîtrise de la couverture radio. Tous les produits du marché sont capables de transporter des trames Ethernet et les topologies utilisées sont semblables à celles du monde filaire: soit une liaison de poste à poste (mode ad-hoc), soit un modèle en étoile, autour d'un point d'accès (AP) à travers lequel sont acheminées les trames radioélectriques (mode architecture).

Pour les petits réseaux (nombre d'abonnés inférieur à 10), l'emploi d'un réseau privé virtuel (VPN) permet d'assurer la défense contre les intrusions. Dès que le WLAN s'étend, les choses se compliquent et une interface d'administration souple pouvant véritablement contrôler l'accès entre plusieurs sous-réseaux doit être mise en œuvre; ce type d'équipement est désigné sous le nom de passerelles de sécurité WLAN. Ces passerelles WLAN sont, de par leur nature, conçues pour fonctionner avec des points d'accès (AP), pour

gérer les problèmes de permanence ou de restauration de clé lors des changements de cellule et surtout pour extraire leurs informations de crédence d'un annuaire central. Cette approche facilite la définition des groupes particuliers ayant le droit d'exploiter les connexions WLAN et élude l'épineux problème de l'acceptation de stations invitées ou temporaires.

**Sécurité des WLAN**

Les entreprises qui utilisent les réseaux locaux (LAN) hertziens, sans prendre les mesures de sécurité appropriées, s'exposent aux piratages les moins sophistiquées. Or, une faille dans la sécurité du réseau, aussi infime soit-elle, est un problème pour l'entreprise. Pénétrant par cette brèche, les pirates (hackers) peuvent en effet accéder aux mots de passe de l'entreprise, se connecter aux serveurs et s'approprier des informations confidentielles, prendre le contrôle du site web, ou même paralyser le réseau tout entier.

L'utilisation d'un WLAN hertzien oblige les entreprises à déployer des mesures de sécurité appropriées.

Le niveau de sécurité le plus élémentaire pour les WLAN est celui de la *Wired Equivalent Privacy* (WEP).

La WEP, élaborée par l'*Institute of Electrical and Electronics Engineers* (IEEE), est conçue pour: a) assurer une sécurité de base; b) prévenir l'écoute accidentelle dans le réseau; et c) protéger le réseau par le chiffrement de toutes les données transmises par la technique hertzienne, au moyen d'un algorithme RC4 (Ron's Code 4) reposant sur une clé de chiffrement partagée à 40 bits.

Les clés WEP sont des mots de passe à secret partagé, qui permettent aux utilisateurs de déchiffrer les données chiffrées transitant sur le réseau hertzien. Dans la pratique, un pirate peut accéder aux clés de chiffrement, en étant simplement posté devant le bâtiment de l'entreprise et en interceptant le flux de données chiffrées sur un ordinateur portable, puis en les décryptant avec un logiciel spécial, facilement téléchargeable sur l'internet. Cette méthode, sorte de décodage à l'envers, révèle la clé au pirate et lui donne accès au réseau de l'entreprise.

La clé de chiffrement de l'algorithme ne constitue pas un défaut en soi, bien qu'une piètre gestion des clés puisse les rendre vulnérables au piratage. Les administrateurs du système ne vont souvent attribuer qu'une seule clé à toute l'entreprise, ce qui veut dire que lorsque le pirate s'est approprié la clé, il a un accès potentiel à l'ensemble des informations propres à l'entreprise, ainsi qu'aux ressources du réseau. L'administrateur peut aussi attribuer une clé différente à chaque utilisateur, mais, dans ce cas, en ne les changeant jamais, il figera le système. Quoi qu'il en soit, lorsque le pirate est entré, il conservera l'accès si l'environnement de clé est statique et partagé. La gestion manuelle de la clé peut facilement s'effectuer dans de plus petits réseaux, rigoureusement administrés. Toutefois, la tâche peut s'amplifier et devenir pesante à mesure que le nombre d'utilisateurs du réseau hertzien s'accroît, reflétant, la plupart du temps, la négligence de l'administrateur du système.

La sécurité des réseaux locaux plus étendus fait appel à des spécifications de pointe, comme le changement automatique de clés, et doit également s'appliquer au-delà des réseaux eux-mêmes, en raison du grand nombre d'utilisateurs et des exigences sécuritaires plus complexes. Habituellement, les plus grandes installations sont celles qui nécessitent une technologie d'administration des clés de chiffrement plus robuste, des mécanismes d'authentification, et une gestion centralisée des utilisateurs par l'intermédiaire de l'infrastructure du réseau, qui ne doivent pas résider dans la mémoire limitée d'un point d'accès WLAN.

Tandis que, en dépit de la vulnérabilité en matière de sécurité, la sécurité de la WEP reste localisée – administrée aux points d'accès du WLAN – un plus grand système doit prendre en charge des milliers d'utilisateurs, ainsi que les techniques de pointe du chiffrement et de l'authentification, exigeant généralement une solution de sécurité administrée à partir d'un point central. D'habitude, ces systèmes sont administrés par une infrastructure RADIUS (*remote authenticated dial-in user service*). Cette dernière autorise la gestion centralisée et l'administration d'un grand nombre d'utilisateurs autorisés à accéder aux ressources du réseau.

Le fait que RADIUS admette la norme de connexion de réseau 802.1x pour un réseau Ethernet filaire 802.11 pour un réseau hertzien améliore considérablement la capacité d'authentification de l'utilisateur dans le réseau hertzien d'entreprise. Etant donné la nature mixte de la plate-forme d'infrastructure des réseaux d'aujourd'hui et la diversité des systèmes d'exploitation Windows en entreprises, la possibilité de simuler la norme 802.1x apporte des moyens supplémentaires de sécurité hertzienne de qualité supérieure et évolutive. Les fonctionnalités techniques assurées sont notamment les suivantes:

- prise en charge de connexions de réseau 802.1x pour les systèmes Windows existants;
- un certificat de client universel permettant l'authentification mutuelle sur la base d'un certificat;
- une administration protégée au moyen de clés, avec prise en charge des protocoles RADIUS-EAP (*extensible authentification protocol*)-TLS (*transport layer security*);
- une intégration dans les environnements RADIUS existants, qui prennent en charge le protocole MD-5 (*message digest* 5);
- une prise en charge des multiples schémas d'authentification avec le protocole EAP.

**Solution technique pour le Wi-Fi**

Afin de rendre l'exploitation des réseaux hertziens d'entreprise Wi-Fi viable et fiable, on applique actuellement une solution technique dénommée «commutation sans fil». Cette démarche innovante consiste à placer l'ensemble des fonctionnalités administratives du réseau (paramètres radio, sécurité, connectivité avec le réseau filaire) dans un commutateur spécifique, de façon à «soulager» les points d'accès et à centraliser la gestion de l'infrastructure Wi-Fi.

Contrairement à un commutateur Ethernet traditionnel, un commutateur Wi-Fi gère comme il convient le trafic IEEE 802.11 provenant des points d'accès avec lesquels il est relié (en fait, de simples ponts Wi-Fi/Ethernet). Cela lui permet de contrôler entièrement le réseau hertzien.

Dans ce modèle, les administrateurs du réseau ont accès à une interface de configuration unique, qui leur donne une vision globale du réseau et de ses utilisateurs. Ils peuvent gérer ceux-ci comme est géré le réseau filaire existant de l'entreprise: authentification auprès d'un service RADIUS, LDAP, ou même Active Directory (ce qui permet de réutiliser les comptes utilisateurs des domaines Windows pour le contrôle d'accès au réseau), contrôle de la bande passante employée par utilisateur, configuration dynamique de réseau DHCP (*dynamic host configuration protocol*), etc.

En adoptant la solution du commutateur Wi-Fi, l'équipe d'administration peut se protéger efficacement contre les menaces propres aux réseaux hertziens:

– Intrusion au point d'accès (désactivation par désauthentification, c'est-à-dire envoi d'instructions qui empêchent les utilisateurs de s'authentifier au niveau du terminal): détection automatique et envoi de paquets de déconnexions à l'ensemble des clients afin d'assurer leur protection.

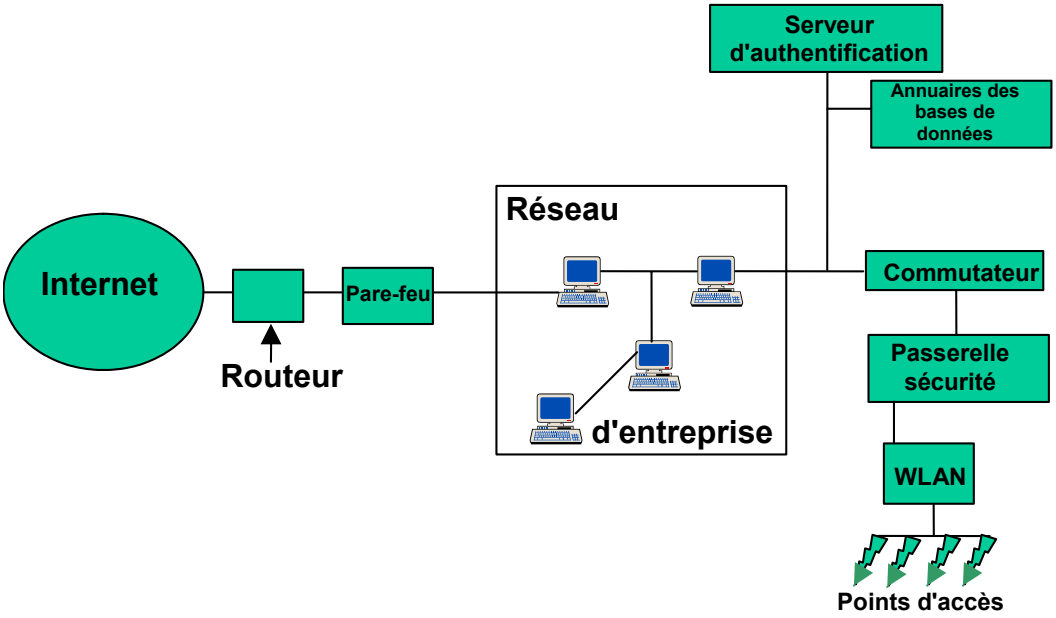
– Déni de service (saturation): contrôle de la fréquence des opérations de gestion de réseau.

– Usurpation d'identité (homme au centre): détection de l'usurpation d'adresses Wi-Fi.

– Ecoute passive (renifleurs): le matériel utilisé prend l'empreinte des outils d'écoute passive et exclut ceux-ci du réseau.

Quels que soient le niveau et l'étendue de la sécurité hertzienne exigés par l'infrastructure du réseau, une solution en couches peut être mise au point pour répondre aux exigences particulières. Les solutions de sécurité hertzienne vont de la simple WEP, fondée sur des normes, à la sécurité administrée aux points d'accès, avec une sécurité robuste et évolutive administrée centralement, et de l'infrastructure filaire à l'infrastructure hertzienne.

**Figure 7 – Réseau de sécurisation WLAN**

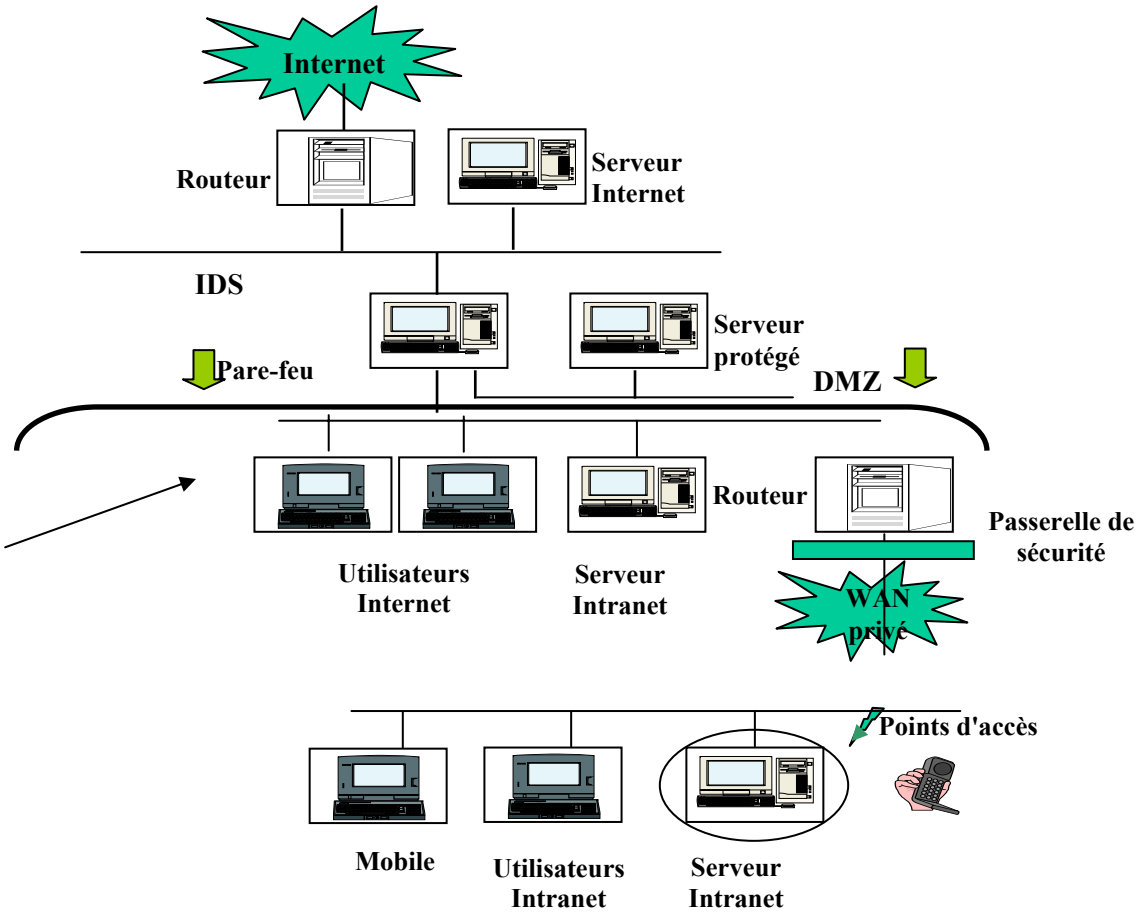



NOTE – Sur de nombreux portables est actuellement utilisée pour le stockage une clé USB (*universal serial bus*), c'est-à-dire de la mémoire flash qui joue le rôle d'un disque dur amovible (de 32 Mo à 512 Mo). De nombreux fabricants fournissent des clés USB avec un logiciel de sécurisation permettant de protéger les données, en cas de perte ou de vol, au moyen d'un mot de passe. Des systèmes plus sophistiqués emploient les empreintes digitales (biométrie).

## 2.10 Résumé

Dans les paragraphes précédents, on a décrit les principaux moyens de sécurisation d'un réseau de communication et d'information et présenté une approche de la sécurité orientée sur la prévention des risques associés aux nouvelles technologies de l'information et de la communication (NTIC). Ci-après est donné un exemple de sécurisation d'un réseau.

**Figure 8 – Exemple de sécurisation d'un réseau**




## 3 Intrusions/attaques automatisées

Les équipements et logiciels décrits dans la section 2 sont les gardiens des réseaux de communication et de télécommunication qui, de par leur connexion à l'internet, sont vulnérables. Chaque message électronique et chaque fichier acheminé par le réseau est traité par ces équipements. Ci-après sont décrits les outils et les techniques couramment employés par les pirates pour les attaques contre les réseaux.

### 3.1 Virus

Les virus sont des morceaux de codes informatiques destinés à s'intégrer dans un programme normal. L'exécution du programme ainsi infecté active le virus qui peut dès lors se propager ou influer plus ou moins gravement sur la stabilité de l'ordinateur. Un virus peut détruire la totalité des données d'un ordinateur tout comme il peut se contenter d'afficher un texte hostile par exemple.

Des virus divers – virus de fichiers exécutables, macrovirus, virus de scripts et vers sophistiqués – exploitent les failles de sécurité des systèmes d'exploitation pour se répandre à travers les réseaux (voir la Figure 9).

Dans sa définition la plus large, un virus informatique est un programme autoreproducteur, c'est-à-dire qui réalise des copies de lui-même dans des fichiers existants.

Les virus se caractérisent par leurs mécanismes de reproduction et d'infection d'un poste – dans la zone de démarrage, dans les fichiers d'application ou encore dans les fichiers exécutables – et non par leurs effets. Les dégâts sont multiples: simple message, effacement de fichiers, formatage du disque, flashage de la mémoire CMOS, voire installation sur le poste d'un cheval de Troie (un cheval de Troie est un programme présent sur un poste, qui attend d'y ouvrir une brèche de sécurité: «bombe dans le temps», portes dérobées, logiciel espion, etc.). Il s'agit d'une fonction malicieuse cachée dans un fichier présenté comme sain. Il est à noter que les chevaux de Troie ne se reproduisent pas: ils sont envoyés ponctuellement par des utilisateurs malveillants ayant bien ciblé leur future victime.

Les premiers virus connus datent de la fin des années 80. Ils s'installaient dans la zone de démarrage des disquettes et des disques durs et contaminaient toute nouvelle disquette insérée. Rapidement, d'autres virus ont infecté les PC en contaminant les fichiers exécutables. Un même programme pouvait être contaminé plusieurs fois et son fichier grossissait donc sans cesse. Puis, les programmeurs se sont inspirés d'un virus existant pour en réaliser une version plus efficace. Ainsi, la deuxième génération de virus de fichiers exécutables, plus perfectionnés, ne réinfectait pas les fichiers déjà atteints.

La prolifération des virus est étroitement liée au mode de sécurisation des systèmes d'exploitation. Ainsi, dans les systèmes Windows, tout utilisateur peut modifier les fichiers système, exécutables compris, sans le moindre contrôle. Même les systèmes d'exploitation récents à vocation professionnelle, comme Windows NT ou 2000, ne mettent en œuvre une véritable politique de sécurité pour les fichiers que s'ils utilisent le format NTFS (*new technology file system*) qui permet de définir des attributs pour chaque fichier. Reste qu'un grand nombre d'utilisateurs se connectent sous le mode administrateur, facilitant ainsi une faille. La diffusion d'un virus exécutable est assez facile sur ce type de système, contrairement à ce qui passe dans les fichiers système. Il existe toutefois des attaques ciblées sur Unix et des vers ciblés sur Linux ou sur Solaris. Ces programmes exploitent les failles de sécurité dans le réseau particulières pour avoir accès au compte racine et contaminer le système.

### 3.1.1 Virus multipartite et polymorphe

A partir de 1996, une nouvelle génération de virus voit le jour: les macrovirus. Initialement, les macrovirus servent à automatiser un certain nombre de tâches. Il existe même des virus multipartites, qui passent d'une application Office à une autre. On entend par virus polymorphes, des virus qui contiennent un code spécial rendant chaque infection différente de la précédente. Ce type de virus comporte un code qui modifie sa signature afin qu'il ne soit pas repéré. Un virus polymorphe peut prendre des millions de formes différentes.

Avant l'apparition des macrovirus, seuls les spécialistes maîtrisant la programmation en langage machine étaient en mesure de créer un virus. Avec un langage de programmation évolué, il est toutefois simple, une fois les principes de base compris, de programmer un macrovirus, et il est très facile de créer une variante (ou un mutant) à partir d'un échantillon de virus existant.

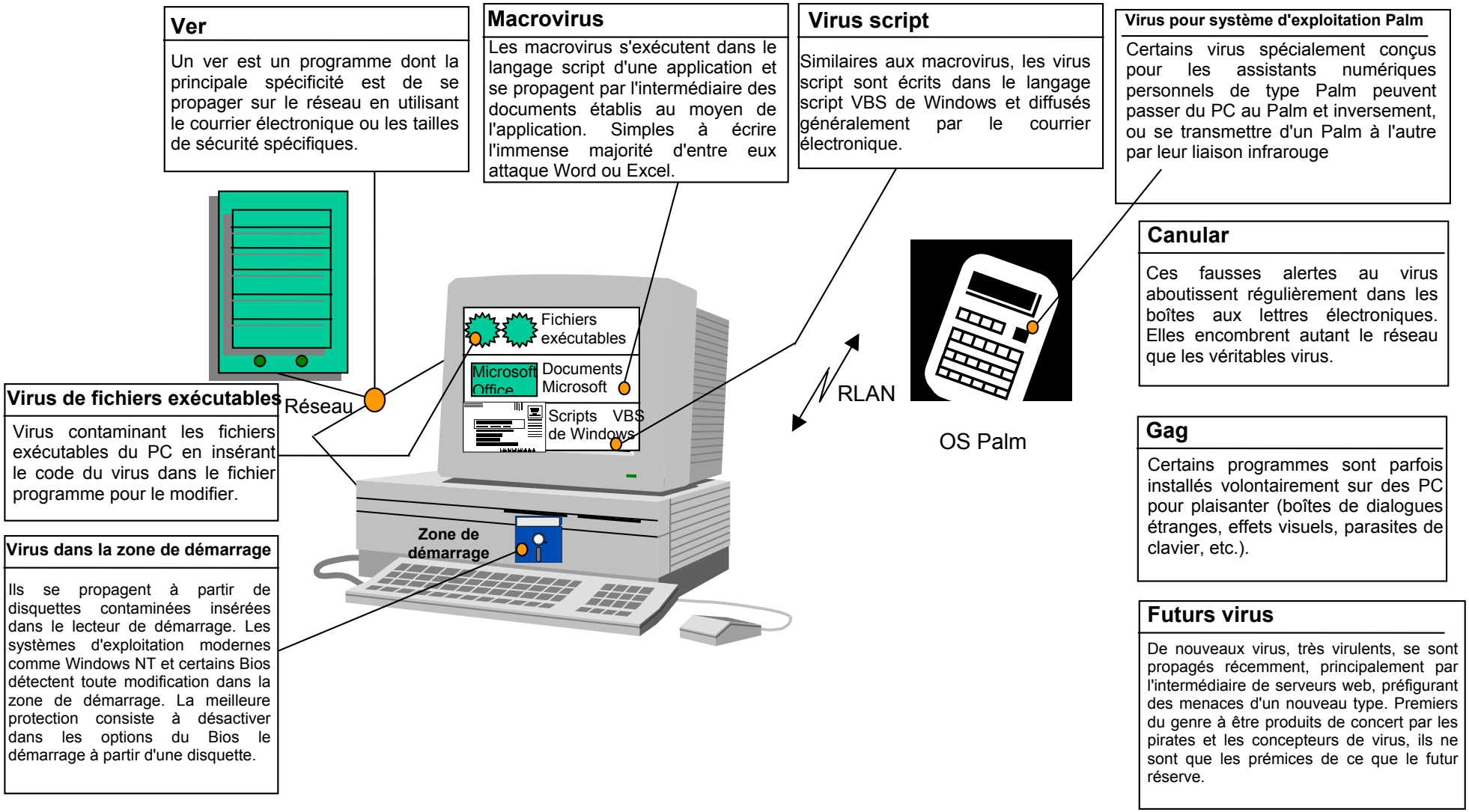
Même si par mutant, on entend une nouvelle variante d'un virus déjà connu, un virus ne mute jamais de lui-même; toute mutation nécessite un programmeur.) Les macrovirus constituent, à l'heure actuelle, plus de 95% des virus en circulation. Ils profitent des facilités d'accès au réseau et au courrier électronique des applications Office.

L'automne 2000 a vu apparaître un autre type de parasite informatique: le virus script, écrit uniquement en VBS (*visual basic script*), ce qui le distingue des macrovirus. Autre différence, il n'affecte que les fichiers système Windows.

Depuis 2001, les virus exécutables connaissent un retour en force. Les mutants récents sont devenus des programmes très complexes qui utilisent des techniques de piratage pour pénétrer dans les systèmes et se propager.

Dans la Figure 9 ci-après sont donnés les différents types de virus pouvant affecter un réseau de communication.

**Figure 9 – Les différents types de virus**



### 3.1.2 Logiciels malveillants, la menace virale de demain

L'accélération du développement des infrastructures de communication, la généralisation du haut débit, la banalisation des échanges sur l'internet, sont autant de facteurs qui ont permis de faire quasiment disparaître la limite de taille des messages électroniques, de leurs pièces jointes, des fichiers téléchargés, etc.

