RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

SECRETARIAT GENERAL DE LA DEFENSE NATIONALE

N˚ 150 SGDN / DISSI / SCSSI 10 février 1991

FICHE D'EXPRESSION RATIONNELLE DES OBJECTIFS DE SÉCURITÉ DES SYSTEMES D'INFORMATION

(F.E.R.O.S.)

- GUIDE TECHNIQUE DU SCSSI -

Délégation interministérielle pour la sécurité des systèmes d'information

SERVICE CENTRAL DE LA SÉCURITÉ DES SYSTEMES D'INFORMATION

Table des matières

- 1.3˚) Confidentialité
- 1.4˚) Intégrité

2.- LES CONTRAINTES A PRIORI

- 2.1˚) Calendrier
- 2.2˚) Budget
- 2.3˚) Flux d'informations
- 2.4˚) Bâtiments et accès
- 2.5˚) Spécifications techniques
- 2.6˚) Évolutions
- 2.7˚) Personnels

3.- LES MENACES

- 3.1˚) Nature
- 3.2˚) Vulnérabilités utilisées
- 3.3˚) Moyens nécessaires

FICHE «BESOINS DE SÉCURITÉ DES INFORMATIONS»

FICHE «CONTRAINTES PAR SITE»

TITRE III : GLOSSAIRE

ANNEXE : MENACES-TYPES

1.- NATURE DE LA MENACE

- 1.1˚) La menace stratégique
- 1.2˚) La menace terroriste
- 1.3˚) La menace ludique
- 1.4˚) La menace avide

2.- VULNÉRABILITÉS DES SYSTEMES D'INFORMATION

- 2.1˚) Vulnérabilités des personnels
- 2.2˚) Vulnérabilités de l'organisation
- 2.3˚) Vulnérabilités des matériels
- 2.4˚) Vulnérabilités des traitements
- 2.5˚) Vulnérabilités des télécommunications

3.- ATTAQUES POSSIBLES

- 3.1˚) Attaques cryptologiques
- 3.2˚) Attaques TEMPEST, piégeages
- 3.3˚) Attaques informatiques
- 3.4˚) Attaques par virus, bombes, etc

- 3.5˚) Attaques sur les réseaux
- 3.6˚) Attaques sur les systèmes de conception
- 3.7˚) Attaques physiques

BUTS DE LA FEROS

Les responsables des *systèmes d'information* doivent garantir une sécurité adéquate à ceux qui leur confient des *informations* ou utilisent les services de leur système. Si l'application des règles de l'art suffit, en général, pour garantir le système contre les pannes et les accidents, la protection contre la malveillance aussi bien que l'application des lois et règlements (loi 'informatique et libertés', protection du secret de Défense, ...) requièrent une analyse particulière.

Les *objectifs de sécurité* d'un système d'information font partie intégrante des spécifications opérationnelles de ce système, au même titre que les fonctions qu'il doit remplir et les performances qu'il doit atteindre. Ils doivent donc être traités comme ces autres spécifications opérationnelles, tout au long du cycle de vie du système.

La première étape de ce cycle est d'expliciter les **besoins de sécurité** *:* quel est le seuil minimal de *disponibilité* requis pour les informations traitées et les services rendus ? Que doit-on obtenir en termes *d'intégrité* et de *confidentialité* pour les données et les traitements associés, compte-tenu notamment des obligations légales et réglementaires auxquelles ils sont soumis.

Il est nécessaire, à ce stade, de rappeler les **contraintes a priori** qui s'exercent sur le futur système et qui peuvent avoir une incidence sur sa sécurité : il peut s'agir de contraintes d'exploitation, comme, par exemple, d'utiliser un centre de calcul ou un réseau préexistants ou d'implanter des équipements d'extrémité dans des lieux publics ; il y a souvent, également, des contraintes techniques comme le respect de certaines normes, l'emploi de certains matériels ou logiciels pour des raisons de standardisation, etc... Les