Cet état de fait a engendré une mutation dans la nature même de l'ensemble des virus informatiques (virus, vers, chevaux de Troie, et autres codes malveillants) qui, en quelques années, sont devenus de véritables progiciels, avec une panoplie de fonctionnalités spécifiques.

Cette nouvelle génération de virus, qu'il convient désormais d'appeler «*malware» (malicious software*), bénéficie d'une telle avancée technologique que la menace actuelle et à venir est sans commune mesure avec ce que nous avons pu connaître jusqu'à présent.

**Fonctionnalités virales utilisées**

Pour bien comprendre cette situation, il convient de décrire certaines fonctionnalités virales qui deviennent de plus en plus courantes.

- Téléchargement et implantation d'outils de piratage automatisés. Le «*malware*» «*HackTool/Scansql.A»* permet, par exemple, d'employer sur le poste atteint un outil légal et bien connu pour rechercher des mots de passe autorisant l'accès aux serveurs MS SQL (*Microsoft structured query language*) en utilisant un simple fichier texte comme liste d'essai de mots de passe.

  Si les mots de passe comportent, comme dans 80% des cas, des prénoms, des noms ou des mots courants, le résultat de cette recherche est alors automatiquement mis à disposition du ver suivant, du hacker ou de l'utilisateur malveillant suivant.

- Prise de contrôle à distance.

  Des chevaux de Troie du type «*W32.Sobig»,* permettent la prise de contrôle à distance d'un ordinateur, et l'exécution de tout programme ou d'une quelconque opération.

- Récupération et envoi automatique des mémoires tampon de clavier par SMTP (*simple mail transfer protocol*) ou FTP (*file transfer protocol*).

  Les vers et/ou chevaux de Troie du type «*W32/lovgate»,* sont très perceptibles, de par leur évolution sur le plan technique et la multiplicité des processus déclenchés.

  En effet, ce type de virus regroupe, pour la première fois, l'ensemble des fonctionnalités décrites ci-dessus, avec, en plus, l'ouverture d'une porte dérobée, qui permet la recontamination du poste informatique après l'éradication du virus. De plus, son mode de compression lui permet d'être exécuté directement, dès la prévisualisation dans le logiciel de messagerie, et sans aucune décompression préalable.

- Création d'un serveur SMTP spécifique, destiné à la diffusion virale, sur chaque poste contaminé.

- Création, en continu, de domaines sur des serveurs distants.

- Récupération de l'ensemble des adresses électroniques sur un poste informatique, afin d'alimenter son propre serveur SMTP.

- Attaque par déni de service des serveurs de messagerie, et exploitation quasi instantanée des failles de sécurité apparues.

- Récupération des adresses IP (Protocole Internet) des postes informatiques, en se connectant au fournisseur d'accès, par l'intermédiaire des adresses de messagerie.

- Modification de la signature automatique dans le logiciel de messagerie, assurant la diffusion lors de l'envoi de chaque message; installation de raccourcis dans la liste des favoris du navigateur internet; ajout de boutons dans la barre d'outils; modification de la page de démarrage qui s'affiche automatiquement à l'ouverture du navigateur.

Le ver «*Js/Fortnight»,* entre autres, utilise cette méthode pour se répandre et surtout recontaminer automatiquement les stations informatiques au moyen du téléchargement de son code lors des accès à l'internet.

Cette complexité de la menace et son ampleur conduisent à l'utilisation d'outils de gestion lourds, comme, par exemple, les bases SQL, dont le seul but est de gérer les alertes générées par les virus.

On assiste également à une situation problématique et extrêmement inquiétante: les systèmes d'exploitation sont de mieux en mieux connus et la «communauté attaquante» découvre sans cesse de nouvelles failles, qui sont immédiatement et délibérément mises à profit.

**Conclusion**

La sécurité des entreprises face aux virus informatiques est une question urgente. L'enjeu est important, si l'on en juge par l'évolution de la vitesse de propagation des virus en fonction de l'évolution de leur nature depuis les années 90.

Au début des années 90, le temps de réaction face à un virus de fichier était de l'ordre du mois, tandis qu'il était de l'ordre de l'heure pour un virus de message électronique à la fin des années 90. Aujourd'hui ce temps de réaction est de l'ordre de la minute. Il est clair que demain, avec l'apparition des menaces instantanées, les codes malveillants causeront des dégâts dans la seconde.

Il est possible d'envisager des actions destructrices comme le *flashage* automatique du *BIOS* à la fermeture d'une session, le déplacement des pistes de démarrage des disques durs, le formatage automatique, la transformation généralisée par écrasement de tous les fichiers exécutables en virus ou la modification généralisée des profils utilisateur en réseau, etc.

Toutes ces possibilités techniques existent, mais sont encore difficiles à implanter sans être détectées avec les langages de programmation actuels. L'élaboration d'un langage spécifique et de son compilateur associé n'est toutefois plus inconcevable et laisse présager de la nature des menaces à venir.

La gestion du risque viral est de plus en plus complexe, et les nouveaux virus informatiques exigent des protections successives de plus en plus nombreuses, même au niveau du système d'exploitation qui doit aussi s'autoprotéger. Le fait que Windows XP dispose aujourd'hui de son propre pare-feu au niveau du poste de travail, est symptomatique de cette tendance.

La sécurisation globale des réseaux et des entreprises face aux virus informatiques de toute nature reste du ressort des spécialistes, en raison de la nécessité de suivre les «nouveautés», l'évolution technique constante des logiciels malveillants et l'imagination hors normes de leurs auteurs.

## 3.2 Techniques d'évasion et d'insertion

Plus les solutions de systèmes de détection d'intrusion (SDI) gagnent en popularité et plus les pirates redoublent d'ingéniosité pour développer de nouvelles méthodes permettant de repérer les détecteurs. Ces techniques, qui visent à empêcher le SDI de déclencher une alerte (voir le paragraphe 2.6), peuvent être classées en deux catégories.

### 3.2.1 Techniques d'évasion

Il s'agit ici de déguiser la chaîne d'attaque, de manière qu'elle soit correctement interprétée par le système cible, mais pas par le SDI.

Le serveur web attaqué va automatiquement supprimer les caractères excédentaires, de sorte que le SDI voit une séquence différente et ne déclenche pas l'alerte. Un certain nombre de systèmes SDI sont capables de détecter ce type de technique d'évasion, mais ce n'est pas systématique et doit être vérifié lors d'une validation technique.

Des techniques plus avancées d'évasion font appel à des codes polymorphes.

### 3.2.2 Techniques d'insertion

Contrairement aux méthodes d'évasion, ces techniques consistent à insérer, dans la signature, des séquences de caractères qui sont décodés par le SDI, mais non par la cible visée. Une méthode courante consiste à découper la signature et à insérer des fragments supplémentaires présentant une erreur au niveau de la somme de contrôle de l'en-tête TCP.

En effet, peu de SDI, disponibles sur le marché, effectuent des contrôles de ce champ (pour des raisons de performance essentiellement), de manière que la séquence parasite est insérée dans la chaîne d'attaque. Du coté de la cible en revanche, le fragment inséré est automatiquement supprimé par la pile TCP/IP qui effectue les contrôles nécessaires sur les sommes de contrôle.

## 3.3 Déni de service

### 3.3.1 Déni de service

Les attaques par déni de service (DoS) sont une préoccupation commune et récurrente dans le monde des réseaux en ce qui concerne leur infrastructure de sécurité. En empêchant les accès entrants et sortants de l'internet, ces attaques peuvent perturber l'entreprise dans la gestion de ses affaires en ligne, ainsi que dans ses relations avec les clients et les actionnaires. Un arrêt pendant quelques heures des systèmes d'information peut nuire énormément à la réputation de l'entreprise et éroder la fidélité de ses clients.

Les attaques DoS traditionnelles visent à faire tomber un ordinateur ou un réseau en panne, en le saturant au moyen d'un grand volume de trafic utilisant les paquets de données TCP (*transmission control protocol*), UDP (*user datagram protocol*) ou ICMP (*internet control message protocol*).

Individuellement, ces paquets semblent inoffensifs, et leur passage à travers les pare-feu et les routeurs d'une entreprise n'en est que plus facile. Déguisés en trafic licite, ou bien en trafic provenant du fournisseur de l'équipement, ces paquets sont souvent exemptés des contrôles que subit normalement chaque paquet.

### 3.3.2 Déni distribué de service

Une attaque DDoS est plus perfectionnée qu'une attaque DoS, et sa popularité augmente dans le milieu des pirates.

Le DDoS utilise de nombreuses machines connectées à l'internet. Cette nouvelle attaque se sert d'un nombre important de systèmes déjà compromis pour lancer un torrent d'attaques distribuées à destination d'une seule cible. Cette opération se fait en chargeant un logiciel sur les machines déjà compromises, situées sur différents réseaux d'entreprises ou d'institutions publiques.

Les pirates préfèrent les réseaux d'universités comme sites de lancement des attaques DDoS, parce que les applications y sont fort réparties. Une fois le logiciel installé sur des centaines de machines, l'attaquant peut les activer à distance.

# 4 Principes de sécurisation des réseaux

## 4.1 Organisation

Dans une administration/entreprise, la sécurité doit être assurée par le service du RSSI (responsable sécurité des systèmes d'information) et le service sécurité production ou SOC (*security operation centre*).

Le service du RSSI relèvera d'une direction générale en vue de définir une politique de sécurité adaptée aux besoins, aux métiers et aux objectifs de l'entreprise/administration.

Le RSSI doit inclure le sujet des réseaux hertziens dans la campagne de sensibilisation des utilisateurs à la sécurité pour leur faire comprendre le danger lié aux réseaux sans fil. Le but est qu'ils signalent au service sécurité toute connexion hertzienne établie sans authentification.

De manière générale, le RSSI doit intégrer la problématique des réseaux hertziens dans sa politique de sécurité et ses procédures. Il est à noter que la norme ISO 17799 ignore l'existence des réseaux hertziens (voir la section 5).

Le service sécurité production ou SOC fera, quant à lui, partie de la direction informatique, au même titre que le service informatique qui gère les serveurs centraux ou le service bureautique qui gère les micro-ordinateurs et les serveurs bureautiques.

Un service sécurité production (SOC) gère, d'une part, les composants du système d'information, dont l'objectif principal est la sécurité et donne, d'autre part, une vision globale de la sécurité dans l'ensemble du système d'information (un point d'accès sans fil est toujours situé sur le périmètre du réseau; en conséquence, comme tous les périphériques situés sur le périmètre du réseau, ce point d'accès doit être géré par le SOC). Ces fonctions centralisées s'appuient notamment sur l'analyse et la corrélation des données répertoriées et sur la détection d'intrusion.

Ces composants du système d'information comportent tous les moyens d'interconnexion avec l'extérieur, qui sont situés sur le périmètre de l'entreprise/administration pour l'accès à l'internet, le VPN (*virtual private network*) pour les accès distants, les extranets et les plates-formes de commerce électronique. Ces équipements sont gérés de manière opérationnelle par un service spécialisé, orienté sécurité. La même chose vaut pour l'authentification des utilisateurs, par exemple, dans le cas des accès distants ou des accès à l'internet.

## 4.2 Recherche de l'origine d'un incident de sécurité

La surveillance de l'activité (*monitoring*) de l'ensemble des composants formant le système d'information est essentielle durant toutes les phases de la recherche d'incident. Cette surveillance a pour objectif de suivre l'activité (sur le réseau, mais aussi dans les composants du système d'information) exercée par la personne malveillante, de déterminer si d'autres personnes utilisent les mêmes failles à des fins malveillantes et également de visualiser l'étendue de l'incident.

Les faits à surveiller sont les échanges sur réseaux (date et heure des activités, volume des données échangées, adresses émettrices et adresses de destination), mais aussi l'activité dans les composants du système d'information (charge CPU et/ou mémoire employée dans un serveur, modification d'un programme binaire, ajout et/ou destruction de données dans un serveur, etc.).

Les éléments de surveillance du réseau (*network monitoring*) doivent être placés à des endroits précis du réseau. On suppose que ces éléments ne sont pas compromis, notamment en ce qui concerne l'intégrité des fichiers d'enregistrement. Les éléments de surveillance de l'activité d'un composant emploient principalement des logiciels de pilotage de la charge (Patrol, HP Open View, etc.) ou des fichiers d'enregistrements (fichiers log).

A ce stade, il est important que l'ensemble des horloges des composants du système d'information soient synchronisées, afin de faciliter la corrélation entre les évènements. Une technique de surveillance du système d'information consiste à effectuer une surveillance à grande échelle pour déterminer le périmètre à couvrir, puis de concentrer cette surveillance sur les composants réellement concernés par l'incident (analyse d'un service particulier ou d'un compte utilisateur spécifique, etc.).

**Reconstitution du système d'information**

L'objectif de cette phase est de reconstruire le système d'information, de manière à mettre fin à l'incident et à empêcher qu'il ne se reproduise. Cette phase ne peut être mise en place qu'après une analyse complète de l'incident: identification des personnes malveillantes, ainsi que de leurs différents modes opératoires (chevaux de Troie, comptes utilisateurs, etc.).

Le niveau de privilège obtenu par la personne malveillante permet de déduire les actions qu'elle a pu mener. En outre, la position dans le réseau du composant compromis (position dans la topologie du réseau, mais aussi position dans le domaine de confiance entre composants) peut révéler d'autres composants à inclure dans le périmètre de reconstruction.

Si l'ensemble des modes opératoires a été identifié, la reconstitution des composants peut se faire en se fondant uniquement sur les vulnérabilités exploitées par les personnes malveillantes. Si des zones d'ombre subsistent, il est recommandé de reconstituer les composants à partir des CD-ROM d'origine de l'éditeur. L'utilisation de sauvegardes ne convient pas toujours. En effet, il faut s'assurer que l'incident a eu lieu après la sauvegarde utilisée, car, si tel n'est pas le cas, le cheval de Troie et la même vulnérabilité seraient aussi restaurées. Après cette restauration, il convient de renforcer la sécurité du composant compromis et de corriger les vulnérabilités.

Evidemment, la procédure de remise en service des composants concernés ne se fait pas dans sa totalité directement sur le réseau. C'est seulement lorsque le composant est complètement reconstitué qu'il peut à nouveau être exploité et raccordé au réseau interne de l'entreprise. De nombreuses entreprises augmentent leur niveau de sécurité en fonction des évènements qui les touchent. C'est donc dans cette phase que de nouveaux moyens de sécurité peuvent être mis en place comme, par exemple: modifier la topologie du réseau et établir des listes de contrôle d'accès, renforcer les contrôles d'intégrité, mettre à jour la base des utilisateurs, appliquer une politique de sécurité, sensibiliser les utilisateurs, etc. Bien entendu, toutes ces mesures ne peuvent être mises en œuvre dans les jours qui suivent l'incident, mais il est essentiel que le responsable de la sécurité des systèmes d'information (RSSI) établisse un plan d'action s'étendant à plusieurs mois, voire à plusieurs années.

**Formalisation**

L'ensemble des actions qui ont été menées dans le cadre de la réponse à un incident doit être formalisé et rassemblé dans un dossier pour analyse ultérieure. Cette documentation permet, le calme revenu, de refaire les mêmes tests, de déterminer si des preuves sur le plan technique peuvent avoir été effacées par des enquêteurs, de reformuler d'éventuelles conclusions, de prouver techniquement l'existence d'un incident (et peut-être d'un suspect) dans le cadre d'une procédure judiciaire ou administrative. Le déroulement d'une affaire peut s'étaler sur plusieurs mois, et il est très difficile de se rappeler de toutes les actions menées, si elles n'ont pas été formalisées dès le début. Il est donc évident que l'étape de formalisation est importante.

Il faut toujours avoir présent à l'esprit que l'attaquant peut avoir atteint le réseau au moyen d'un grand nombre d'éléments et mis en place plusieurs détecteurs qui lui permettent de savoir si son activité a été repérée. L'ensemble des échanges électroniques, les preuves techniques recueillies, ainsi que les rapports sur l'incident, etc., doivent être enregistrés en dehors du système d'information. Il n'est pas rare, en effet, que l'attaquant se tienne informé en lisant ces informations, puis modifie certaines données ou détruise certaines preuves techniques. Ce rapport permet, à terme, de proposer de nouvelles actions de sécurisation du système d'information et d'élever le niveau de sécurité globale de l'entreprise.

**Conclusion**

La recherche des preuves techniques d'un incident n'est pas simple. Seules des actions précises, menées selon une méthodologie telle que celle décrite précédemment, peuvent encadrer avec précision une démarche rigoureuse, afin que l'attaquant, après un premier effet de surprise initiale, ne continue pas à surprendre, et que les incidents de sécurité ne constituent plus une menace de catastrophe.

## 4.3 Solutions intégrées de sécurisation du cyberespace

La sécurité doit être assurée dans tous les domaines de la société de l'information et des nouvelles technologies. Tout acteur de la chaîne de l'information doit être conscient du problème sécuritaire et doit participer à la mise en place de **solutions intégrées**.

Les solutions globales pour la sécurité du cyberespace (société de l'information) doivent prendre en compte tous les aspects, de l'analyse globale des risques jusqu'à l'intégration des solutions optimisées, et des avancées à moindre coût jusqu'à la maîtrise de la sécurité:


### 1) Analyser: conseil et services de gestion de risques sécuritaire

- Analyse et évaluation des risques (informatiques, juridiques, sociaux, etc.)
- Audits techniques et fonctionnels de sécurité (ISO, UIT, etc.)
- Tests de vulnérabilité et d'intrusion/recensement des failles
- Organisation de la gestion de la sécurité
- Politique de sécurité et schémas directeurs y compris la veille sécuritaire active
- Formation et sensibilisation à la sécurité
- Secours informatique, suivi des activités et gestion de crise.

### 2) Sélectionner et déployer: mise en œuvre et déploiement de la sécurité

Sélectionner: Valider l'architecture, évaluer les pilotes, sélectionner les technologies, fournir les solutions

Déployer: Mettre en œuvre, intégrer les solutions, assurer la gestion du projet, le rendre fonctionnel

Soit en résumé:

- Proposer des solutions intégrées et/ou adaptées pour:
  - garantir la sécurité des réseaux et des infrastructures déployées
  - assurer la connectivité sécurisée des accès mobiles
  - sécuriser la gestion des identités et les données critiques
  - garantir la confiance numérique pour les échanges
- Construire des architectures sécurisées pérennes et évolutives
- Garantir une maîtrise d'œuvre et une gestion de projet rigoureuses
- Déployer techniquement et humainement le système de sécurité

### 3) Contrôler et pérenniser: administration globale de la sécurité

Contrôler: Administrer, superviser, exploiter, entretenir, modifier les systèmes déployés (incorporation de nouvelles technologies)

Pérenniser: Maintenir, contrôler et assurer une veille active, mettre à jour, adapter la politique de sécurité.

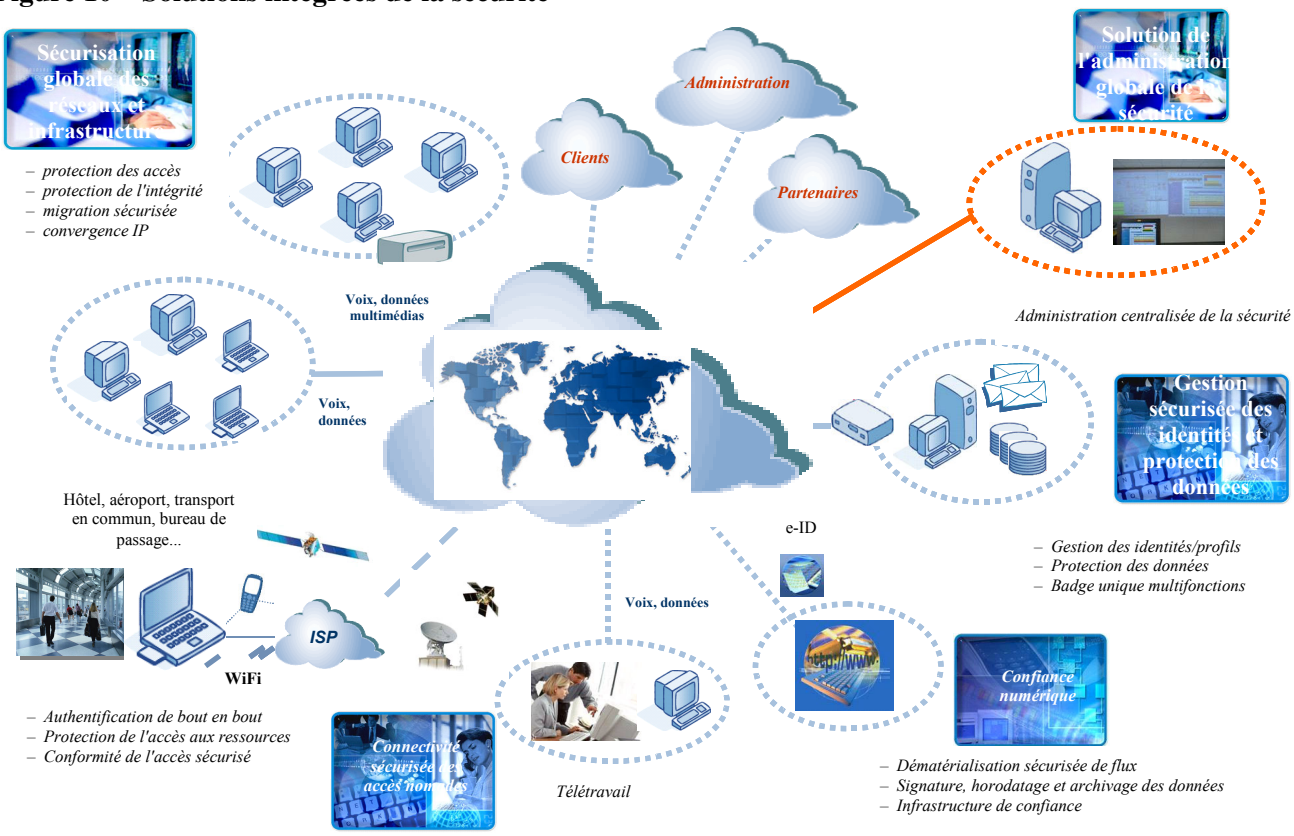
Soit en résumé, assistance/soutien et supervision active en permanence

- Téléadministration
  - Solutions de sécurité (COTS) et administration à distance sécurisée

- Pôle de lutte antivirale
  - Veille proactive et application de mesures préventives/réactives
- Gestion de la sécurité des postes de travail fixes ou mobiles
  - Gestion des droits d'accès et contrôle de la conformité du niveau de sécurité
- Hébergement sécurisé
  - Structure et horodatage
  - Infrastructures de confiance (IGC)

La figure ci-après donne un aperçu non exhaustif des différents composants de solutions sécuritaires intégrées.

**Figure 10 – Solutions intégrées de la sécurité**




## 5 Aspects juridiques

Les rapides progrès des techniques de l'information ont des répercussions directes sur tous les secteurs de la société moderne. L'intégration des systèmes de télécommunication et d'information, en permettant le stockage et la transmission – quelle que soit la distance – de toutes sortes de données, ouvre un immense champ de possibilités nouvelles. Ces progrès ont été favorisés par l'apparition des réseaux informatiques et des autoroutes de l'information, notamment l'internet, grâce auxquels toute personne ou presque peut avoir accès à la totalité des services d'information électronique, où qu'elle se trouve sur la planète. En se connectant aux services de communication et d'information, les usagers créent une sorte d'espace commun, dit «cyberespace», qui sert à des fins légitimes, mais peut aussi donner lieu à des abus. Les infractions commises dans ce cyberespace le sont contre l'intégrité, la disponibilité et la confidentialité des systèmes informatiques et des réseaux de télécommunication, à moins qu'elles ne consistent en l'utilisation de ces

réseaux ou de leurs services dans le but de commettre des infractions classiques. Le caractère international des infractions en question – par exemple celles commises au moyen de l'internet – se heurte à la territorialité des institutions nationales de répression. De plus en plus souvent les délinquants se trouvent dans des lieux fort éloignés de ceux où leurs actes produisent leurs effets. Or, les lois internes ne sont généralement applicables qu'à un territoire donné. Aussi les solutions aux problèmes posés relèvent-elles du droit international, ce qui nécessite l'adoption d'instruments juridiques internationaux adéquats. Le droit pénal doit donc suivre le rythme de ces évolutions techniques, qui offrent des moyens extrêmement perfectionnés d'employer à mauvais escient les services du cyberespace et de porter ainsi atteinte à des intérêts légitimes. Etant donné que les réseaux informatiques ignorent les frontières, un effort international concerté s'impose pour faire face à de tels abus.

Par contre, certains secteurs de l'activité humaine cherchent à «sécuriser» les lieux publics des perturbations liées à l'usage des TIC.

Par exemple en France, une loi a été votée en juillet 2001 permettant le brouillage des communications mobiles dans les salles de spectacles, de cinéma et les prisons. Pour des raisons de sécurité, cette loi a été appliquée dès 2003 dans les prisons. En octobre 2004, le Ministre français des télécommunications a signé le décret autorisant les mêmes dispositifs pour les salles de spectacles et les cinémas.

Trois technologies sont possibles. Il y a en effet trois solutions pour bloquer les communications mobiles. La plus radicale est celle des appareils appelés «barbouilleurs»: ces émetteurs utilisent, en permanence, la même fréquence que les relais téléphoniques. La moins agressive repose sur des «répéteurs»; elle permet de passer un appel d'urgence depuis un portable, tout en interdisant l'arrivée d'appels dits entrants. Cette solution est celle qui doit être utilisée en principe par les cinémas et les salles de spectacle.

Entre ces deux extrêmes, il y a les brouilleurs proprement dits. Ces systèmes bloquent la communication entre un mobile et le relais de l'opérateur grâce à l'émission d'un signal parasite, quel que soit le sens de la communication, mais seulement lorsqu'un appel est détecté (ce dernier dispositif est celui qui équipe les prisons).

## 5.1 Lignes directrices établies par les Nations Unies et l'Organisation de coopération et de développement économiques (OCDE)

Dès 1994, l'ONU s'est intéressée à ce problème de cybercriminalité en publiant un Manuel sur la prévention et le contrôle liés à cette criminalité informatique. Ce manuel a été actualisé en 1997. Depuis, l'Assemblée générale des Nations Unies ainsi que l'OCDE ont adopté des lignes directrices sur la sécurité des systèmes d'information et de communication. Les principes sont les suivants:

1) Sensibilisation

   Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

2) Responsabilité

   Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

3) Réaction

   Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

4) Ethique

   Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

5) Démocratie

La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.

6) Evaluation des risques

Les parties prenantes doivent procéder à des évaluations des risques.

7) Conception et mise en œuvre de la sécurité

Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.

8) Gestion de la sécurité

Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

9) Réévaluation

Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

Puis l'OCDE a publié en août 2002 un Rapport intitulé «Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux de l'information: vers une culture de la sécurité». Les lignes directrices de 2002 concernent tous les acteurs de la société de l'information. Elles mettent en évidence le fait qu'il est nécessaire de mieux comprendre les problèmes de sécurité et même qu'il faut développer une «culture de la sécurité». En effet, la sécurité devrait être un sujet de préoccupation centrale lors du développement des systèmes et des réseaux. Il faut adopter de nouveaux modes de pensée et de comportement en matière d'utilisation des systèmes et réseaux d'information ainsi que dans le cadre des échanges qui y ont lieu. Ces lignes directrices offrent un fondement aux efforts visant à instaurer une culture de la sécurité dans l'ensemble de la société.

Lors du Forum mondial de l'OCDE sur la sécurité des systèmes d'information et des réseaux qui s'est tenu les 13 et 14 octobre 2003 à Oslo (Norvège), on a fait le bilan de la première année de l'application des lignes directrices de l'OCDE publiées en 2002.

En novembre 2003, l'OCDE a publié un rapport, intitulé «Lignes directrices sur la protection de la vie privée et les meilleures pratiques» qui regroupe tous les travaux réalisés en vue de disposer d'une politique efficace de protection de l'usager privé en ligne.

La crédibilité du commerce électronique dépend de la fiabilité des infrastructures et des services, de la sécurité et de la confidentialité des opérations, et de la protection des données à caractère personnel. Le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée favorise une approche mondiale et coordonnée dans l'élaboration des politiques visant à créer une culture de sécurité en ligne. Dans ce rapport est donné un ensemble d'approches de réglementations et d'autorégulations, notamment juridiques, techniques et éducationnelles, en fonction du contexte culturel et social de l'environnement. Ce rapport attire l'attention sur la nécessité d'une coopération étroite entre tous les acteurs dans le domaine. Il est structuré comme suit:

**Partie I**

Panorama des travaux menés par le Groupe de travail de l'OCDE sur la sécurité de l'information et la protection de la vie privée.

**Partie II**

Lignes directrices fondées sur les travaux décrits dans la Partie I.

**Partie III**

Cette partie du document contient tous les documents présentés dans la Partie I et notamment les documents intitulés comme suit:

- Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel.
- Déclaration ministérielle relative à la protection de la vie privée sur les réseaux.

Inventaire des instruments et des mécanismes de nature à contribuer à la mise en œuvre et au respect sur les réseaux mondiaux des lignes directrices de l'OCDE sur la protection de la vie privée. (http://www.oecd.org/dataoecd/12/54/2092454.pdf)

Le 1er décembre 2003, l'OCDE a ouvert un nouveau site web intitulé «Culture de la sécurité» consacré au «combat» des attaques contre la sécurité des réseaux et des systèmes de l'information (voir http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase)

NOTE 1 – Tous les documents susmentionnés de l'OCDE sont disponibles sur le site http://www.oecd.org/document/20/0,2340,en_2649_33703_15589524_1_1_1_1,00.html

NOTE 2 – La 26e Conférence internationale sur la protection de la confidentialité et des données personnelles s'est tenue du 14 au 16 septembre 2004 à Varsovie (Pologne).

NOTE 3 – Un groupe spécial antispam a été créé le 22 octobre 2004, regroupant les 30 Etats Membres de l'OCDE, le monde des affaires, la société civile et les organisations internationales, y compris l'UIT. Les travaux dureront 2 ans.

## 5.2 Conseil de l'Europe

Le Conseil de l'Europe s'est proposé de relever le défi dans la mesure du possible, en tenant compte de la nécessité de respecter les droits de l'homme dans la nouvelle société de l'information et en fixant les principes d'une coopération internationale, conformément aux instruments internationaux pertinents en matière pénale et aux arrangements fondés sur les législations uniformes ou réciproques, dans le but de procéder à des investigations, d'entamer des procédures en rapport avec les infractions pénales liées aux systèmes et aux données informatiques ou de recueillir les preuves sous forme électronique d'une infraction pénale. Ces travaux ont abouti à la signature d'une convention multinationale sur la cybercriminalité.

*Convention sur la cybercriminalité (Conseil de l'Europe)*

Le Comité européen pour les problèmes criminels a décidé en novembre 1996 de créer un comité d'experts. Les travaux de cette instance ont conduit à l'élaboration d'une «Convention sur la cybercriminalité», texte présenté pour signature à la Conférence internationale sur la cybercriminalité le 23 novembre 2001 à Budapest. Cette convention mondiale a été signée par la plupart des pays européens, y compris les pays de l'Europe de l'Est et de la CEI ainsi que d'autres Etats du monde: Etats-Unis d'Amérique, Japon, République sudafricaine, Canada.

Cette convention vise pour l'essentiel:

1) à harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matières de cybercriminalité;
2) à fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique;
3) à mettre en place un régime rapide et efficace de coopération internationale.

Les principaux sujets traités dans le cadre de cette convention sont les suivants:

- Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques:
  - accès illégal
  - interception illégale
  - atteinte à l'intégrité des données, du système

  - abus de dispositifs
- Infractions informatiques:
  - falsification informatique
  - fraude informatique
- Infractions se rapportant au contenu
- Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes
- Autres formes de responsabilité et de sanctions:
  - tentative et complicité
  - responsabilité des personnes morales
  - sanctions et mesures

La convention comporte en outre les chapitres suivants:

- droit de procédures (droit pénal matériel, droit procédural et compétence)
- coopération internationale:
  - principes généraux relatifs à la coopération internationale, à l'extradition, aux demandes d'entraide en l'absence d'accords internationaux applicables
  - dispositions spécifiques.

Le Conseil de l'Europe prend en compte que la mondialisation présente des risques pouvant conduire à l'exclusion et à l'accroissement des inégalités, très souvent sur une base raciale et éthique. Alors que les développements technologiques, économiques et commerciaux devraient rapprocher les peuples du monde entier, le racisme, la xénophobie et d'autres formes d'intolérance continuent d'exister dans nos sociétés.

En conséquence, le Conseil de l'Europe a adopté le 7 novembre 2002 un Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

Les textes des deux documents susmentionnés sont disponibles sur les sites:
<http://conventions.coe.int/Treaty/FR/Reports/Html/185.htm>et
<http://conventions.coe.int/Treaty/FR/Reports/Html/189.htm>.

## 5.3 Union européenne

A sa session à Lisbonne en juin 2000, le Conseil de l'Union européenne (UE) a adopté un plan d'action dénommé *e*Europe 2002 qui préconise principalement la connectivité à l'internet pour tous comme moyen de stimuler la croissance économique dans les Etats Membres.

Les principaux résultats obtenus en application de *e*Europe 2002 ont été:

- la pénétration de l'internet dans les foyers a doublé;
- le cadre des télécommunications a été mis en place;
- les prix de l'accès à l'internet ont chuté (http://europa.eu.int/eeurope).

Au vu des résultats de *e*Europe 2002 le «Barcelona European Council» a demandé à l'UE d'établir un nouveau plan: *e*Europe 2005. Les priorités de ce plan d'action sont au nombre de quatre:

- modernisation des services publics en ligne: administration en ligne, services d'apprentissage en ligne et services de santé en ligne;
- environnement dynamique du commerce électronique;
- accès à large bande à des prix concurrentiels;
- infrastructure sécurisée de l'information.

Pour la sécurité de l'information, l'UE a mis en œuvre une stratégie fondée sur la sécurité des réseaux de communications [Network Information Society COM (2001) 398 du 6.6.2001]. Cette stratégie a fait l'objet de la Résolution du 28 janvier 2002 (http://register.consillium.eu.int/pdf/en/01/st15/1512enI.pdf). Plus récemment la Commission a proposé de décider d'un cadre général sur les attaques contre les systèmes de l'information (http://europa.eu.int/comm/dgs/justice-home/index-en.htm), COM(2002)173 final du 19 avril 2002.

Les actions proposées sont les suivantes:

- **Equipe spéciale pour la sécurité (CTSF)**. A la fin de 2003, la CSTF devait être opérationnelle. En se fondant sur les propositions de la Commission européenne (CE), le Conseil et le Parlement devaient adopter dans les meilleurs délais les fondements juridiques compte tenu de la dimension «transpilier» des réseaux et de la sécurité de l'information. La CSTF devait devenir un centre de compétence sur les questions de sécurité, et les Etats Membres devaient développer avec la CE le concept d'un système européen d'alerte informatique.
- **Culture de la sécurité**. A la fin de 2005, une «culture de la sécurité», concernant tant le développement que l'implantation des produits de l'information et de la communication, doit être mise en œuvre (Rapport intermédiaire fin 2003).
- **Communications sécurisées entre les différents services publics**. A la fin de 2003, la Commission et les Etats Membres devaient examiner les possibilités d'établir un environnement de communication sécurisé pour l'échange d'informations gouvernementales classifiées.

### *e*Europe 2005

Le Conseil européen réuni à Barcelone en 2002 a invité la Commission à établir un plan d'action *e*Europe axé sur «la mise en place et [-----] l'utilisation généralisées dans l'Union, d'ici 2005, de réseaux à large bande, ainsi que le développement du protocole internet IPv6 [----], sur **la sécurité des réseaux et des informations** [----] et le commerce électronique».

Le paragraphe 3.1.3 du document de l'UE intitulé «*e*Europe 2005 – Une société de l'information pour tous» concerne l'infrastructure d'information sécurisée.

L'Union européenne a déjà mis sur pied une stratégie globale, fondée sur les communications, concernant la sécurité des réseaux[1], la cybercriminalité[2], et sur la directive actuelle[3] et future concernant la protection des données dans le cadre des communications électroniques. L'approche proposée a été approuvée et développée davantage par la résolution du Conseil du 28 janvier 2002[4] et par la récente proposition de décision-cadre du Conseil relative aux attaques visant les systèmes d'information[5] présentée par la Commission.

Les activités de recherche communautaire dans le domaine de la sécurité se poursuivront sous le sixième programme-cadre. Les priorités seront: des infrastructures de réseau et d'information fiables, avec une attention particulière aux technologies émergentes (par exemple, architectures sans fil, à large bande, intelligence ambiante); la mise en évidence des vulnérabilités et des interdépendances dans les infrastructures. La recherche communautaire devrait aussi soutenir la normalisation afin de susciter une plus large utilisation des normes ouvertes et des logiciels ouverts. Les activités de recherche devraient aussi tenir compte du «facteur humain» dans le domaine de la sécurité, par exemple dans les normes de sécurité de base, la convivialité des systèmes.

---

1 Sécurité des réseaux et de l'information: proposition pour une approche politique européenne, COM(2001) 298 du 6.6.2001.

2 Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité – *e*Europe 2002, COM(2000) 890 du 22.1.2001.

3 Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO L 24 du 30.1.1998).

4 Voir http://register.consilium.eu.int/pdf/fr/01/st15/15152en1.pdf

5 COM(2002) 173 final du 19.4.2002. Voir http://europa.eu.int/comm/dgs/justice_home/index_fr.htm

Les actions proposées pour remplir ce mandat sont:

1) Equipe spéciale pour la cybersécurité

   Le Conseil et le Parlement seront en mesure d'adopter la base juridique nécessaire dans les meilleurs délais, en prenant en considération la dimension «transpilier» de la sécurité des réseaux et de l'information. Les Etats Membres et le secteur privé devraient appuyer les activités de l'Equipe spéciale. Celle-ci devrait devenir un centre de compétence sur les questions de sécurité, par exemple pour mettre au point avec les Etats Membres le schéma d'un système européen d'alerte informatique, faciliter les discussions «transpilier» et améliorer la coopération transfrontalière.

2) Culture de la sécurité

   Une «culture de la sécurité» devrait être instaurée pour la fin de 2005 dans le domaine de la conception et de la mise en œuvre des produits d'information et de communication. Le secteur privé devrait élaborer des bonnes pratiques et des normes et promouvoir leur application cohérente. La Commission compte soutenir des projets et œuvrera à une meilleure sensibilisation de tous les utilisateurs aux risques pour la sécurité. Un rapport intermédiaire sur les progrès réalisés devait être publié à la fin de 2003 et une évaluation finale paraîtra à la fin de 2005.

3) Communications sécurisées entre les différents services publics

   Pour la fin de 2003, la Commission et les Etats Membres devaient étudier les possibilités d'établir un environnement de communication sécurisé pour l'échange d'informations classifiées du secteur public.

NOTE – En 2004, la Commission européenne a mis en place l'«European Network and Information Security Agency» (ENISA). L'ENISA est un Centre d'excellence européen pour la sécurité. Cette agence est le centre de «dialogue» entre les partenaires publics-industries privées devant permettre de définir au sein de l'UE les lignes directrices et les meilleures pratiques pour la sécurité.

## 5.4 Stratégie nationale pour la sécurité du cyberespace (Etats-Unis)

Des études commanditées par la Maison blanche sur la protection contre la perturbation malveillante du fonctionnement des systèmes informatiques et sur la protection des personnes, de l'économie et de la sécurité nationale des Etats-Unis, ont été suivies de rapports publiés en février 2003.

Cette stratégie nationale pour la sécurité du cyberespace fait partie de l'effort global de protection de la nation américaine. Elle contribue à la mise en œuvre de la Stratégie nationale pour la sécurité de la patrie et est complétée par une Stratégie nationale pour la protection physique des infrastructures essentielles et des ressources essentielles. Ce document a pour objet d'engager et d'habiliter les Américains à assurer la sécurité des sections du cyberespace qu'ils possèdent, exploitent ou contrôlent, ou avec lesquelles ils interagissent. Assurer la sécurité du cyberespace est un grand défi stratégique qui exige un effort coordonné et résolu de la part de notre société tout entière – le gouvernement fédéral, les pouvoirs publics et les pouvoirs locaux, le secteur privé et le peuple américain.

- Objectifs stratégiques

  Dans le sens de la Stratégie nationale pour la sécurité de la patrie (arrêtée le 25 novembre 2002 par le Département de la sécurité de l'Etat, DHS), la stratégie nationale pour la sécurité du cyberespace a pour objet de:

  – prévenir les cyberattaques contre les infrastructures essentielles des Etats-Unis;

  – réduire la vulnérabilité du pays aux cyberattaques; et

  – minimiser les dommages causés par les cyberattaques et les délais de remise en état.

Après un chapitre consacré aux menaces et aux risques qui pèsent sur le cyberespace, il est question de la politique nationale et des principes directeurs. La protection des cybersystèmes étant essentielle à l'ensemble des secteurs de l'économie, la mise au point et l'application de la directive du programme fédéral d'octobre 2001 a suivi les principes suivants:

1) Effort national

2) Protection de la sphère privée et des libertés civiles

3) Réglementation et forces du marché

4) Obligation redditionnelle et responsabilité

5) Besoin de souplesse

6) Planification pluriannuelle.

**Priorités essentielles pour la sécurité du cyberespace**

La Stratégie nationale pour la sécurité du cyberespace s'articule autour de cinq priorités nationales, à savoir:

I Système national de riposte pour la sécurité du cyberespace

II Programme national de réduction des menaces et des risques pour la sécurité du cyberespace

III Programme national de sensibilisation et de formation à la sécurité du cyberespace

IV Sécurisation du cyberespace du gouvernement

V Coopération nationale et internationale pour la sécurité du cyberespace.

La première priorité doit nous permettre d'améliorer notre riposte face aux cyberincidents et de réduire les dommages potentiels causés par ces derniers. Les deuxième, troisième et quatrième priorités visent à réduire les menaces et les risques de cyberattaques. La cinquième priorité vise à prévenir des cyberattaques qui pourraient porter préjudice aux ressources de la sécurité nationale et à améliorer la gestion de ces attaques et la riposte sur le plan international.

Pour chaque priorité nationale, des **actions et des recommandations** sont préconisées; elles sont résumées dans l'Appendice du rapport.

## 5.5 Mesures de sécurité prises par les éditeurs de logiciels

Des éditeurs de logiciels ont mis à disposition le «code source» de certains de leurs logiciels pour renforcer la sécurité en réponse à une demande des organisations gouvernementales ou publiques d'une «transparence» accrue.

a) Après avoir lancé Windows en 2001, Microsoft a décidé en septembre 2004 de rendre accessible le cœur des différents programmes constituant sa suite bureautique Office 2003 (traitement de texte Word, tableur Excel et messagerie Outlook). Ainsi, grâce à cette initiative, les organismes publics et de l'Etat pourraient mieux connaître les mécanismes de stockage des fichiers et procéder en parallèle à des dialogues et des échanges avec les ingénieurs de Microsoft: *les administrations devaient répondre à des obligations légales d'archivage à long terme*.

   En septembre 2004:

   - Une trentaine de pays dont la Chine, l'Australie et l'Espagne avaient déjà conclu un accord pour Windows; le Royaume-Uni était le premier pays à avoir conclu un accord lui permettant d'avoir accès au code source d'Office.
   - En France, une trentaine d'organisations (en majorité des établissements d'enseignement supérieur) ont conclu un accord avec Microsoft dans le cadre du programme de diffusion des codes sources de Windows et d'Office.

b) Des éditeurs de logiciels ont décidé, dès la mise sur le marché de leurs logiciels, d'assurer un accès libre et gratuit aux codes sources, par exemple Linux pour son système d'exploitation, ainsi que d'autres éditeurs dans d'autres domaines, tels que ceux des serveurs d'application, des portails ou des suites bureautiques.

# 6 Normes ISO

La norme ISO/CEI 15408 qui, depuis 1996, permet de certifier les niveaux de défense assurés par les dispositifs de sécurité des systèmes d'information est mieux connue sous son appellation «critères communs». Elle résulte de la fusion progressive des TCSEC (*Trusted Computer Systems Evaluation Criteria*) ou «Livre orange» avec les ITSEC (*Information Technology Security Evaluation Criteria*), eux-mêmes issus de la fusion de différents critères nationaux.

En décembre 2000, la norme britannique BS 7799-1 a été adoptée par l'ISO (*International Organization for Standardization*) sous la référence ISO/CEI 17799.

Dans la norme ISO/CEI 17799, on note que de nombreux systèmes d'information n'ont pas été conçus pour être sécurisés. La mise en œuvre de moyens techniques de protection a donc un impact limité et doit être complétée par une organisation et des procédures appropriées.

Dans cette norme est donc proposé un ensemble de règles et de recommandations décrivant les meilleures pratiques en matière de sécurité des informations, au sens large. Il ne s'agit pas de se restreindre aux seuls dispositifs informatiques, mais de prendre en compte l'information sous toutes ses formes, en tant que véritable patrimoine de l'organisme.

Ces règles s'articulent autour de dix thèmes:

1) **Politique de sécurité**. Il s'agit, dans ce chapitre, de décrire le document où est exposée la politique de sécurité de l'organisme, en termes de responsabilité, d'approbation, de révision et d'adaptation.

2) **Organisation de la sécurité**. Les règles de ce chapitre traitent du rôle des acteurs de la politique de sécurité et tout particulièrement du comité chargé de la stratégie de l'organisme dans ce domaine. Ce comité, émanation de la direction générale, intervient dans la définition et le suivi de la politique de sécurité, sa «cheville ouvrière» étant le RSSI (Responsable de la sécurité des systèmes d'information). Les aspects contractuels liés à la sécurisation de l'accès de tiers au système d'information sont également étudiés dans ce chapitre.

3) **Classification et contrôle des actifs**. L'objectif est de maintenir un niveau de protection, adapté à chaque actif du système d'information, en le répertoriant, en le classant et en le plaçant sous la responsabilité d'un «propriétaire» nommément désigné.

4) **Sécurité des ressources humaines**. Les règles dans ce chapitre visent à réduire le risque d'erreur, de vol, de fraude ou de mauvais usage des ressources informatiques, en favorisant l'information des utilisateurs sur les risques et les menaces qui pèsent sur les informations.

5) **Sécurité physique et sécurité de l'environnement**. L'objectif de ce chapitre est de signaler les accès non autorisés, les dommages et les interférences affectant les informations, dans les locaux de l'entreprise.

6) **Exploitation et réseaux**. Il s'agit dans ce chapitre de minimiser les risques de pannes et leur impact, en assurant une exploitation correcte et sûre des moyens de traitement et en garantissant l'intégrité et la disponibilité des informations, des traitements et des communications.

7) **Contrôle d'accès**. Les règles dans ce chapitre visent à gérer et contrôler les accès logiques aux informations, à assurer la protection des systèmes en réseau et à détecter les activités non autorisées.

8) **Développement et maintenance des systèmes**. Sur la base du principe qui consiste à inclure la sécurité dès la phase de rédaction du cahier des charges, il est proposé dans ce chapitre des règles visant à prévenir la perte, la modification ou la mauvaise utilisation des informations dans les systèmes d'exploitation et les logiciels d'application.

9) **Continuité de service**. L'objectif de ce chapitre est de développer la capacité de l'organisme à répondre rapidement à l'interruption de ses activités critiques en cas de pannes, d'incidents, de sinistres ou de catastrophes.

10) **Conformité**. Il s'agit de s'assurer du respect des lois et des réglementations, de la conformité des procédures en place, eu égard à la politique de sécurité, pour réaliser les objectifs décrits par la Direction générale. Il s'agit aussi de l'efficacité des dispositifs de traçabilité et de suivi des procédures en place, notamment les journaux d'activités, les audits et les enregistrements de transactions.

Si la norme ISO/CEI 17799 a permis de faire connaître la norme BS 7799-1, dont elle est la reproduction fidèle, la seconde partie de la norme portant la référence BS 7799-2 est moins connue, celle-ci n'ayant pas encore été proposée à l'ISO. Il s'agit pourtant d'un document particulièrement intéressant, dont la lecture est indispensable pour avoir une vision globale du mécanisme permettant de définir la stratégie d'un organisme en matière de gestion de la sécurité de l'information. Dans sa dernière version, datant de septembre 2002, la norme BS 7799-2 propose une harmonisation avec les normes ISO 9001:2000 (gestion et assurance de la qualité) et ISO 14001 (gestion environnementale), ainsi qu'avec les principes de l'OCDE (voir le paragraphe 4.1). Il s'agit donc d'un véritable référentiel de certification déjà largement utilisé dans de nombreux pays, dont la Grande-Bretagne, l'Australie, la Norvège, le Brésil et le Japon.

# 7 Sommet mondial sur la société de l'information (SMSI)

Sous l'égide de l'ONU et organisée par l'UIT la première phase du SMSI s'est tenue à Genève du 10 au 12 décembre 2003. Ce Sommet a réuni des chefs d'Etat, de gouvernement, des chefs de secrétariat des institutions spécialisées des Nations Unies, des représentants du secteur privé ainsi que des médias et de la société civile pour coordonner la mise en place harmonieuse de la société de l'information dans le monde. Au cours de cette réunion, on a examiné un document de travail contenant une liste de thèmes établie à titre de cadre de référence. Les thèmes sont les suivants:

1) Infrastructure de l'information et de la communication: financement et investissement, accessibilité économique, développement et durabilité.
2) Accès à l'information et au savoir.
3) Rôle des Etats, du secteur privé et de la société civile dans la promotion des TIC en faveur du développement.
4) Renforcement des capacités: développement des ressources humaines, éducation et formation.
5) Sécurité.
6) Création d'un environnement propice.
7) Promotion des applications orientées: développement des TIC pour tous, par exemple administration publique en ligne, cybercommerce, téléenseignement et cybersanté.
8) Diversité culturelle et linguistique, contenu local et développement des médias.
9) Moyens permettant de franchir les obstacles à la réalisation d'une société de l'information à dimension humaine.

Les résultats du SMSI ont été l'adoption le 12 décembre 2003 d'une **Déclaration de principes** et d'un **Plan d'action**.

Sont donnés ci-après les éléments pertinents des deux documents adoptés concernant la sécurisation du cyberespace.

## 7.1 Déclaration de principes

**Construire la société de l'information: un défi mondial pour le nouveau millénaire**

*A Notre conception commune de la société de l'information*

Nous, représentants des peuples du monde, réunis à Genève du 10 au 12 décembre 2003 pour la première phase du Sommet mondial sur la société de l'information, proclamons notre volonté et notre détermination

communes d'édifier une société de l'information à dimension humaine, inclusive et privilégiant le développement, une société de l'information, dans laquelle chacun ait la possibilité de créer, d'obtenir, d'utiliser et de partager l'information et le savoir et dans laquelle les individus, les communautés et les peuples puissent ainsi mettre en œuvre toutes leurs potentialités en favorisant leur développement durable et en améliorant leur qualité de vie, conformément aux buts et aux principes de la Charte des Nations Unies ainsi qu'en respectant pleinement et en mettant en œuvre la Déclaration universelle des droits de l'homme.

*B Une société de l'information pour tous: principes fondamentaux*

**5 Etablir la confiance et la sécurité dans l'utilisation des TIC**

35. Renforcer le climat de confiance, notamment grâce à la sécurité de l'information et à la sécurité des réseaux, aux procédures d'authentification et à la protection de la vie privée et du consommateur est un préalable au développement de la société de l'information et à l'établissement de la confiance parmi les utilisateurs des TIC. Une culture globale de la cybersécurité doit être encouragée, développée et mise en œuvre en coopération avec tous les partenaires et tous les organismes internationaux compétents. Ces efforts devraient être soutenus par une coopération internationale renforcée. Dans cette culture mondiale de la cybersécurité, il importe d'accroître la sécurité et d'assurer la protection des données et de la vie privée, tout en améliorant l'accès et les échanges commerciaux. Cette culture mondiale de la cybersécurité doit en outre tenir compte du niveau de développement socio-économique des pays et respecter les aspects de la société de l'information qui sont orientées vers le développement.

36. Tout en reconnaissant les principes d'un accès universel et non discriminatoire aux TIC pour toutes les nations, nous soutenons les activités menées par les Nations Unies pour empêcher que les TIC puissent être utilisées à des fins qui sont incompatibles avec les objectifs du maintien de la stabilité et de la sécurité internationales et risquent de nuire à l'intégrité des infrastructures nationales, au détriment de la sécurité des Etats. Il est nécessaire d'éviter que les ressources et les technologies de l'information soient utilisées à des fins criminelles ou terroristes, tout en respectant les droits de l'homme.

37. Le spam est un problème important et qui ne cesse de s'aggraver pour les utilisateurs, les réseaux et l'internet dans son ensemble. Les questions de spam et de la cybersécurité devraient être traitées aux niveaux national et international appropriés.

48. L'internet est devenu une ressource publique mondiale et sa gouvernance devrait être un point essentiel de l'ordre du jour de la société de l'information. La gestion internationale de l'internet devrait s'exercer de façon multilatérale, transparente et démocratique, avec la pleine participation des Etats, du secteur privé, de la société civile et des organisations internationales. Elle devrait assurer une répartition équitable des ressources, faciliter l'accès de tous et garantir le fonctionnement stable et sécurisé de l'internet, dans le respect du multilinguisme.

**7 Les applications TIC et leur apport dans tous les domaines**

51.h Elaborer un cadre pour le stockage et l'archivage en toute sécurité des documents et des informations sur support électronique.

51.i Les pouvoirs publics et les parties prenantes devraient promouvoir activement la formation des utilisateurs et les sensibiliser aux problèmes de la confidentialité en ligne et de la protection de la vie privée.

Inviter les parties prenantes à faire en sorte que les pratiques visant à faciliter le commerce électronique donnent également au consommateur le choix d'utiliser ou non des moyens de communication électroniques.

**C7 Les applications TIC et leur apport dans tous les domaines**

**15 Administration électronique**

a) Mettre en œuvre des stratégies d'administration électronique axées sur les applications, visant à innover et à promouvoir la transparence dans les processus administratifs et démocratiques, à en améliorer l'efficacité et à renforcer les relations avec les citoyens.

b) Elaborer, à tous les niveaux, des programmes et des services nationaux dans le domaine de l'administration électronique, adaptés aux besoins des citoyens et des entreprises, afin de parvenir à une répartition plus efficace des ressources et des biens publics.

**10 Les dimensions éthiques de la société de l'information**

58. L'utilisation des TIC et la création de contenus devrait respecter les droits de l'homme et les libertés fondamentales d'autrui, notamment la vie privée ainsi que la liberté d'opinion, de conscience et de religion, conformément aux instruments internationaux pertinents.

64. Les compétences fondamentales de l'Union internationale des télécommunications (UIT) dans le domaine des TIC – assistance pour réduire la fracture numérique, coopération internationale et régionale, gestion du spectre des fréquences radioélectriques, élaboration de normes et diffusion de l'information – sont déterminantes pour l'édification de la société de l'information.

## 7.2 Plan d'action

### A Introduction

2) La société de l'information est un concept évolutif et son stade de réalisation diffère d'un pays à l'autre, en fonction du niveau de développement. L'évolution de la technologie, entre autres, transforme rapidement les conditions dans lesquelles cette société prend corps. Le Plan d'action est donc un cadre évolutif destiné à promouvoir la société de l'information aux niveaux national, régional et international. La structure particulière du Sommet mondial sur la société de l'information (SMSI), qui comprend deux phases, offre la possibilité de tenir compte de cette évolution.

### B Objectifs, buts et cibles

5) Des cibles spécifiques correspondant à la société de l'information seront définies selon qu'il conviendra, à l'échelle nationale, dans le cadre des cyberstratégies nationales et conformément aux politiques de développement nationales, compte tenu des conditions propres aux pays considérés. Ces cibles pourront constituer d'utiles critères d'action et d'évaluation des progrès réalisés dans la concrétisation des objectifs généraux de la société de l'information.

### C Grandes orientations

**C1 Le rôle des gouvernements et de toutes les parties prenantes dans la promotion des TIC pour le développement**

8.1 La participation effective des gouvernements et de toutes les parties prenantes est cruciale pour le développement de la société de l'information et implique de leur part à tous collaboration et partenariat.

a) Tous les pays devraient encourager l'élaboration de cyberstratégies nationales, y compris en ce qui concerne le nécessaire renforcement des ressources humaines, d'ici à 2005, compte tenu des conditions propres à chaque pays.

**C5 Etablir la confiance et la sécurité dans l'utilisation des TIC**

**12 La confiance et la sécurité sont au nombre des principaux piliers de la société de l'information**

a) Promouvoir la coopération entre les gouvernements dans le cadre de l'Organisation des Nations Unies, ainsi qu'avec toutes les parties prenantes, dans le contexte d'autres tribunes appropriées en vue de renforcer la confiance des utilisateurs, d'améliorer la sécurité et de protéger l'intégrité des données et des réseaux; envisager les menaces existantes et potentielles qui pèsent sur les TIC; traiter d'autres questions liées à la sécurité de l'information et des réseaux.

b) En coopération avec le secteur privé, les pouvoirs publics devraient prévenir et détecter la cybercriminalité et l'utilisation abusive des TIC et y remédier: en élaborant des lignes directrices qui tiennent compte des efforts en cours dans ces domaines; en envisageant une législation qui autorise des investigations efficaces et des poursuites en cas d'utilisation illicite; en encourageant les efforts d'assistance mutuelle; en renforçant l'appui institutionnel sur le plan international afin de prévenir et de détecter de tels incidents et d'y remédier; et en encourageant l'éducation et la sensibilisation.

c) Les gouvernements, et les autres parties prenantes, devraient encourager activement les utilisateurs à se former et à se sensibiliser aux problèmes de la confidentialité en ligne et de la protection de la vie privée.

d) Prendre des mesures appropriées aux niveaux national et international en ce qui concerne le spam.

e) Encourager l'évaluation interne de la législation nationale en vue de surmonter les obstacles à l'utilisation efficace des documents et des transactions électroniques, y compris grâce aux moyens d'authentification électronique.

f) Renforcer le cadre de sécurité et de confiance en adoptant des initiatives complémentaires et synergiques dans les domaines de la sécurisation de l'utilisation des TIC, ainsi que des initiatives ou des lignes directrices relatives au droit à la confidentialité, à la protection des données et à la protection des consommateurs.

g) Echanger les meilleures pratiques dans le domaine de la sécurité de l'information et de la sécurité des réseaux d'information et encourager leur utilisation par toutes les parties concernées.

h) Inviter les pays intéressés à établir des centres de coordination pour la gestion et le traitement en temps réel des incidents, et à les relier en un réseau de coopération pour le partage des informations et des technologies relatives aux interventions après incident.

i) Encourager la poursuite de l'élaboration d'applications sûres et fiables pour faciliter les transactions en ligne.

j) Encourager les pays intéressés à contribuer activement aux activités en cours dans le cadre des Nations Unies pour renforcer la confiance et la sécurité en ce qui concerne l'utilisation des TIC.

**C6 Créer un environnement propice**

13) Afin de tirer le meilleur parti des avantages socio-économiques et environnementaux qu'offre la société de l'information, les pouvoirs publics doivent créer un cadre juridique, réglementaire et politique fiable, transparent et non discriminatoire. A cette fin, il faudrait agir comme suit:

e) Les pouvoirs publics devraient continuer d'actualiser leur législation sur la protection du consommateur, afin de tenir compte des nouveaux besoins de la société de l'information.

c) Appuyer, à l'échelle internationale, des programmes de coopération dans le domaine du cybergouvernement, afin d'améliorer la transparence, de préciser l'obligation de rendre des comptes et de renforcer l'efficacité à tous les niveaux administratifs.

**C11 Coopération internationale et régionale**

26) Une coopération internationale entre toutes les parties prenantes est essentielle pour la mise en œuvre du présent Plan d'action et doit être renforcée afin de promouvoir l'accès universel et de réduire la fracture numérique, notamment en mettant à disposition les moyens de cette mise en œuvre.

**D Pacte de solidarité numérique**

27) Le Pacte de solidarité numérique vise à instaurer les conditions propres de la mobilisation des ressources humaines, financières et technologiques nécessaires pour que tous les hommes et toutes les femmes participent à la société de l'information naissante. Une étroite coopération nationale, régionale et internationale entre toutes les parties prenantes à la mise en œuvre de ce programme est indispensable.

**E Suivi et évaluation**

28) Il y a lieu d'élaborer un système international réaliste de suivi et d'évaluation (à la fois qualitative et quantitative) utilisant des indicateurs statistiques comparables et les résultats des recherches, afin de suivre les progrès réalisés, par référence aux objectifs, buts et cibles du présent Plan d'action et compte tenu des conditions propres à chaque pays.

e) Concevoir et mettre en place un site web consacré aux meilleures pratiques et à des exemples de réussite, regroupant les contributions de toutes les parties prenantes, dans une présentation concise, accessible et percutante, conforme aux normes d'accessibilité au web reconnues au plan international. Ce site pourrait être mis à jour régulièrement et devenir un instrument permanent d'échange d'expérience.

**Tunis 2005: deuxième phase**

La deuxième phase du Sommet mondial, accueillie par le Gouvernement tunisien, aura lieu du 16 au 18 novembre 2005 à Tunis. Elle sera essentiellement consacrée à des thèmes portant sur le développement. Elle permettra de faire le point sur les progrès accomplis et d'adopter tout autre plan d'action jugé nécessaire.

En conclusion, parmi les grandes orientations du SMSI, on peut mentionner celles qui suivent:

**Etablir la confiance et la sécurité dans l'utilisation des TIC**

• Authentification • Etablissement de la confiance et la sécurité • Protection du consommateur • Lutte contre l'utilisation abusive des TIC • Lutte contre le spam • Cybercriminalité • Cybersécurité • Protection des données • Sécurité de l'information et sécurité des réseaux • Intégrité des réseaux • Sécurité des transactions en ligne • Protection de la vie privée • Gestion et traitement en temps réel des incidents • Applications sûres et fiables.

NOTE – Pour un complément d'informations, voir les sites web: www.itu.int/wsis.index-fr.html et www.un.org/milleniumgoals/, un site de l'ONU où sont indiqués les Objectifs de développement pour le Millénaire, correspondant à ceux du SMSI de Genève.

# 8 Travaux de l'UIT

## 8.1 Résolutions (sécurité) de l'AMNT-04

Lors de sa réunion au Brésil du 5 au 14 octobre 2004, l'AMNT (Assemblée mondiale de normalisation des télécommunications) a adopté et approuvé de nouvelles Résolutions concernant la sécurité. De telles solutions sont les premières à être adoptées par une assemblée de haut niveau de l'UIT après la Résolution 130 (Marrakech, 2002) de la Conférence de plénipotentiaires:

- **Résolution 50: Cybersécurité**

Reconnaissant l'activité et l'intérêt marqués pour l'élaboration de normes et de Recommandations sur la sécurité au sein de l'UIT et plus particulièrement dans la CE 17, l'AMNT a décidé,

1 que l'UIT-T doit évaluer les Recommandations existantes et les nouvelles Recommandations en cours d'élaboration, notamment les Recommandations concernant les protocoles de signalisation et de communication, quant à la robustesse de leur conception et aux risques d'une exploitation par des acteurs malveillants cherchant à intervenir de manière destructive dans leur déploiement dans l'infrastructure mondiale de l'information et de la communication;

2 que l'UIT-T, dans sa sphère d'action et d'influence, doit continuer à sensibiliser au besoin de défendre les systèmes d'information et de communication contre la menace de cyberattaques, et à promouvoir la coopération entre les entités appropriées afin de renforcer l'échange de renseignements techniques dans le domaine de la sécurité des réseaux d'information et de communication,

*décide en outre*

de transmettre au Groupe consultatif de la normalisation des télécommunications (GCNT) le rapport du Symposium sur la cybersécurité tenu le 4 octobre 2004 à Florianópolis, afin qu'il l'examine et lui donne la suite voulue,

*charge le Directeur du Bureau de la normalisation des télécommunications*

d'élaborer, en consultation avec le président du GCNT et les présidents des commissions d'études compétentes, un plan visant à procéder à l'évaluation ci-dessus des Recommandations pertinentes dans les meilleurs délais, compte tenu des ressources disponibles et des autres priorités, et de tenir régulièrement le GCNT informé des progrès accomplis,

*charge en outre le Directeur du Bureau de la normalisation des télécommunications*

1 de faire état, dans le rapport annuel au Conseil prévu par la Résolution 130 (Marrakech, 2002) de la Conférence de plénipotentiaires, des progrès accomplis dans les évaluations visées au *décide* ci-dessus;

2 de continuer de prendre les mesures appropriées pour sensibiliser au besoin de défendre les réseaux d'information et de communication contre la menace des cyberattaques, et de collaborer avec d'autres entités pertinentes dans le cadre de ces efforts;

3 d'assurer une liaison avec d'autres organismes travaillant dans ce domaine, par exemple l'Organisation internationale de normalisation (ISO) et le Groupe d'étude sur l'ingénierie Internet (IETF),

*invite, selon le cas, les Etats Membres, les Membres du Secteur et les Associés*

à participer activement à la mise en œuvre de la présente Résolution et des mesures connexes.

- **Résolution 51: Lutte contre le pollupostage**

L'Assemblée mondiale de normalisation des télécommunications (Florianópolis, 2004), à la suite des «*reconnaissant*» reprenant le SMSI:

a) les dispositions pertinentes des instruments fondamentaux de l'UIT;

b) que les mesures approuvées pour lutter contre le pollupostage relèvent de l'objectif 4 du plan stratégique de l'Union pour la période 2004-2007 (partie I, § 3) donné dans la Résolution 71 (Rev. Marrakech, 2002) de la Conférence de plénipotentiaires;

c) la Résolution 52 visant à lutter contre le pollupostage par des moyens techniques;

d) le rapport du président de la réunion thématique du SMSI organisée par l'UIT pour lutter contre le pollupostage, qui préconisait à cette fin l'adoption d'une approche globale, à savoir:

   i) une législation vigoureuse,

   ii) le développement de mesures techniques,

iii) l'établissement de partenariats industriels,

iv) l'éducation,

v) la coopération internationale,

*charge le Directeur du Bureau de la normalisation des télécommunications, en coopération avec les Directeurs des autres Bureaux et le Secrétaire général*

d'établir d'urgence un rapport à l'intention du Conseil sur les initiatives pertinentes prises par l'UIT et sur les autres initiatives internationales en vue de lutter contre le pollupostage et de proposer des mesures de suivi possibles pour examen par le Conseil,

*invite les Etats Membres et les Membres du Secteur*

à contribuer à ces travaux,

*invite en outre les Etats Membres*

à prendre des dispositions appropriées au sein de leur cadre juridique national pour veiller à ce que soient adoptées des mesures indiquées et efficaces de lutte contre le pollupostage.

- **Résolution 52: Lutte antispam par des moyens techniques**

Après les *considérant* a) à f)

*reconnaissant*

a) les dispositions pertinentes des instruments fondamentaux de l'UIT;

b) que le pollupostage pose des problèmes de sécurité pour les réseaux de télécommunication, et constitue notamment un véhicule pour les virus, vers informatiques, etc.;

c) que le pollupostage est un problème mondial qui nécessite une coopération internationale afin de trouver des solutions;

d) qu'il est urgent de traiter le problème du pollupostage,

*charge les commissions d'études compétentes*

en coopération avec le Groupe d'étude sur l'ingénierie Internet (IETF) et les autres groupes concernés, d'élaborer d'urgence des Recommandations techniques sur la lutte contre le pollupostage, y compris les définitions nécessaires, selon qu'il conviendra, et de rendre régulièrement compte au Groupe consultatif de la normalisation des télécommunications des progrès accomplis,

*charge le Directeur du Bureau de la normalisation des télécommunications*

d'apporter toute l'assistance nécessaire en vue d'accélérer les travaux et de communiquer au Conseil les résultats obtenus.

**En conclusion**, l'application de ces trois Résolutions incombera à la CE 17 (voir le paragraphe 8.2.2). En outre, le Directeur du TSB devra fournir à l'AMNT-08 un rapport sur l'application de ces trois Résolutions.

NOTE – Tous les documents cités ci-dessus peuvent être obtenus sur le site de l'UIT-T (AMNT-04).

## 8.2 Commissions d'études de l'UIT-T

### 8.2.1 Période d'études 2001-2004

Sont données ci-après les mesures prises par les Commissions d'études de l'UIT-T concernant la sécurité des réseaux d'information et de communication.

- La Commission d'études 2 de l'UIT-T élabore actuellement des projets de Recommandation sur les impératifs de sécurité pour les réseaux de télécommunication (E.408), l'organisation de la gestion des incidents et la prise en charge des incidents touchant à la sécurité (E.409 – soumis à approbation le 18 mai 2004 (Groupe de travail 2/2)).

- La Commission d'études 4 de l'UIT-T a élaboré un ensemble de Recommandations qui traitent des aspects de sécurité des réseaux de gestion des télécommunications (RGT): M.3010, *Principes des réseaux de gestion des télécommunications*; M.3210.1, *Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000*; M.3013, *Considérations relatives aux réseaux de gestion des télécommunications*; M.3016, *Aperçu général de la sécurité du RGT*; M.3210.1, *Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000*; M.3320, *Cadre général des prescriptions de gestion pour l'interface X du réseau de gestion des télécommunications*; M.3400, *Fonctions de gestion RGT*; Q.813, *Elément de service d'application des transformations de sécurité pour l'élément de service d'opérations distantes (STASE-ROSE)*; Q.815, *Spécification d'un module de sécurité pour la protection des messages complets*; Q.817, *Infrastructure des clés publiques des RGT – Certificats numériques et profils de listes d'annulation de certificats*. Des travaux sur la sécurité sont actuellement effectués dans le cadre des Questions 7, 9, 10 et 18/4.

- La Commission d'études 9 de l'UIT-T a élaboré la Recommandation UIT-T J.170, *Spécifications de la sécurité sur IPCablecom*, dans le cadre de son projet IPCablecom. Cette Recommandation traite des services de sécurité d'authentification, de contrôle d'accès, d'intégrité de la signalisation et du contenu du support physique, de confidentialité et de non-répudiation.

- La Commission d'études 11 de l'UIT-T élabore actuellement des protocoles de contrôle et de signalisation des réseaux, intégrant les impératifs de sécurité identifiés par les Commissions d'études pertinentes et d'autres organes. Des études connexes sont effectuées par le Groupe de travail 1/11 (Questions 1, 2, 3, 4 et 5/11), le Groupe de travail 2/11 (Question 6/11) et le Groupe de travail 3/11 (Question 11/11).

- La Commission d'études 13 de l'UIT-T examine les aspects sécurité des réseaux IP et des réseaux multiprotocoles. Ce domaine est traité dans le cadre des projets NGN 2004 et IP de l'UIT-T. A la dernière réunion de la Commission d'études 13 (29 octobre – 8 novembre 2002), il a été décidé d'ajouter une clause sur la sécurité pour tous les textes en cours d'élaboration ou à venir. On peut constater que la Recommandation UIT-T Y.110 définit certains aspects généraux de la sécurité pour l'infrastructure mondiale de l'information. Concernant la Question 1/13, on élabore actuellement une nouvelle Recommandation UIT-T Y.1271, *Cadres généraux applicables aux spécifications et aux capacités de réseau pour la prise en charge des télécommunications d'urgence*. La nouvelle Recommandation UIT-T Y.140.1, en cours d'élaboration, également dans le cadre de la Question 1/13, présente de l'intérêt parce qu'elle traite d'un certain nombre d'attributs de sécurité aux frontières d'interconnexion possibles entre opérateurs de réseaux et fournisseurs de services. La Recommandation UIT-T Y.140, *Infrastructure mondiale de l'information: cadre général des points de référence d'interconnexion*, donne les informations générales ayant servi à élaborer la Recommandation UIT-T Y.140.1.

- La contribution de la Commission d'études 15 de l'UIT-T aux activités de normalisation sur la sécurité traite de deux domaines: la fiabilité et la sécurité des communications.

- La Question 9/15 sur les équipements de transport et la protection/rétablissement du réseau traite de la commutation de protection SDH (Recommandation G.841, *Types et caractéristiques des architectures de protection des réseaux à hiérarchie numérique synchrone* et la Recommandation UIT-T G.842, *Interfonctionnement des architectures de protection des réseaux à hiérarchie numérique synchrone*) et de la commutation de protection OTN (projets de Recommandation UIT-T G.808.1 et UIT-T G.808.2, *Commutation de protection générique*, projets de Recommandation UIT-T G.873.1 et UIT-T G.873.2, *Protection OTN*). Les spécifications de rétablissement du réseau seront ajoutées aux Recommandations sur les équipements ou le rétablissement du réseau.

- La Question 15/15, *Caractéristiques et méthodes d'essai des fibres et câbles optiques, la Question 16/15, Caractéristiques des systèmes optiques dans les réseaux de transport de Terre, la Question 17/15, Caractéristiques des composants et sous-systèmes optiques* et la Question 18/15, *Caractéristiques des systèmes sous-marins en câbles optiques*, contiennent chacune un point traitant de la fiabilité. La Recommandation UIT-T G.911, *Paramètres et méthodes de calcul de la fiabilité et de la disponibilité des systèmes à fibres optiques*, traite aussi de ce sujet. Les Questions 15, 16, 17 et 18/15 prévoient aussi d'étudier les aspects de fiabilité et de disponibilité pour les câbles et les fibres optiques ainsi que pour les composants, sous-systèmes et systèmes optiques de Terre et sous-marins.

  Tous les travaux concernant la sécurité des communications sont effectués dans le cadre de la Question 14/15, *Gestion de réseau pour systèmes et équipements de transport*. Les Recommandations UIT-T G.784, *Gestion de la hiérarchie numérique synchrone*, et UIT-T G.874, *Aspects de gestion de l'élément de réseau optique de transport*, traitent des fonctions de gestion des dérangements, gestion de configuration, gestion de compte, gestion de performance et gestion de sécurité (FCAPS) des éléments de réseau SDH et OTN. Dans ces Recommandations, les aspects de gestion de la sécurité doivent faire l'objet d'un complément d'étude. La Recommandation UIT-T G.7712/Y.1703, *Architecture et spécification des réseaux de communication de données*, couvre les aspects de sécurité des réseaux de communication de gestion (MCN) et des réseaux de communication de signalisation (SCN).

- La Commission d'études 16 de l'UIT-T, dans le cadre de la Question G/16 (http://www.itu.int/ITU-T/studygroups/com16/sg16-qg.html), a élaboré et continue à améliorer plusieurs Recommandations permettant d'assurer la sécurité de différentes familles de protocoles et de systèmes de conférence audiovisuelle, comme les Recommandations UIT-T H.320 sur le RNIS, UIT-T H.310 sur le RNIS à large bande, UIT-T H.324 sur le RTPC et les réseaux mobiles de la troisième génération (3G) et UIT-T H.323 sur les réseaux en mode paquet (y compris la téléphonie sur IP). Les Recommandations UIT-T H.233, *Système de confidentialité pour les services audiovisuels,* et UIT-T H.234, *Système de gestion de clés de chiffrement et d'authentification pour les services audiovisuels* (pour les systèmes H.320), sont actuellement en vigueur. Les Recommandations de la série H.sets, *Sécurité pour les systèmes de télécommunication d'urgence* sont en cours d'élaboration et la version 3 de la Recommandation UIT-T H.235, *Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)* a été approuvée récemment. La Question I/16 ayant aussi été approuvée récemment, on a entrepris des études visant à permettre d'assurer la sécurité dans divers scénarios d'opérations de secours en cas d'urgence et de catastrophe (par exemple, prévention des vols de services, autorisation des utilisateurs, confidentialité) à l'aide des communications multimédias, en liaison avec la Question G/16, *Sécurité des systèmes et services multimédias*, et en collaboration avec d'autres Commissions d'études et d'autres organisations de normalisation.

- La Commission d'études 17 de l'UIT-T a été désignée Commission d'études directrice chargée de la sécurité des télécommunications. Les travaux pertinents y sont coordonnés par la Q.4/17, *Projet relatif à la sécurité des systèmes de communication*. Les informations relatives à ces travaux peuvent être consultées sur la page web de la Commission d'études 17 du site de l'UIT (http://www.itu.int/ITU-T/studygroups/com17/tel-security-fr.html).

- La Commission d'études 17 a élaboré un catalogue des Recommandations de l'UIT relatives à la sécurité des systèmes de communication et a préparé un recueil des définitions concernant la sécurité extraites des Recommandations approuvées par l'UIT-T – le catalogue et le recueil sont disponibles sur la page du site web de l'UIT réservée à la Commission d'études 17 (http://www.itu.int/ITU-T/studygroups/com17/cssecurity-fr.html). La Commission d'études 17 a aussi élaboré un compendium des définitions sur la sécurité approuvées par l'UIT-T; ce document ainsi que son addendum assurent une compréhension commune des termes de sécurité pour tous les groupes de travail, les commissions d'études de l'UIT-T (voir le paragraphe 8.7). Le groupe chargé de la Question 10/17, *Impératifs de sécurité, modèle et directives pour les systèmes et les services de communication*, met régulièrement à jour les recueils sur la sécurité des systèmes de communication et a élaboré une série de nouvelles Recommandations.

La Commission d'études 17 traite d'un certain nombre de Questions relatives à la sécurité, à savoir:

- Q.2/17 – Services d'annuaire, systèmes d'annuaire et certificats d'attributs et de clés publiques. Dans le cadre de cette Question, la Recommandation UIT-T X.509 bien connue, *L'annuaire: cadre général des certificats de clé publique et d'attribut,* est le fondement des infrastructures de clé publique (PKI) et des infrastructures de gestion de privilège (PMI); une version mise à jour devrait être approuvée en 2005.
- Q.4/17 – Projet relatif à la sécurité des systèmes de communication. Cette Question traite de la vision et de la coordination générales du travail lié à la sécurité.
- Q.5/17 – Architecture et cadre général de la sécurité. Les Recommandations de la série X.800 sont largement consacrées au thème de la sécurité. En 2003, une adjonction importante a été faite – la Recommandation UIT-T X.805: *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.
- Q.6/17 – Cybersécurité. Des études ont été entamées pour traiter des nombreuses questions liées à la sécurité dans le cyberespace.
- Q.7/17 – Gestion de la sécurité. La Recommandation UIT-T X.1051, *Systèmes de gestion de la sécurité de l'information – Prescriptions pour les télécommunications (ISMS-T)*, a été approuvée en 2004.
- Q.8/17 – Télébiométrie. La Recommandation UIT-T X.1081, *Le modèle télébiométrique multimodal – Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie*, a été approuvée en 2005. Un complément d'information est donné au paragraphe 8.4.
- Q.9/17 – Services de communication sécurisés. Deux Recommandations sur la sécurité des réseaux mobiles ont été approuvées en 2004: les Recommandations UIT-T X.1121, *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout,* et UIT-T X.1122, *Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clés publiques (PKI)*.

Les activités de normalisation de l'UIT-T sont gérées dans le cadre d'un nouveau projet de l'UIT-T sur la sécurité, qui a été approuvé à la réunion de la Commission d'études 17 tenue en novembre 2002.

De plus, afin de faire face à une croissance des activités sur la sécurité, la Commission d'études 17 a décidé en mars 2004 que pour la période d'études 2005-2008 la Question 10/17 serait divisée en 6 nouvelles questions de G à L/17.

NOTE – La Commission d'études spéciale sur les «IMT-2000 et les systèmes ultérieurs» a inclus la sécurité parmi les aspects fondamentaux de ses Recommandations de référence pour les membres de la famille des IMT-2000 (3G). Parmi les sujets traités: évaluation des menaces perçues et liste des impératifs de sécurité pour faire face à ces menaces, principes et objectifs de sécurité, architecture de sécurité bien définie (c'est-à-dire mécanismes et caractéristiques de sécurité), besoins en matière d'algorithmes cryptographiques, conditions d'interception légale et fonctions et architectures d'interception légale. Ces études sont effectuées dans le cadre de la Question 3/SSG.

### 8.2.2 Période d'études 2005-2008

Suite à la **Résolution 2 de l'AMNT-04**, les différentes Commissions d'études (CE) mises en place pour la période 2005-2008 sont les suivantes:

CE 2 **Aspects opérationnels de la fourniture des services, réseaux et qualité de fonctionnement,** Commission d'études directrice pour la définition des services, le numérotage et l'acheminement

CE 3 **Principes de tarification et de comptabilité et questions connexes de politique générale et d'économie des télécommunications**, Commission d'études pour les principes de tarification et de comptabilité et les opérations connexes de politique générale et d'économie des télécommunications

CE 4 **Gestion des télécommunications**, Commission d'études directrice pour la gestion des télécommunications

CE 5 **Protection contre les effets dus à l'environnement électromagnétique,** Commission d'études pour la protection contre les effets dus à l'environnement électromagnétique

CE 6 **Installations extérieures et installations intérieures connexes,** Commission d'études pour les installations extérieures et installations intérieures connexes; le titre pourrait aussi apparaître en plus de la fonction LS4

CE 9 **Réseaux en câble intégrés à large bande et transmission télévisuelle et sonore**, Commission d'études directrice pour les réseaux de télévision et câblés intégrés à large bande

CE 11 **Spécifications et protocoles de signalisation**, Commission d'études directrice pour la signalisation et les protocoles. Commission d'études directrice pour les réseaux intelligents

CE 12 **Qualité de fonctionnement et qualité de service**, Commission d'études directrice pour la qualité de service et de fonctionnement

CE 13 **Réseaux de prochaine génération – architecture, évolution et convergence**, Commission d'études directrice pour les réseaux NGN et les questions relatives aux satellites

CE 15 **Infrastructures des réseaux optiques et autres réseaux de transport**, Commission d'études directrice pour le transport dans le réseau d'accès. Commission d'études directrice pour les technologies optiques

CE 16 **Terminaux, systèmes et applications multimédias**, Commission d'études directrice pour les terminaux, systèmes et applications multimédias. Commission d'études directrice pour les applications ubiquitaires («tout en ligne», par exemple la télésanté et le commerce électronique)

CE 17 **Sécurité, langages et logiciels de télécommunication**, Commission d'études directrice pour la sécurité des télécommunications. Commission d'études directrice pour les langages et les techniques de description

CE 19 **Réseaux de télécommunication mobiles**, Commission d'études directrice pour les réseaux de télécommunication mobiles et la mobilité (Commission d'études provenant de la transformation de la CE spéciale sur les IMT-2000 de la période 2001-2004)

La nouvelle répartition des travaux au sein des Commissions d'études de l'UIT-T nous amène à formuler les observations suivantes:

L'internet relève aussi de la **Commission d'études 2** puisque celle-ci doit recommander des orientations en matière de planification et de dimensionnement de l'ingénierie du trafic en vue de la mise en place et de l'exploitation de tous les types de réseaux et des éléments de réseaux.

**Commission d'études 11**

La Commission d'études 11 doit élaborer des Recommandations sur les aspects fondamentaux de l'architecture et des protocoles de signalisation et de commande des réseaux, y compris la convergence vers les réseaux de prochaine génération, en collaboration et en coordination étroite avec les autres commissions d'études responsables des Questions relatives aux autres réseaux et aux réseaux NGN.

Des Recommandations devront être élaborées sur les Questions suivantes, compte tenu de la convergence entre réseaux fixe et mobile:

- architectures fonctionnelles de signalisation et de commande de réseau dans les environnements NGN émergents;
- spécifications et protocoles de commande et de signalisation d'application;
- spécifications et protocoles de commande et de signalisation de session;
- spécifications et protocoles de commande et de signalisation de support;
- spécifications et protocoles de commande et de signalisation de ressource;
- spécifications et protocoles de signalisation et de commande pour la prise en charge du rattachement aux environnements NGN.

La Commission d'études 11 sera appelée à prêter son concours à l'élaboration d'un Manuel sur la mise en place de réseaux en mode paquet.

Elle devra réutiliser, le cas échéant, les protocoles en cours d'élaboration par d'autres organisations de normalisation, de manière à utiliser au mieux les investissements consacrés à l'élaboration de normes.

La Commission d'études 11 devra s'attacher à apporter des améliorations aux Recommandations existantes sur les protocoles d'accès et de signalisation interréseaux de la commande BICC, de l'ATM, du RNIS à bande étroite et du RTPC, par exemple le Système de signalisation N$^{O}$ 7, les systèmes DSS 1 et DSS 2, etc. L'objectif est de satisfaire aux besoins commerciaux des organisations membres qui souhaitent offrir de nouvelles fonctionnalités et de nouveaux services en plus des réseaux fondés sur les Recommandations existantes.

La Commission d'études 11 est encouragée, chaque fois que possible, à tenir pour certaines activités des réunions colocalisées avec les Commissions d'études 13 et 19, comme le décideront les équipes de direction des Commissions d'études.

**Commission d'études 17**

Elle est responsable des études relatives à la sécurité, à l'application des communications entre systèmes ouverts, y compris le réseautage et l'annuaire, et aux langages techniques, à leurs méthodes d'utilisation et à d'autres questions connexes liées aux aspects logiciels des systèmes de télécommunication.

Dans le domaine de la sécurité, la Commission d'études 17 est responsable de l'élaboration des principales Recommandations sur la sécurité telles que l'architecture et les cadres liés à la sécurité. En outre, cette Commission d'études assure la coordination générale des travaux menés par l'UIT-T dans le domaine de la sécurité.

En ce qui concerne les communications entre systèmes ouverts, la Commission d'études 17 est responsable des Recommandations dans les domaines suivants:

- interconnexion des systèmes ouverts (OSI) (Recommandations des séries X.200, X.400, X.600, X.800, etc.);
- services et systèmes d'annuaire (Recommandations des séries F.500 et X.500);
- traitement réparti ouvert (ODP) (Recommandations de la série X.900).

Dans le domaine des langages, la Commission d'études 17 est responsable des études relatives aux techniques de modélisation, de spécification et de description. Ces travaux, qui portent sur différents langages (ASN.1, SDL, MSC, eODL, URN et TTCN), seront menés en fonction des besoins des Commissions d'études concernées (CE 4, 9, 11, 13, 15 et 16) et en collaboration avec elles.

S'agissant des aspects logiciels des systèmes de télécommunication, les travaux porteront essentiellement sur les aspects pour lesquels l'industrie juge utile d'appliquer des Recommandations de l'UIT-T, afin d'améliorer l'utilisation des technologies informatiques et des processus associés et de stimuler le marché de ces technologies.

Les travaux de la Commission d'études 17 seront synchronisés avec d'autres organisations de normalisation tels que le JTC 1 de l'ISO/CEI, l'IETF et l'ETSI. Les travaux pertinents effectués dans le cadre de forums et de consortiums, comme l'OMG, le TMF, le SDL Forum Society, le Consortium ASN.1, OASIS, etc., seront eux aussi pris en compte pour obtenir la plus grande synergie possible dans l'élaboration de nouvelles Recommandations.

**Commission d'études 19**

Cette Commission d'études est responsable au premier chef, au sein de l'UIT-T, de tous les aspects «réseau» de la mobilité et des réseaux de communication mobiles, y compris les systèmes IMT-2000 et les systèmes ultérieurs. Elle est chargée:

- des besoins en matière de capacité de service et de capacité de réseau et de l'architecture de réseau;
- de la gestion de la mobilité;

- de l'identification des systèmes IMT-2000 existants ou en évolution;
- de l'élaboration d'un Manuel sur les IMT-2000;
- de la convergence des réseaux IMT-2000 en évolution et des réseaux fixes en évolution;
- de la définition d'un scénario d'évolution concernant les aspects «réseau» et la mobilité entre les systèmes IMT-2000 existants et les systèmes postérieurs aux IMT-2000;
- du développement d'un schéma d'orientation général sur les aspects «réseau» et la mobilité des systèmes IMT-2000 spécifiés par l'UIT-T et des organismes extérieurs (organisations de normalisation, projets en partenariat, IETF et autres forums extérieurs compétents, etc.);
- de l'étude des besoins et des techniques en matière de gestion de la mobilité, en vue d'assurer la mobilité mondiale entre les systèmes IMT-2000 en évolution et les systèmes ultérieurs, spécifiés par des organismes extérieurs.

Les points ci-dessus supposent l'élaboration d'une architecture commune à long terme des réseaux IP, applicable aux réseaux de communication mobiles, y compris à la mobilité dans le cadre des réseaux de prochaine génération. De plus, compte tenu de l'évolution actuelle de l'infrastructure des réseaux, ces points comprennent les travaux d'interréseautage IP à court terme.

De plus, la Commission d'études 19 étudiera:

- l'harmonisation de différentes normes de la famille IMT-2000 au fur et à mesure de leur évolution au-delà de ces systèmes, notamment en ce qui concerne la gestion de la mobilité et la convergence avec les réseaux fixes en évolution, autant que possible en collaboration avec les organismes compétents;
- les aspects «réseau» de la convergence des réseaux fixes et hertziens et, à terme, le passage à des architectures de réseau compatibles et harmonisées, pour offrir des services de manière transparente aux utilisateurs, selon différentes modalités d'accès.

Pour aider les pays en développement à appliquer les technologies des systèmes IMT-2000 et les autres techniques hertziennes connexes, une concertation devra s'instaurer avec des représentants de l'UIT-D, afin de déterminer comment mener au mieux les activités appropriées conjointement avec ce Secteur.

La Commission d'études 19 devra établir des relations de coopération étroite avec des organisations de normalisation extérieures ainsi que les partenariats 3GPP et élaborer un programme complémentaire. Elle devra encourager, de manière anticipative, les communications avec ces organisations extérieures, afin que les spécifications sur les réseaux mobiles élaborées par ces dernières puissent être mentionnées comme références normatives dans les textes des Recommandations de l'UIT-T.

La Commission d'études 19 est encouragée, chaque fois que possible, à tenir pour certaines activités des réunions colocalisées avec les Commissions d'études 11 et 13, comme le décideront les équipes de direction des Commissions d'études.

NOTE – L'Annexe C de la Résolution 2 (Florianópolis, 2004) donne la liste des Recommandations relevant de la compétence de chaque CE et du GCNT pour la période d'études postérieure à 2004.

## 8.3 Large bande et sécurité de l'information (Rapport UIT)

La présente section est un bref résumé du Rapport UIT intitulé «Naissance du large bande» de septembre 2003 (www.itu.int).

L'explosion des multipostages abusifs, ou spam, des farces électroniques et des cyberattaques met en évidence la grande vulnérabilité des utilisateurs et souligne la nécessité pour eux de prendre des mesures pour se protéger. Toutes les connexions, qu'elles soient téléphoniques ou à large bande, peuvent être victimes de ces types de violation, mais il est indubitable qu'une connexion à large bande permanente est plus exposée; attaques et actes de piratage peuvent en effet se produire à tout moment, 24 heures sur 24, ce qui augmente fortement le risque par rapport à un ordinateur qui ne reste branché que pendant un temps limité. Heureusement, il existe de nombreux outils qui permettent de sécuriser les connexions à large bande et de les rendre ainsi attractives aux yeux des utilisateurs potentiels.

- Prise de conscience du risque

  La plupart des utilisateurs du large bande sont des particuliers qui ont peu conscience du risque. Si le large bande est réputé pour la grande facilité avec laquelle il permet d'accéder à l'information, il risque également de se faire la réputation d'être particulièrement vulnérable, en l'absence de précautions ou faute d'une information suffisante, au point que des utilisateurs potentiels pourraient hésiter à passer au large bande par peur du risque accru pour leurs données, personnelles ou commerciales.

  Les pouvoirs publics et les fournisseurs de services internet (ISP) peuvent prendre des mesures pour sensibiliser les utilisateurs du large bande et accroître la sécurité des systèmes, tandis que les auteurs des normes relatives à cette technologie ont en partie la responsabilité de garantir un degré de sécurité acceptable au niveau du réseau.

- Pare-feu: un gardien vigilant

  Le pare-feu (voir le paragraphe 2.4) est un bon moyen d'interdire à toute personne non autorisée d'accéder aux ressources personnelles conservées dans un ordinateur à accès à large bande. Il s'agit d'un logiciel, ou d'un équipement, qui fait obstacle à toute communication à destination ou en provenance de l'ordinateur (ou du réseau).

  Nombreux sont les fournisseurs de pare-feu qui proposent en libre accès des versions de leur logiciel que l'on peut télécharger sur le web, même si la configuration de ces produits présente souvent des difficultés pour les utilisateurs. Des fournisseurs de large bande ont pris l'initiative d'aider les utilisateurs dans le domaine de la sécurité en incorporant gratuitement des pare-feu aux progiciels qu'ils proposent pour les réseaux familiaux et, en collaborant avec des producteurs de pare-feu, à la normalisation des procédures d'installation.

  Des fabricants ont mis au point d'autres types d'outils pour combattre l'un des problèmes les plus fréquents qu'ont à affronter les utilisateurs du large bande. Ce problème se présente sous la forme de logiciels espions qui sont subrepticement introduits dans un ordinateur par l'intermédiaire d'un programme téléchargé sur l'internet. Des programmes de partage de fichiers ont été accusés d'introduire des applications logicielles espionnes lors de leur installation sur un ordinateur.

  Fort heureusement, il existe des programmes d'utilisation libre, qui permettent de procéder à la recherche des fichiers correspondants et de les éliminer, l'ordinateur étant alors déverminé.

- Chiffrement et cryptage

  Si un pare-feu aide à rejeter une communication suspecte, il existe un autre moyen, encore meilleur, de protéger des données sensibles, qui sont soit stockées dans un ordinateur, soit acheminées sur l'internet; il s'agit du chiffrement, ou cryptage (voir le paragraphe 2.8). Les connexions à large bande peuvent en effet utiliser diverses techniques de chiffrement pour que ces données restent dans le domaine privé et puissent être acheminées sur l'internet sans être piratées; par ailleurs, elles se prêtent tout à fait bien à l'acheminement de communications chiffrées, qui exigent normalement une largeur de bande de 10 à 20% supérieure à celle qui est nécessaire pour des informations non cryptées.

- Dispositions législatives et réglementaires

  La mise en œuvre des systèmes de sécurité améliorés et l'élaboration de dispositions législatives et réglementaires pertinentes revêtent une importance fondamentale pour le développement d'applications commerciales et publiques telles que l'administration électronique, la télésanté ou le cybercommerce. Pour pouvoir utiliser ces services en ligne, il faudrait que les utilisateurs aient la garantie que seules des personnes autorisées pourront accéder à leurs données et les manipuler, que leurs boîtes à lettres électroniques ne seront pas des déversoirs à spam (messages non sollicités diffusés massivement) ou que les informations données par certains services sont dignes de confiance.

- Sécurité pour les particuliers

  La sécurité est également une question importante pour les particuliers, qui ne bénéficient généralement pas des contrôles et de l'assistance technique que peuvent fournir les entreprises ou les administrations. Laisser son ordinateur connecté à l'internet 24 heures sur 24 peut être comparé à une fenêtre laissée

ouverte, par laquelle n'importe qui peut entrer. La sécurité est donc nécessaire à l'établissement de la confiance, pour que des technologies comme le large bande puissent être exploitées dans toutes leurs possibilités, ce qui contribuera à créer un environnement propice à la société mondiale de l'information.

## 8.4 Manuel UIT-T «Sécurité dans les télécommunications et les technologies de l'information»

### 8.4.1 Edition 2003 du Manuel

En décembre 2003, l'UIT-T a publié un Manuel, intitulé «Sécurité des télécommunications et technologies de l'information» donnant un panorama des travaux et des résultats des Recommandations de l'UIT-T en ce qui concerne la sécurité des télécommunications et une vue d'ensemble des nombreuses Recommandations émises par le Secteur de la normalisation de l'UIT afin de permettre aux différents acteurs de la société de l'information de sécuriser l'infrastructure des communications ainsi que les services associés.

Ce Manuel décrit les pratiques usuelles en matière de sécurité et indique comment appliquer les différents aspects sécuritaires prescrits par l'UIT-T (www.itu.int/ITU-T/ publications). Faisant suite à l'introduction, les différentes sections composant ce Manuel portent sur les principaux sujets suivants:

- Architecture fondamentale de sécurité et ses applications (Recommandation UIT-T X.805).
- Cadre d'implantation des mesures de sécurité dans un réseau de télécommunication.
- Mécanismes pour la sécurité des informations personnelles (Recommandation UIT-T X.509-PKI).
- Applications en deux parties:
  1) Applications usager final
     - Voix sur IP
     - Télécopie
     - Multimédia
  2) Applications réseau (qualité et intégrité des services)
     - Gestion des réseaux
     - Cybersanté

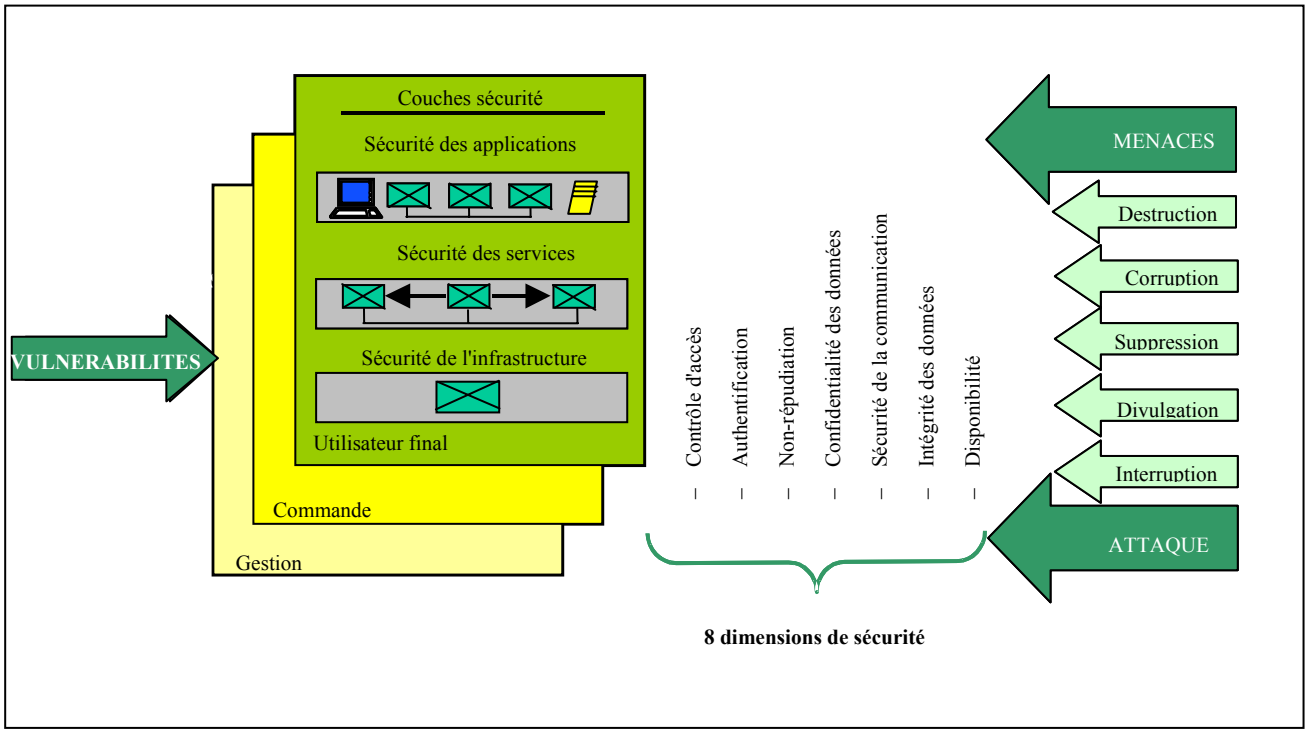
L'Annexe A fournit un glossaire de la terminologie et des acronymes utilisés en matière de sécurité, tandis que l'Annexe B contient un catalogue des Recommandations de l'UIT-T relatives à la sécurité.

### 8.4.2 Edition 2004 du Manuel

L'édition 2004 du Manuel (4 octobre 2004) fournit un panorama complet des nombreuses Recommandations élaborées par l'UIT-T, parfois en collaboration avec d'autres organismes internationaux de normalisation, en matière de sécurisation de l'infrastructure de communication ainsi que des services associés. Cette deuxième édition est complémentaire à celle parue fin 2003 et couvre d'autres aspects de la sécurité, en particulier ceux relatifs à la faisabilité et aux dommages que peuvent causer l'absence de sécurité dans les réseaux de communication. De plus, le manuel inclut les résultats des travaux réalisés depuis 2003 dans le cadre de l'élaboration de normes. Il est à noter que, pour prendre en compte les multiples facettes de la sécurité, ce Manuel définit un cadre de travail et une architecture permettant un langage commun permettant à tous d'en aborder tous les concepts.

Après l'introduction dans la section 1, dans la section 2 sont introduits les éléments et l'architecture fondamentale de la sécurité tels qu'ils sont définis dans les Recommandations de l'UIT-T. Huit dimensions de sécurité sont ainsi indiquées: respect de la vie privée, confidentialité des données, non-répudiation, contrôle d'accès, sécurité des communications et disponibilité. Ces principes généraux sont utilisés comme fondements pour l'élaboration de normes de sécurité par d'autres organismes (Recommandations de la série X.800).

**Figure 11 – Les éléments de sécurité basés sur la Recommandation UIT-T X.805**




Dans la section 3 sont introduits les concepts fondamentaux de la sécurité face aux menaces, aux vulnérabilités et aux risques et sont expliquées les relations entre ces concepts et les normes établies par les organismes de normalisation dans ce domaine.

La section 4 contient des informations qui permettent de développer des moyens assurant la sécurité dans les réseaux de télécommunication.

Cette section aborde en particulier les objectifs en matière de sécurité des réseaux de télécommunication ainsi que les services associés qui doivent être pris en compte pour remplir ces objectifs.

Dans la section 5 sont introduits les concepts très importants des «clés publiques» et les infrastructures autorisant une gestion optimisée. Ces infrastructures sont particulièrement importantes en tant que support des services d'autorisation et d'authentification.

L'UIT-T a mené de nombreux travaux sur la sécurité pour différents systèmes et services, qui ont abouti à l'élaboration de Recommandations. Un des principaux objectifs du Manuel est l'application de ces Recommandations. Ce sujet est abordé à la section 6. Y sont traitées la voix et les applications multimédias sur IP (H.323 et IPCablecom), la protection de la santé de l'utilisateur et la télécopie. Ces applications sont décrites en termes d'architecture de déploiement et de définition des protocoles, qui permettent de remplir les

besoins en matière de sécurité. En outre, afin de fournir des informations sur les modalités d'application des moyens de sécurité, on a énuméré les besoins pour la sécurité des infrastructures de réseaux et la gestion des services de réseau; des exemples sont donnés.

La section 7 aborde la disponibilité des différentes dimensions de sécurité et de l'infrastructure. Ces deux concepts sont les principaux sujets des travaux de l'UIT-T. Des informations sont données sur le calcul de disponibilité et les voies à suivre pour obtenir cette disponibilité pour un réseau de transport. Cette section inclut aussi des lignes directrices pour la sécurisation des réseaux de transports.

Dans la section 8 sont énoncées les lignes directrices récemment approuvées par l'UIT-T au sujet de l'incidence de l'organisation et des voies à suivre face aux incidents de sécurité.

Il est généralement admis que ces concepts sont de première importance pour l'établissement de la sécurité face aux menaces qui peuvent affecter l'infrastructure des systèmes de télécommunications et de l'information.

Enfin, le Manuel comporte en annexes:

- la liste des Recommandations de l'UIT-T en vigueur sur les aspects de la sécurité;
- la liste des acronymes et des définitions relatifs à la sécurité, utilisés dans le Manuel, dans les Recommandations UIT-T et dans celles d'autres services, telle que la base de données SANCHO UIT-T ou le compendium de l'UIT-T «Approved Sécurity Definitions» développé par la CE 17 de l'UIT-T;
- la liste des CE de l'UIT et des travaux en cours des CE (Questions) sur la sécurité.

En conclusion, l'UIT-T est l'un des acteurs les plus importants chargés de répondre aux besoins de sécurité en ce qui concerne non seulement les technologies fondées sur l'IP mais aussi les nombreux secteurs où les demandes de sécurité sont variées.

Le Manuel montre comment les solutions fondées sur les Recommandations de l'UIT-T répondent aux besoins de sécurité tant du point de vue général (cadre de travail et architecture) que de points de vue spécifiques (systèmes et applications). Ces solutions sont des solutions qui sont généralement adoptées et mises en œuvre par les opérateurs de services et de réseaux.

Ces rapports sont disponibles sur les sites:

http://www.itu.int/ITU-T/edh/files/security-manual.pdf et itu.int/indoc/itu.t/85097.pdf

## 8.5 Symposium UIT-T sur la cybersécurité (octobre 2004)

Sur le triple plan national, régional et international, il apparaît de plus en plus nécessaire d'élaborer, de mettre en œuvre et de promouvoir un ensemble de politiques, normes, directives techniques et procédures propres à rendre les systèmes et les réseaux TIC moins vulnérables aux diverses menaces et à protéger les informations mémorisées et échangées dans ces systèmes.

Dans le cadre de l'action qu'elle mène pour faire face à ces préoccupations, l'Union internationale des télécommunications a tenu le 4 octobre 2004, soit à la veille de l'ouverture de son Assemblée mondiale de normalisation des télécommunications (AMNT-04), à Florianópolis (Brésil) un Symposium sur la cybersécurité qui a rassemblé à un haut niveau des représentants d'un grand nombre d'administrations, d'équipes d'intervention rapide du secteur informatique (CERT, *computer emergency response teams*), d'opérateurs de réseau et de fabricants d'équipements venus faire le point de la situation dans le domaine de la sécurité et débattre des approches envisageables pour assurer la sécurité du cyberespace.

Ce Symposium d'une journée s'est articulé autour de quatre thèmes:

a) menaces sur la cybersécurité: les enjeux;

b) menaces sur la cybersécurité: expériences et réponses;

c) normes, politique, aspects réglementaires et juridiques;

d) les leçons de l'expérience et la voie à suivre – les types de bonnes pratiques, d'approches et d'initiatives qui seraient susceptibles de sécuriser davantage le cyberespace.

Les principales conclusions qui se sont dégagées du Symposium sur la cybersécurité peuvent être résumées comme suit:

1) **La sécurisation insuffisante des réseaux, en particulier de l'internet, pose un très sérieux problème, et ce problème s'aggrave**. De surcroît, le problème dépasse largement le monde des télécommunications, puisque l'informatique touche désormais la quasi-totalité des aspects de notre vie, dans laquelle les réseaux sont pour ainsi dire omniprésents. Et lorsque toutes les infrastructures seront des infrastructures IP, les problèmes seront encore plus grands. En l'absence d'une sécurité adéquate, il se pourrait que l'internet devienne inutilisable en quelques années, tout particulièrement comme base structurelle des relations économiques mondiales. Comme le téléphone mobile remplace l'ordinateur personnel dans un nombre croissant de ses fonctions, les réseaux mobiles sont de plus en plus souvent la cible d'attaques malveillantes.

2) **La sécurité doit être intégrée, et non pas rajoutée**. Elle doit être initialement prévue dans le système, et non pas organisée après coup. Il découle de ce principe fondamental que toutes les Recommandations, toutes les normes, doivent comporter une section consacrée aux architectures et protocoles de communication, et que cette section aura toujours son importance.

3) **Les opérateurs de réseau et les fournisseurs de services internet doivent faire ce que l'on attend d'eux et lutter contre les cyberagressions en suivant les meilleures pratiques et en restant vigilants**. Ils ne peuvent pas s'en remettre uniquement aux fabricants pour la prévention. Les opérateurs doivent établir des plans d'urgence, surveiller les activités sur le réseau et mettre en place des mécanismes d'alerte rapide. La sécurité des communications ne doit pas être un problème pour l'utilisateur: elle doit aller de soi.

4) **Il est nécessaire de sensibiliser et d'éduquer les parties prenantes (personnes, fabricants, opérateurs, entreprises et gouvernements).** Il faut accorder une attention particulière aux problèmes de sécurité avec lesquels les pays en développement sont aux prises. Aujourd'hui, la sécurité nous concerne nécessairement tous, avec l'importance que les ordinateurs et les réseaux ont désormais dans notre vie. Mais la sécurité est une chaîne, dont la résistance est égale à celle du maillon le plus faible. Il faut disposer d'un langage commun pour définir une vision d'ensemble constructive des différents aspects juridiques, techniques, politiques et normatifs de la cybersécurité.

5) **Les diverses parties prenantes doivent partager les informations dont elles disposent**. La constitution d'équipes de sécurité/d'intervention rapide (CSIRT/CERT) du secteur informatique doit être encouragée. Les manuels qui traitent de la sécurité (par exemple, le manuel intitulé «Security in Telecommunications and Information Technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications», octobre 2004 (110 pages), www.itu.int/itudoc/itu-t/85097.pdf) et les directives qui existent sur les «meilleures pratiques» constituent un bon point de départ, tout comme le code de pratique sur la gestion de la sécurité de l'information (ISO/IEC 17799:2000). Aujourd'hui, il importe au plus haut point de disposer d'une norme sur les systèmes de gestion de la sécurité de l'information (ISMS, *information security management system*) qui soit reconnue à l'échelle internationale, et ce travail est en cours (certains aspects relatifs aux télécommunications sont déjà couverts, par exemple, dans la Recommandation UIT-T X.1051 qui a été approuvée récemment).

6) **Il est nécessaire de renforcer la collaboration, la coopération et les partenariats internationaux dans le domaine des politiques de normalisation et des cadres juridiques qui ont trait à la cybersécurité.** Il existe déjà dans le monde diverses initiatives en la matière, qu'il serait avantageux de regrouper.

7) **Les pays en développement demandent à l'UIT d'assumer un rôle de leadership dans le domaine de la sécurité, de telle sorte qu'ils puissent participer davantage aux efforts qui permettront de sécuriser le cyberespace.**

8) **La normalisation est nécessairement une composante vitale de l'approche mondiale de la cybersécurité.** Dans l'élaboration des normes, la sécurité doit toujours figurer au premier plan.

   - Il faut accélérer l'élaboration de normes relatives à la sécurité, tout particulièrement pour les réseaux de prochaine génération (NGN). Il conviendrait que l'UIT montre la voie dans les efforts de normalisation relatifs aux NGN (à cet égard, signalons que l'un des sept groupes de travail du Groupe spécialisé de l'UIT sur les réseaux de prochaine génération est précisément chargé de la sécurité).

   - Les organismes et les forums de normalisation se multiplient, et le grand nombre de normes relatives à la cybersécurité déjà disponibles ou en cours d'élaboration se traduit par des problèmes de compatibilité. L'UIT pourrait centraliser les efforts en la matière.

   - Les opérateurs, qui s'étaient quelque peu désengagés des activités de normalisation, doivent de nouveau s'impliquer dans ces efforts, alors que le marché des télécommunications se rétablit après une crise sans précédent.

9) **Il est nécessaire de «sponsoriser» des activités concernant la cybersécurité dans les pays qui, à ce jour, n'ont ni stratégie ni programme en ce domaine.** Un certain nombre de vecteurs pourront être utilement exploités en un premier temps: groupes de discussion dans les milieux universitaires, associations de consommateurs, associations professionnelles. De telles activités initiales peu onéreuses peuvent en temps utile déboucher sur une collaboration et des partenariats aussi bien à l'échelle régionale qu'à l'échelle internationale, et l'on peut même envisager ensuite la mise en place d'un système de contre-attaque véritablement efficace.

10) **Les gouvernements doivent veiller à la mise en place d'un cadre juridique solide pour la cybersécurité.** Les lois et les politiques doivent être adéquates, et leur application effective.

11) **La sécurité est un objectif, et non pas une situation acquise**. Puisque les problèmes de sécurité procèdent presque toujours de questions d'organisation, il faut manifestement revoir sans cesse les politiques, les mesures et les procédures pour faire en sorte de les adapter aux nouveaux problèmes d'insécurité qui apparaissent dans le monde des ordinateurs, des réseaux et des équipements de communication.

Pour plus d'informations, on consultera le site www.itu.int/ITU-T/worksen/cybersecurity/

Une deuxième édition de ce symposium UIT-T sur la cybersécurité était prévue en mars 2005 à Moscou.

## 8.6 Télébiométrie

### 8.6.1 Introduction

La biométrie humaine (du grec ancien*: tele*: éloigné, à distance, *bio*: vivant et *metron*: mesure) est la mesure des paramètres qui concernent la physiologie humaine. Il s'agit de systèmes de données naturels.

Lorsque ses résultats servent à l'identification à distance d'une personne en son absence par le destinataire de la communication, la biométrie est appelée télébiométrie (du grec ancien: *tele: loin, distant*). Les signes uniques d'identifiants codés sous la forme qui représentent un individu et permettent d'éviter les vols et autres fraudes sont recueillis par des machines normalisées.

Plus difficilement réparables en cas d'endommagement, les systèmes de données qui font appel aux réseaux de télécommunication exigent une normalisation des dispositifs de collecte des enregistrements biométriques qui soit cohérente avec les systèmes normalisés de mesure.

### 8.6.2 Travaux à l'échelle mondiale

Le Bureau international des poids et mesures (chargé d'assurer la conformité des mesures avec le Système international des unités) a élaboré la norme ISO 31, [Comité technique 12 (ISO/TC12), «Quantités, unités, symboles et facteurs de conversion» – www.iso.ch] et la norme CEI 60027 [Comité technique 25 (CEI/TC25), «Quantités, unités et leurs symboles» – www.iec.ch], spécifiant une liste adoptée à l'échelle internationale des valeurs et des expressions de mesure, étayées par des accords dans tous les domaines des sciences. Le JTC 1/SC 37 de l'ISO/CEI «Biometrics» élabore de nouvelles normes sur les technologies de biométrie génétique pour le corps humain, devant assurer l'interfonctionnement et l'échange de données entre applications et systèmes.

La sécurité de l'utilisateur des systèmes d'identification biométrique pour les télécommunications nécessite l'introduction de manière ordonnée des champs d'informations au cours du processus d'élaboration de la norme de sécurité. Les études physiologiques et comportementales ont déjà été attribuées aux sous-comités afin que soient fournies les spécifications nécessaires aux équipementiers de l'industrie télébiométrique naissante pour que ceux-ci puissent mettre sur le marché des produits conformes aux connaissances scientifiques actuelles concernant la protection totale des paramètres naturels de la personne, et capables d'extraire et de crypter les données biométriques recueillies.

L'ISO et la CEI collaborent actuellement en vue de la parution d'une nouvelle série de normes ISO/CEI 80.000. La CEI travaille en outre sur une nouvelle proposition de travail (NWP 277) sur les unités physiologiques.

D'autres organisations internationales de normalisation se sont penchées sur la télébiométrie telles que:

– Le Biometrics Focus Group de l'ETSI (www.etsi.org)

– Le Groupe de travail d'ingénierie de l'Internet (IETF) (www.ietf.org)

– L'Organisation for the Advancement of Structured Information Standards (OASIS), (www.oasis.open.org).

### 8.6.3 Travaux de l'UIT-T

Au cours de la période d'études 2001-2004, le groupe chargé de la Question 10/17 «Impératifs de sécurité, modèle et directives pour les systèmes et les services de télécommunication» de la Commission d'études 17 de l'UIT-T a examiné de nombreux documents traitant de l'arrivée prochaine sur le marché de solutions de sécurité qui emploient du matériel (hardware) recueillant un ou des paramètres biométriques.

La «personal privacy sphere» (PPS) ou sphère privée individuelle de 2 mètres de diamètre (l'Homme Parfait de Leonardo Da Vinci) a été prise en compte. L'utilisateur de systèmes biométriques, lorsqu'il doit faire l'objet d'une identification et d'une authentification normalisées, doit pouvoir bénéficier d'une sécurité bien définie qui est assurée à tous les niveaux lors de l'entrée automatisée sur les réseaux de télécommunication des données biométriques uniques (et irremplaçables). L'identification et l'authentification volontaires, possibles en raison de la signature numérique sécurisée, fondée sur la physiologie de l'utilisateur, offrent en outre une série d'informations utilisables à des fins de sécurité et de tarification, appréciées par les opérateurs de réseaux. Un consensus au sujet du modèle-cadre télébiométrique multimodal a pu être obtenu grâce à la multifonctionnalité de ces taxinomies permettant d'ôter aux usagers toute phobie des techniques et de réassurer les opérateurs de réseau.

La Recommandation-cadre UIT-T X.1081 traite de la taxinomie multimodale des opérations télébiométriques. Cette Recommandation, publiée au début de 2004, après quatre années de travail, a ouvert la voie à de très nombreux produits destinés aux nouveaux terminaux sécurisés de téléphonie et de sémaphonie. Le modèle-cadre télébiométrique multimodal (TMMF) défini dans la Recommandation UIT-T X.1081 permet d'autre part d'arriver à un compromis pour l'usager des réseaux: le citoyen fournit librement à son fournisseur de services de télécommunication une garantie, fondée sur les sciences biométriques, en échange d'une garantie, fondée sur l'ensemble des connaissances actuelles, de la complète innocuité des terminaux télébiométriques sur les paramètres de la personne qui s'en sert. Les

fournisseurs de solutions télébiométriques offriront prochainement des appareils de téléphonie et de sémaphonie qui comportent un senseur biométrique et des capacités de codage suffisantes pour établir sur le terminal du destinataire de la télécommunication la véracité de l'identité de l'initiateur de cette communication, afin de garantir une politique de sécurité optimale. On a donné le nom de «optimal safety and security» (OS&S) (sûreté et sécurité optimales) à ce concept fondamental de modèle-cadre télébiométrique multimodal.

Les équipementiers pourront donc mieux s'armer contre les imposteurs en adoptant cette norme internationale: les spécifications relatives aux caractéristiques des terminaux télébiométriques de télécommunication ont été étoffées. Les solutions technologiques permettront d'éviter le recours au règlement juridique en cas de plaintes non fondées sur le plan scientifique et plus encore de distinguer les problèmes réels de sécurité des menaces imaginaires relevant de la psychologie ou de phobies technologiques.

En mars 2004, la Question 10/17 a été subdivisée pour la période de travail 2005-2008 en 6 nouvelles Questions, parmi lesquelles la Question K/17 ayant pour sujet la «télébiométrie sécurisée».

Différentes solutions technologiques appropriées ont été envisagées lors de la spécification des senseurs télébiométriques. Dans le cadre de la Question 8/17, les mesures ci-après ont été considérées comme nécessaires:

1) Pour authentifier l'identité des citoyens, il faut recueillir les données biométriques au moyen de senseurs sûrs et fiables. La Recommandation UIT-T X.1081, qui définit le modèle-cadre télébiométrique multimodal, doit être complétée par une base de données télébiométriques pour une sécurité et une sûreté optimales.

2) La transmission et le stockage sûrs de ces données personnelles biométriques confidentielles ne sont pas sans risque. La question est traitée dans une Recommandation, en cours d'élaboration, sur la procédure de protection télébiométrique.

3) Pour résoudre ce problème de sécurité et de confidentialité, un mécanisme de type X.509 est proposé dans une Recommandation, en cours d'élaboration, consacrée aux mécanismes du système télébiométrique employant les PKI.

4) Il convient d'étudier les senseurs biométriques et le matériel de traitement permettant de comparer les données biométriques stockées à celles qui ont été mesurées lors de la procédure d'authentification. Il faut effectuer un classement hiérarchique des appareils de sécurité afin de répondre aux besoins des pays en développement. Cela suppose la définition d'un support matériel inviolable.

**Conclusion**

Le modèle-cadre télébiométrique multimodal permet de s'assurer de manière optimale de l'identité d'un usager des réseaux de télécommunication, tout en respectant les libertés élémentaires liées à la protection des données uniques conférées par la nature – et souvent irremplaçables – de l'usager.

De plus, l'introduction sur les réseaux de télécommunication d'un agent intelligent autorisant d'être télébiométriquement identifié et authentifié ouvre la voie à un partage des responsabilités entre l'opérateur qui sécurise les données (codage) et l'usager qui sécurise son terminal au moyen de la fonction télébiométrique.

### 8.6.4 Etude de cas: Etats-Unis

Afin de mieux se protéger, les Etats-Unis ont mis en place des contrôles biométriques à l'entrée de leur territoire. C'est ainsi qu'en septembre 2004, 115 aéroports internationaux, 14 zones portuaires et une cinquantaine de points de passage frontaliers ont été dotés de systèmes qui prennent systématiquement la photo et les empreintes digitales des voyageurs internationaux; environ 40 millions de passagers chaque année devront se soumettre à cette contrainte biométrique lorsqu'ils présenteront leur passeport à l'officier d'immigration.

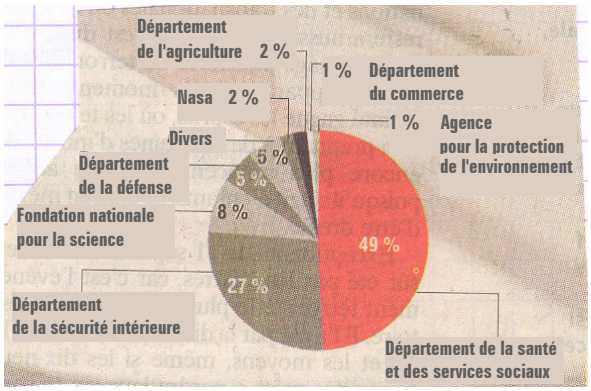
Ces données, aussitôt numérisées, sont centralisées. Elles sont comparées à la base de données *computer assisted passenger prescreening system* (CAPPS), qui détermine si un passager doit être considéré comme suspect par les officiers d'immigration.

La base est aussi alimentée par les données fournies par certaines compagnies d'aviation américaines et les deux principaux systèmes de réservation aérienne Sabre et Galileo, qui ont accepté de transmettre une partie de leurs informations à la *Transportation Security Administration* (TSA), qui gère le système. D'autres ont refusé et des négociations serrées ont lieu actuellement entre toutes les parties concernées pour déterminer la nature exacte des informations qui devront être fournies obligatoirement par les transporteurs.

Le système de contrôle ralentit fortement les formalités d'entrée dans le pays. Pour anticiper un engorgement qui deviendrait ingérable, les autorités américaines viennent de lancer un programme pilote baptisé «Registered Traveller». Il concerne aujourd'hui 10 000 passagers (octobre 2004), tous grands voyageurs, qui peuvent passer pratiquement sans s'arrêter lors du contrôle des frontières, le plus souvent des cadres voyageant à l'étranger pour des motifs professionnels. Porteurs d'une carte à puce qui contient leurs données biométriques, ils n'ont qu'à s'arrêter quelques secondes devant une caméra qui compare la photo prise à ces données.

Avec un tel dispositif hautement informatisé – qui implique l'interconnexion de bases de données gérées par des organismes publics et privés – l'administration espère à la fois augmenter la sécurité et accélérer le processus de passage à l'immigration. «Les informations contenues dans Registered Traveler ne seront pas utilisées à d'autres fins que celles liées à la sécurité.»

**Figure 12 – Financement de la recherche sur la sécurité aux Etats-Unis**




(Pourcentages pour 2004. Total: 3,4 milliards USD)
*Source: AAAS/*Les Echos

## 8.7 Recueil sur la sécurité

Dans le cadre de la Question 4/17, «Projet relatif à la sécurité des systèmes de communication», la Commission d'études 17 a établi et met régulièrement à jour un recueil sur la sécurité des systèmes de communication. L'ouvrage se compose des trois parties suivantes:

– un catalogue des Recommandations de l'UIT-T approuvées ayant trait à la sécurité;
– un extrait des définitions relatives à la sécurité tirées de Recommandations approuvées de l'UIT-T et d'autres normes,
– une liste des Questions de l'UIT-T liées à la sécurité.

Le recueil peut être consulté sur la page web de la Commission d'études 17 du site de l'UIT (http://www.itu.int/ITU-T/studygroups/com17/tel-security.html). Le recueil de définitions relatives à la sécurité permet de comprendre globalement les termes relatifs à la sécurité employés par les différentes Commissions d'études de l'UIT-T.

# 9 Centre de contrôle et d'acquisition des données transmises, y compris l'IP

## 9.1 Introduction

La présente section décrit un système de contrôle des transmissions de données, y compris l'IP, nommé Centre de contrôle et d'acquisition des données transmises (CCATD), destiné au régulateur national des télé-communications pour qu'il puisse assurer la sécurité et le contrôle des communications dans la mesure de ses compétences nationales face à une utilisation frauduleuse ou abusive. Ce système est conforme aux Recommandations de l'UIT ainsi qu'à la section 5 du Manuel de l'UIT-R «Contrôle technique du spectre radioélectrique».

Le CCATD permet le traitement des données interceptées sur les différents réseaux de télécommunication, qu'elles soient non codées, codées, comprimées ou protégées. Il reconnaît les différents formats de données transmises (les types de modem, les niveaux de protocole IP), assure une démodulation et un décodage fiable des formats connus et reconnus et en effectue une conversion claire et compréhensible, en particulier pour les protocoles utilisés sur le réseau internet.

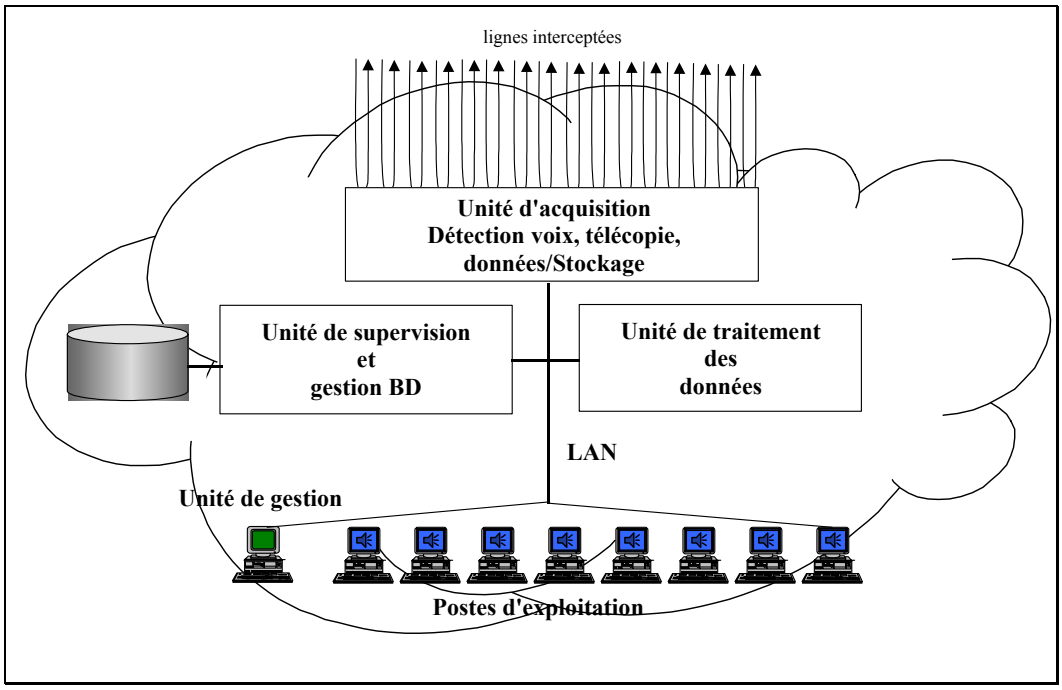
Le CCATD, système ouvert, flexible et convivial, comporte les trois unités fonctionnelles principales suivantes (voir la Figure 13):

- Unité d'acquisition: unité qui intercepte les communications acheminées vers le CCATD en provenance des opérateurs de télécommunication (téléphonie fixe, téléphonie mobile, câble ou voie à haut débit), extrait le contenu et convertit les informations de signalisation des communications dans des formats donnés et classe les informations non codées (voix, télécopie, données) et codées.

- Unité de supervision: unité qui supervise les interceptions de routage vers les centres extérieurs au CCATD, et le système (état des modules d'acquisition, journalisation des évènements, administration des profils utilisateur, statistiques sur le système, etc.).

- Unité de traitement: unité qui fournit l'accès au contenu par démodulation et décodage, et formatage des fichiers produits.

**Figure 13 – Schéma de principe du centre de contrôle et d'acquisition des données transmises**




Les capacités de «traitement» des interceptions (démodulation, «remontée» des protocoles internet, etc.) sont intégrées sous forme de modules logiciels à travers le serveur de traitement. Les capacités du système, en termes de puissance de calcul (ajout de serveurs physiques, répartition des traitements) et de cibles traitées (ajout d'un nouveau traitement dans le serveur), peuvent ainsi être aisément augmentées.

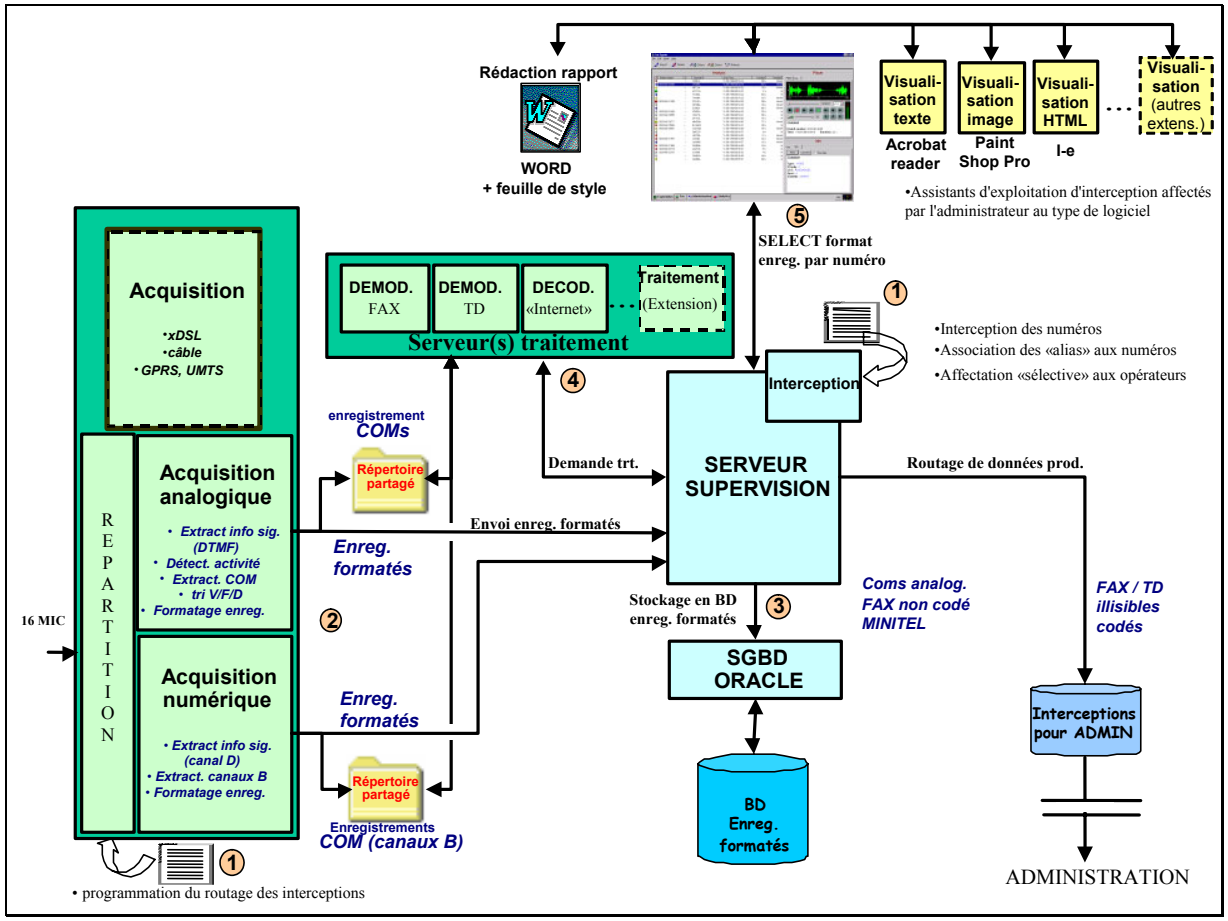
## 9.2 Description et architecture du CCATD

Les principales fonctions du CCATD sont les suivantes:

- acquisition des communications sur des liaisons spécifiques;
- extraction des informations de signalisation, converties dans un enregistrement mis en forme;
- détection du type de transmission (voix/télécopie/données);
- démodulation des principales normes de transmission de données;
- décodage des protocoles et formats des principales normes de transmission de données;
- détection de la manière de transmission (codée/non codée);
- enregistrements à l'échelle locale;
- routage des transmissions codées vers une entité extérieure.

L'architecture du CCATD est représentée ci-dessous dans la Figure 14.

**Figure 14 – Architecture du système CCATD**




(1) Le cœur du système est le serveur de supervision, qui gère tous les échanges entre les différentes composantes internes du système (acquisition => traitement => exploitation) et avec les composantes extérieures Le démarrage opérationnel du système passe par une première étape de configuration des interceptions, effectuée par le chef du CCATD. Celui-ci dispose de privilèges d'administration lui permettant d'entrer au niveau du serveur de supervision, pour chaque canal d'acquisition, les numéros à intercepter et les alias associés. Il programme également la répartition des communications interceptées transmises par l'opérateur de télécommunication et les regroupe dans un canal d'acquisition selon les moyens d'acquisition.

Pour terminer cette étape de configuration, le chef du CCATD regroupe les numéros à intercepter en fonction des différents utilisateurs et de leur utilisation.

subject to interception depending on the various users and purposes in question.

(2) Au niveau de l'acquisition, le principe de fonctionnement exige que l'acquisition soit adaptée au moyen de communication et utilise les mécanismes de stockage appropriés. Chaque module d'acquisition est chargé de trier en amont les interceptions à l'aide d'une analyse de la signalisation et du contenu des communications (tri par numéro et détection voix/données). Il stocke le contenu des communications et produit un enregistrement cliché d'interception à destination du serveur de supervision, contenant les informations nécessaires au tri et à la localisation de la communication correspondante.

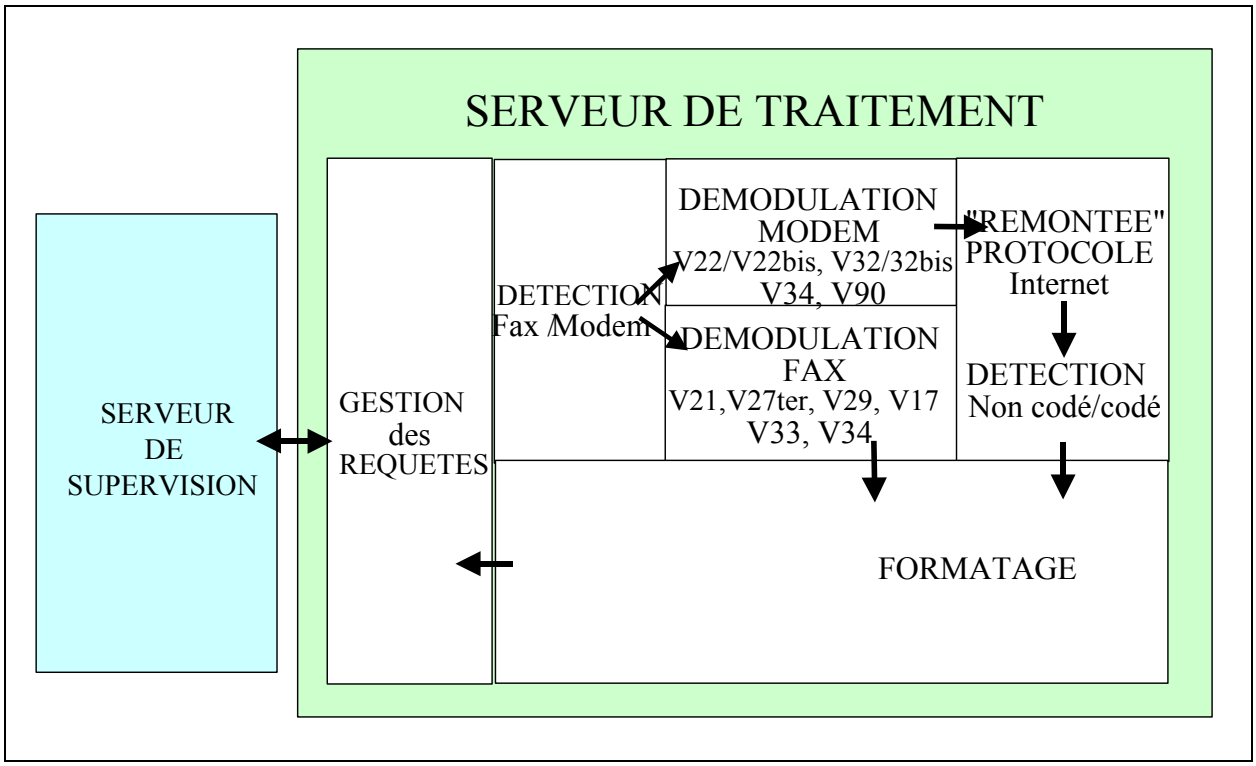
③ L'enregistrement est placé dans la base de données des interceptions par le serveur de supervision. Si l'enregistrement nécessite un traitement avant que l'on puisse accéder au contenu (cas des transmissions de données), le module de supervision invoque automatiquement le serveur de traitement en lui fournissant toutes les informations utiles de l'enregistrement (type de communication, localisation de la communication, etc.).

④ Le serveur de traitement récupère les données brutes numérisées de la communication au niveau du module d'acquisition spécial, ordonne les traitements et renvoie les données produites au niveau du module d'acquisition. Il avertit le serveur de supervision de l'état du traitement.

Le serveur de traitement (voir la Figure 15) permet les traitements suivants:

- démodulation,
- décodage des protocoles et formats associés;
- détection des transmissions de données codées.

**Figure 15 – Fonctions du module de traitement du CCATD**




⑤ L'opérateur peut alors utiliser les fichiers traités en fonction de la liste des interceptions auxquelles il a accès.

Dans cette architecture répartie, chaque module d'acquisition (actuel et futur) dispose de ses propres moyens de stockage. La répartition de la charge à stocker entre les modules d'acquisition permet au serveur de supervision de ne pas saturer ses moyens de communications et ses capacités de stockage en cas d'accroissement des types et du nombre de modules d'acquisition.

Ce choix d'architecture répartie permet d'optimiser l'utilisation des ressources informatiques et réseau et de faciliter l'évolution du système.

L'architecture du CCATD favorise les évolutions en termes de capacités et de performance, de par sa conception:

- utilisation systématique des interfaces et formats normalisés (par exemple, page HTML «.htm», fichier son «.wav», etc.);
- emploi de langages normalisés et d'une conception orientée objet;
- conservation des capacités d'extension technologique;
- réalisation des traitements sur PC pour faciliter les évolutions et mises à jour (atelier de programmation de haut niveau, compétences informatiques étendues) et emploi de postes et d'équipements informatiques normalisés.

Ces choix d'architecture permettent une intégration aisée des développements ultérieurs, sans devoir recourir systématiquement au fournisseur du système.

Ce choix d'architecture répartie permet d'optimiser l'utilisation des ressources informatiques et réseau et de faciliter l'évolution du système.

# 10 Etudes de cas

## 10.1 UIT

Dans le cadre des activités de l'UIT-T, un atelier s'est tenu en mai 2002 en Corée ayant pour objet la sécurité des réseaux et portant principalement sur les aspects techniques qui permettent la sécurisation des réseaux de communication. Il a été introduit la notion d'«infrastructure critique» (*critical infrastructure*). Les infrastructures de réseaux au sens de l'UIT sont des réseaux publics ou privés capables de transporter de grandes quantités de données au-delà des frontières nationales. Les «réseaux critiques» sont ceux qui transportent des informations relevant de la sécurité nationale ou financières à très fortes valeurs ajoutées. Des études de cas ont été présentées sur la sécurité des réseaux et sur leurs réglementations pour les pays suivants: Brésil, Canada, Corée et Pays-Bas.

Toutes les informations sont présentées sur le site: http://www.itu.int/org/spu/ni/ipdc/index.html.

L'UIT-T a envisagé de rééditer un atelier du même type en octobre 2005.

## 10.2 Sécurisation des réseaux dans le monde

Le Gouvernement français a publié un document (www.cfce.fr/ntic) à la fin de 2002, qui dresse un état des lieux de la sécurisation des systèmes et réseaux de communication au niveau mondial; un résumé de cette étude est donné ci-après:

**Afrique du Nord et Proche-Orient:**

Compte tenu du faible taux de pénétration de l'internet et du commerce électronique dans la majorité des pays de cette région, la problématique de la sécurisation des réseaux se pose à moindre échelle et le cadre réglementaire est dans la plupart des cas quasi inexistant.

**Afrique subsaharienne:**

Sur le plan réglementaire, la sécurisation des réseaux n'est pas encore une préoccupation majeure des autorités locales, beaucoup plus concernées par la mise en place desdits réseaux que par leur protection.

Le cryptage et le chiffrement des données sont encore faiblement pratiqués, d'où un contrôle limité des autorités.

**Amérique du Nord:**

Cette zone se caractérise par une absence de restrictions concernant la cryptographie et la confidentialité des communications. Cette situation correspond à une volonté de ne pas entraver le développement des échanges électroniques et de l'industrie des NTIC en général, en favorisant plutôt une autorégulation du secteur. En revanche, les gouvernements interviennent beaucoup plus activement dans le domaine de la sécurité intérieure. Sur le plan de l'offre, on note le développement commercial des techniques de biométrie ou des systèmes à base de carte à puce. Les solutions de sécurisation qui se développent le plus actuellement en Amérique du Nord concernent les VPN et les réseaux hertziens WLAN.

**Amérique latine:**

La sécurisation des réseaux de communication est une préoccupation secondaire chez la plupart des pays de la zone. La norme internationale ISO/CEI 17799 qui identifie les procédures de sécurité de l'information a déjà été adoptée par certains organes en charge de la normalisation mais reste peu implantée dans la région. En matière de chiffrement, l'Amérique latine se caractérise par un vide juridique qui autorise une libre utilisation de ces technologies.

**Asie:**

Les pays d'Asie se caractérisent d'abord par l'absence de cadre législatif sur la sécurité et la sécurisation des réseaux. Libre choix est laissé aux consommateurs et aux entreprises pour déployer les solutions de sécurité qui leur semblent appropriées. Les gouvernements montrent souvent l'exemple, en s'appuyant notamment sur des systèmes de type PKI.

Le marché de la sécurité a connu un réel essor au cours des deux dernières années. On peut noter que la demande indienne a évolué récemment vers des systèmes plus sophistiqués tels que des services de détection d'intrusion, la gestion du contenu, l'identification, le filtrage URL, les services de conseil en sécurité, les systèmes de cryptographie, comprenant des PKI (*public key infrastructure*) et des réseaux privés virtuels, et est en forte hausse.

**Europe:**

La plupart des gouvernements européens ont pris conscience de l'importance de la sécurité des infrastructures de télécommunication. La disponibilité et l'intégrité des réseaux sont garanties essentiellement par des règles imposées aux opérateurs de télécommunication dans le cadre des licences attribuées. De nombreux pays ont mis ou mettent en place des réseaux privés destinés à leurs forces de police et de protection civile. La cryptographie est maintenant couramment utilisée dans les Etats Membres de l'UE. Les enjeux prioritaires sont la sécurisation des communications mobiles et le passage au protocole IPv6.

**Moyen-Orient:**

L'usage de systèmes de chiffrement reste relativement libre au Moyen-Orient. Les opérateurs nationaux de télécommunication, souvent en position monopolitique, administrent les communications électroniques par un système de filtrage.

Si les dernières technologies de sécurité des réseaux sont disponibles, elles ne sont pas encore utilisées par les entreprises locales qui se contentent dans la majorité des cas de systèmes simples. Les sociétés commencent tout juste à prendre conscience de l'importance de sécuriser leurs communications à l'heure où le commerce électronique débute au Moyen-Orient.

**Synthèse Monde:**

Dans une société de l'information de plus en plus interconnectée, les menaces d'actes terroristes depuis la fin de 2002 ont rappelé l'importance de la sécurisation des réseaux de communication. La prise de conscience de ces enjeux, principalement économiques, varie d'un pays à l'autre en fonction de son niveau de développement: les pays les plus défavorisés s'intéressent plus à la mise en place des réseaux qu'à leur protection, alors que les pays plus développés s'impliquent essentiellement dans la sécurisation des communications du secteur public.

## 10.3 Lutte contre le spam

Nous sommes entrés dans l'âge du courrier électronique, de l'«e-mail» et des messages instantanés. Malheureusement, le fait que l'«e-mail» soit si bon marché et si facile à utiliser constitue la source de nouveaux problèmes, dont l'un des principaux est le spam, aussi appelé «spamming», «pourriel», ou «junk e-mail».

### 10.3.1 Origine et définition

Le spam est le courrier électronique envoyé à des personnes qui ne l'ont pas sollicité. N'importe qui peut envoyer un spam, c'est très facile et ça ne coûte pas cher. Cependant, rares sont ceux qui aiment en recevoir et plus rares encore ceux qui savent l'arrêter. Le spam n'est pas simplement source de perte de temps. Les fournisseurs d'accès à l'internet et les opérateurs mobiles dépensent des millions de dollars tous les ans pour stocker, transmettre et contrôler le spam. Ces coûts, à leur tour, sont transmis aux clients finals. Le spam a en outre un impact négatif sur la productivité des entreprises. Les administrations et entreprises comprennent désormais que le courrier électronique est essentiel à la bonne marche de leurs opérations. Comme leurs employés passent de plus en plus de temps à se servir du courrier électronique, rendre cet outil plus efficace devient une priorité, et filtrer le spam, une nécessité.

### 10.3.2 Spam: phénomène social et technique

Le spam est un phénomène social et technique. Son aspect social, le fait que des êtres humains – et non des ordinateurs – créent le spam, en fait autant un phénomène organique que mécanique. Le combat contre le spam n'est pas simplement un combat contre un logiciel ou des ordinateurs. Nous combattons une armée d'individus qui pensent et respirent, et qui ont à leur disposition un arsenal d'armes déployées contre nous. L'arme la plus puissante dans l'arsenal des «spammeurs» est le changement, la possibilité de modifier constamment son comportement.

Le spam est en mutation permanente. Les «spammeurs» changent constamment leurs tactiques pour éluder les filtres mis en place. Par exemple, les en-têtes de message, qui incluent des détails, tels que l'adresse IP de la source, sont le plus souvent modifiés, et les «spammeurs» changent également fréquemment les noms de leurs sites internet.

Pour être vraiment efficace, un filtre doit être capable de s'adapter en permanence pour contrer un adversaire adroit.

Puisque les «spammeurs» modifient leurs techniques d'attaque et changent leurs messages constamment, un système de filtrage qui se concentrerait sur une seule variable (adresse IP ou contenu du message par exemple) serait inefficace. Une solution efficace dans la lutte contre le spam doit être suffisamment complexe pour viser simultanément plusieurs variables.

### 10.3.3 Critères fondamentaux de la lutte antispam

Les quatre critères suivants sont fondamentaux: efficacité, prévision, facilité d'adoption, performance.

- Le critère le plus important pour une solution antispam est l'efficacité, à savoir la quantité de spam pouvant être bloquée par un filtre.

- Un autre facteur très important est la précision: la solution ne doit pas bloquer les messages licites. Pour qu'une solution antispam puisse être acceptée par une majorité d'utilisateurs potentiels, elle doit distinguer de manière très précise le spam des messages licites.
- Le critère suivant est la facilité d'adoption qui est reliée directement à la facilité d'installation et d'utilisation. La solution exige-t-elle des utilisateurs qu'ils créent leurs propres filtres? Nécessite-t-elle d'être mise à jour par les utilisateurs finals eux-mêmes? Est-elle fondamentalement transparente pour les utilisateurs? Si elle n'est pas facile à utiliser, elle sera probablement mal ou pas du tout employée.
- Pour conclure, la performance ou la rapidité du filtrage est importante. La solution ralentit-elle la livraison du courrier électronique? Ceci peut être décisif, en particulier pour les grands fournisseurs d'accès qui contrôlent et doivent transmettre des volumes importants de messages.

### 10.3.4 Solutions techniques de lutte contre le spam

Les principales solutions antispam s'appuient sur les méthodologies suivantes:

a) Blocage d'adresses IP

Le «Mail Abuse Prevention System's Realtime Blackhole List (MAPS RBL)» se présente sous la forme d'une «liste noire», mise à jour en temps réel, où sont énoncés les domaines identifiés comme étant «favorables, ou au moins neutres» pour les «spammeurs». Le système MAPS RBL permet aux gestionnaires de messagerie de mettre immédiatement à jour leurs listes de domaines et d'adresses IP bloqués et assure l'exécution automatique de ces mises à jour à partir des serveurs.

Cependant, le système bloque sans discernement des domaines entiers. L'organisation chargée du système MAPS RBL est donc tout naturellement prudente quand elle ajoute des noms à sa liste noire. Décider du blocage d'un domaine exige une recherche complète qui peut être longue. Lorsque finalement un domaine est ajouté à la liste noire, le nombre de spam est considérablement réduit.

En résumé, le système MAPS RBL n'est pas, à lui seul, une solution viable de lutte contre le spam. Il est souvent combiné avec d'autres techniques de combat, en dépit de sa tendance à bloquer les e-mails licites.

b) Filtrage du contenu

En termes d'efficacité, le filtrage du contenu a tendance à créer des problèmes semblables à la technique du blocage d'adresses IP.

Certaines solutions de filtrage combinent le filtrage du contenu avec le blocage d'adresses IP. Ces solutions incluent généralement un certain nombre de filtres statiques et permettent aux gestionnaires de réseaux de concevoir leurs propres filtres. Ces filtres de contenu ne sont, le plus souvent, pas mis à jour de façon dynamique, à partir d'une base centrale. Dans le meilleur des cas, les mises à jour sont mensuelles. Ces solutions permettent, non seulement un filtrage du contenu du corps ou du sujet du message, mais aussi parfois un filtrage de l'expéditeur. Ces solutions filtrent les messages au niveau du serveur et obtiennent donc de bons résultats en ce qui concerne la facilité d'utilisation. Mais, elles ne permettent pas d'arrêter systématiquement le spam car elles bloquent de 0% à environ 2,21% du courrier électronique licite.

c) Utilisation de signatures antispam

L'utilisation de signatures antispam spécifiques s'inspire du modèle des éditeurs de logiciels antivirus. Ces derniers surveillent et détectent l'apparition de nouvelles menaces et construisent des règles qui permettent de mettre à jour les filtres, protégeant ainsi l'intégralité et la sécurité des systèmes. La même architecture peut s'appliquer au courrier électronique. Les règles de filtrages sont créées par des opérateurs spécialisés et/ou des ordinateurs, qui déterminent si les messages sont effectivement du spam ou pas.

Un point critique reste la capacité à surveiller en temps réel l'activité des «spammeurs»: un réseau d'adresses électroniques leurres placées sur l'internet, aux emplacements connus pour être favorables,

attire le spam. Ce spam est ensuite automatiquement expédié vers un centre d'opérations, opérationnel 24 heures sur 24. Des règles fondées sur le spam le plus récent sont alors immédiatement transmises aux logiciel de filtrage installé sur les serveurs de messagerie des clients.

Cette solution est performante dans la mesure où les règles de filtrage peuvent être activées ou désactivées à volonté, en fonction de leur degré d'utilité à un moment donné.

### 10.3.5 Travaux de l'OCDE sur le spam

L'OCDE a organisé les 2 et 3 février 2004 à Bruxelles, en collaboration avec la Commission européenne (Direction de l'entreprise et de la société de l'information), un atelier de travail sur le spam. Le programme ainsi que les exposés prononcés lors de cet atelier de travail sont disponibles sur le site web de l'OCDE.

Nous pouvons noter les points suivants:

*Session 1*

Les gouvernements, les usagers et les représentants de l'industrie se doivent d'identifier les caractéristiques du spam afin de pouvoir établir un rapport sur ce problème et l'éradiquer. De plus, on doit établir des principes permettant de mesurer les efforts à entreprendre pour supprimer le spam et de réduire son taux d'expansion; on doit déterminer les mesures à prendre pour lutter contre le spam.

*Session 2*

Les impacts néfastes du spam sont communs à toutes les catégories d'usagers de l'internet, aussi bien les particuliers que les utilisateurs commerciaux, les gouvernements, les administrations des services de gestion et les fournisseurs de tels services. L'éradication du spam implique des coûts importants tant économiques que sociaux pour tous les acteurs susmentionnés. Cette session a permis d'explorer tous les coûts associés au spam, compte tenu du principe de la protection des usagers, de la confidentialité des messages et de la sécurité des réseaux, conformément aux lignes directrices de l'OCDE à ce sujet.

*Session 3*

Cette session a permis d'examiner les mécanismes, les nouvelles technologies et les modèles de spam et à conduit aux questions suivantes:

- Comment les spammeurs obtiennent-ils les adresses électroniques?
- Comment les spammeurs restent-ils indétectables?
- Comment l'émission de spam peut-elle être bénéficiaire financièrement?
- Comment peut-on changer les technologies en évitant de nouvelles possibilités pour les spammeurs (par exemple, le spam via les SMS ou la messagerie instantanée)?
- Comment peut-on, à l'aide de nouvelles technologies et de lois, éradiquer et arrêter le phénomène spam et accroître la croissance du volume des courriers électroniques?

*Session 4*

On a exploré les différentes voies techniques permettant de combattre les attaques spam tant dans le domaine commercial que dans celui des fournisseurs de services internet (ISP).

*Session 5*

On a examiné les différentes lois des pays membres de l'OCDE, entrées en vigueur en vue de réguler le spam.

*Session 6*

Le spam est un problème au niveau mondial et demande une solution mondiale. Une loi antispam internationale efficace est très difficile à mettre en œuvre, mais en se fondant sur les lois nationales existantes, elle pourrait «voir le jour»; des efforts de coopération doivent être fournis.

*Session 7*

On a étudié les meilleures pratiques afin de minimiser l'impact du spam sur les communications électroniques.

*Session 8*

On a constaté qu'une approche multidimensionnelle était nécessaire afin d'éradiquer le spam.

*Session 9*

On a défini les prochaines étapes antispam au niveau international.

(voir le site http://www.oecd.org/document/47/0,2340,en_2649_22555297_26514927_1_1_1_1,00.html)

### 10.3.6 Séminaire de l'UIT sur le spam

Dans la Déclaration de principes adoptée lors du Sommet mondial sur la société de l'information (SMSI) à Genève en décembre 2003, au paragraphe 37, les participants ont reconnu que le spam *est un problème important et croissant pour les utilisateurs, les réseaux et l'internet dans son ensemble.* De plus, dans le Plan d'action du SMSI adopté à la même session dans le paragraphe C5 d), il est fait mention qu'en vue de renforcer la confiance des utilisateurs, d'améliorer la sécurité lors de l'utilisation des TIC, il est nécessaire de «prendre des mesures appropriées aux niveaux national et international en ce qui concerne le spam».

Dans le prolongement des mesures adoptées par le SMSI, le Secrétaire général de l'UIT a convoqué une réunion internationale à Genève du 7 au 9 juillet 2004 ayant pour titre «Réunion thématique SMSI UIT sur la lutte contre le spam» (documents disponibles au site www.itu.int/spam).

### 10.3.7 Colloque mondial des régulateurs (UIT)

Au cours du cinquième Colloque mondial des régulateurs qui a eu lieu à Genève du 8 au 10 décembre 2004, une demi-journée a été consacrée au thème «Lutte contre le spam?».

Après avoir rappelé les actions menées par l'UIT et les organisations internationales et les travaux du SMSI (voir sections précédentes), l'assemblée a approuvé les lignes directrices suivantes, destinées à lutter efficacement contre le spam:

1) Législation nationale

   Il a été noté que peu de pays disposaient de lois efficaces: certitude juridique du «spam» en fonction de sa nature; une solution administrative pouvait être plus rapide qu'une solution pénale. Il ne fallait pas omettre la coordination au niveau national de tous les acteurs impliqués. Cette législation devait aussi disposer de moyens techniques de contrôle.

2) Evaluation de l'effet «spam»

   Des enquêtes, des sondages et des consultations auprès du public et des principales personnes concernées étaient indispensables pour rechercher les spammeurs aux niveaux national et international et pour les identifier, dans la mesure du possible (promotion des solutions techniques).

3) Coopération internationale

Celle-ci était indispensable, surtout pour les pays en développement, dont les infrastructures des télé-communications étaient non achevées et qui, par conséquent, avaient peu ou pas de «spammeurs» nationaux.

Le problème étant à l'origine situé hors du territoire national, une coopération internationale fondée sur la législation nationale était indispensable.

Le rapport et les conclusions de ce colloque sont disponibles sur le site de l'UIT.

NOTE – Programme mondial d'échange d'informations entre les régulateurs (G-REX).

Le G-REX, lancé en mai 2001 par l'UIT, est un forum en ligne d'échanges de vue et de partage d'expériences entre les régulateurs et les autorités chargées des politiques. L'adresse du site est la suivante: www.itu.int/ITU-D/treg/index-fr.html

Ce site contient des informations par pays et par région, telles que le profil des agences de réglementation dans le monde et la **législation antispam.**

**Conclusion**

Il est très difficile de combattre le spam efficacement. La réussite d'une solution exige une démarche à plusieurs niveaux, tant technique qu'organisationnel, qui soit capable, en outre, d'être très rapidement mise à jour.

Parmi les trois méthodologies décrites dans cette section, seule celle qui utilise des signatures antispam spécifiques a prouvé sa capacité à vaincre le spam.

## 10.4 Hameçonnage

La «Federal Trade Commission» aux Etats-Unis définit le hameçonnage (phishing) de la manière suivante: «le hameçonnage, également nommé fraude à la carte bancaire, est une escroquerie de haute technicité qui utilise le spam pour tromper les consommateurs et leur demander de fournir leurs numéros de carte de crédit, le numéro de leur compte bancaire, leur numéro de sécurité sociale, leurs mots de passe et d'autres informations sensibles.»[6]

Dans les cas recensés, il s'agissait de messages électroniques mystifiés, censés émaner d'une banque, qui utilisaient le langage HTML (*hyper text mark up language*) pour recréer l'image de la marque et l'adresse de la banque. Ces courriers électroniques orientaient les clients vers de faux sites web disposant d'adresses URL (*uniform ressource locators*) semblables à celles de sites officiels, où ils étaient priés de «réenregistrer» leurs informations personnelles et financières. Les pirates recueillaient ainsi des données pouvant être utilisées frauduleusement par la suite.

L'efficacité du courrier électronique et des communications en ligne qui les rend si attractifs pour le commerce électronique licite, les rend également attractifs aussi bien pour les «spammeurs» que pour les cybercriminels.

Si les entreprises veulent préserver l'efficacité et la commodité du courrier électronique avec leurs clients, elles doivent tenir compte du fait qu'il faille sécuriser cette voie de communication contre les criminels, attirés par le potentiel financier du monde en ligne. La réponse doit reposer sur l'utilisation d'une messagerie sécurisée avec chiffrement et signatures numériques pour protéger l'information, et authentifier le message et l'expéditeur.

Il faudrait en fait disposer d'une solution de messagerie sécurisée, qui n'exige aucune action particulière de l'utilisateur final. Une telle solution se chargerait du chiffrement et du déchiffrement, ainsi que celui de la signature et de la vérification des messages, ainsi que de la découverte et de la mémorisation des clés

---

6 FTC Consumer Alert, «How Not Get Hooked by a 'Phishing' Scam», <http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm>

nécessaires. Ce serait donc un système automatisé qui travaillerait de façon invisible au niveau réseau. Cependant, pour que la messagerie électronique soit automatiquement sécurisée, afin d'être vraiment efficace et largement utilisée en entreprise, elle doit reposer sur des normes ouvertes et offrir un moyen de paramétrer et de maintenir des connexions sécurisées avec les destinataires qui n'ont pas mis en place de messagerie sécurisée et/ou ne peuvent pas être formés à son utilisation.

Ces solutions doivent non seulement être invisibles aux expéditeurs, mais une fois les destinataires authentifiés, elles doivent également assurer la vérification et le déchiffrement automatiques des messages électroniques et garantir la signature des réponses. Pour répondre à ce besoin, on a mis au point des systèmes qui fonctionnent de manière transparente au niveau d'une couche réseau et utilisent de petites «empreintes» de protection à la fin du message électronique reçu. Ces systèmes peuvent assurer une sécurité bilatérale automatisée du message électronique, et une authentification sans formation préalable des deux utilisateurs (émetteur et destinataire du message électronique).

Lorsque de tels systèmes sont mis en œuvre, le courrier électronique et les communications en ligne, de cible principale pour les cybercriminels, deviennent un moyen sûr de communication avec les clients et les partenaires, tout en réduisant significativement le vol potentiel d'identité.

Voir les sites www.ftc.gv/bcp/conline/pubs/alorts/phishingalrt.htm (Etats-Unis) et www.data.gov.au/spam (Australie).

NOTE – En août 2004, une entreprise américaine spécialisée dans les filtres antispam a pu intercepter en 5 heures plus de 125 000 mails frauduleux à l'en-tête d'une grande banque américaine. Face à ces attaques qui se produisaient au niveau mondial, les banques ont mis en place, en plus des filtres antispam, des systèmes d'accès variant de façon aléatoire: jetons de sécurité changeant à chaque cession, calculateurs changeant toutes les minutes (système généralisé en Suisse depuis la mi-2004). Des attaques plus élaborées peuvent permettre au pirate (en cliquant sur l'URL d'un site en construction) d'implanter un cheval de Troie. La solution consiste à jeter ce courrier à la poubelle.

## 10.5 Convergence des systèmes d'information, des biens et des personnes: la vidéosurveillance sur IP

La tendance actuelle en ce qui concerne les marchés de la sécurité et de la sûreté consiste à accroître la convergence des ressources et à optimiser les systèmes déployés (tant physiques qu'informatiques), qu'il s'agisse de la sécurité des bâtiments, des personnes ou des systèmes d'information. Jusqu'à présent, les divers systèmes de sécurité (vidéosurveillance, contrôle d'accès, système d'information, etc.) étaient indépendants et autonomes et fonctionnaient en circuit spécialisé fermé. Aujourd'hui, avec l'explosion de l'internet, l'interconnexion IP, devenue incontournable, permet d'intégrer des systèmes de sûreté au système d'information. Ce partage de l'infrastructure physique/logique répond également au besoin croissant de partage de flux à tout moment et en tout lieu.

Avec les nouvelles tendances telles que la dérégulation des télécommunications, la multiplication des sites, la mobilité des collaborateurs et le besoin de suivi en temps réel, les entreprises sont entrées dans une phase d'optimisation des investissements se traduisant par:

– un partage et une consolidation des infrastructures;
– une normalisation et une évolution des technologies (protocole, compression, etc.);
– un besoin d'identification des sources d'économie substantielles;
– une augmentation de la productivité à moindre coût.

L'enjeu de la sécurité devient parallèlement de plus en plus important. Il faut assurer un niveau de sécurité adapté à l'ensemble du système interconnecté (tant au niveau du système que des données et de leur transfert). Il intervient:

– au niveau stratégique (pour les dirigeants);
– au niveau opérationnel (pour les gestionnaires techniques et de ligne);
– au niveau technologique (pour les responsables du système).

L'une des applications concrètes illustrant le rapprochement de l'informatique et de la vidéo est la vidéosurveillance sur IP.

Avec le développement des réseaux et du haut débit, l'accès à de nouvelles applications de plus en plus sophistiquées comme la vidéo est facilité. Les systèmes de vidéosurveillance sont donc de plus en plus interconnectés avec les systèmes d'information afin d'optimiser les infrastructures.

Le marché de la vidéosurveillance est en pleine mutation avec le passage du monde analogique au tout numérique. En 2003, la vidéosurveillance sur IP représentait 10% du marché européen de la vidéosurveillance, soit environ 65 millions EUR avec une très forte croissance (doublement chaque année). Aujourd'hui en France, une entreprise sur cinq dispose de caméras de vidéosurveillance et plus de 600 000 nouveaux raccordements sont enregistrés chaque année.

Jadis réservée aux sites dits «sensibles», la vidéosurveillance s'ouvre à de nouvelles applications (laboratoires, tourisme, services, gestion de projet, etc.), dépassant largement le cadre de la sécurité comme la fluidification des files d'attente ou l'analyse du comportement d'achat par exemple. La demande d'une surveillance sécurisée de la part des utilisateurs n'en est que plus forte.

La vidéosurveillance permet, entre autres, le suivi à distance, une gestion multisite, un enregistrement numérique centralisé ou une télésurveillance couplée au contrôle d'accès et d'alarmes. Tout responsable de la sûreté ou de la sécurité doit pouvoir accéder en temps réel à son système de vidéosurveillance en respectant:

– la surveillance hors site, par exemple à partir d'un simple navigateur web;
– la disponibilité du système et la gestion de la bande passante;
– la performance, la fiabilité et la qualité du service fourni en temps réel;
– l'interopérabilité avec des systèmes tiers comme le contrôle d'accès, la biométrie;
– la transparence, la facilité d'installation et la souplesse d'utilisation pour l'utilisateur.

Mais l'interconnexion de la vidéosurveillance avec le système d'information en IP doit faire l'objet d'une analyse minutieuse quant aux risques auxquels elle est exposée:

– risques au niveau des protocoles utilisés (H323, SIP, etc.), comme les attaques contre l'implémentation du protocole par les équipements déployés ou les attaques par usurpation d'identité;
– risques liés à l'utilisation du système d'information, comme l'écoute des communications, leur interception ou l'attaque par déni de service pour rendre indisponible le système.

Il est important de tenir compte des impératifs en matière de sécurité, que ce soit:

– lors de la sensibilisation aux risques existants, lors de tests d'intrusion ou de tests d'exploitation des vulnérabilités (physique ou logique);
– lors de l'audit technique des infrastructures mises en place;
– lors de l'implémentation de protections techniques, comme:
  • l'application de correctifs en fonction des équipements déployés pour assurer une surveillance active;
  • l'utilisation du protocole SIP contre l'usurpation d'identité;
  • l'utilisation de SRTP (*secure real-time transport protocol*) contre l'interception;
  • l'utilisation de systèmes de prévention d'intrusion (IPS) contre le déni de service (pouvant influencer les performances et donner lieu à de faux positifs).

Les besoins en vidéosurveillance sur IP sont croissants pour les parkings, les grandes agglomérations, les lieux publics (stades, centres sportifs, etc.), les transports en commun, les officines, les banques, etc. Un nombre toujours plus grand d'entreprises cherchent à intégrer dans leur réseau unique le trafic de vidéosurveillance, les signaux et alarmes de contrôle d'accès.

Imprimé en Suisse
Genève, 2006

Crédits de photos: Photothèque UIT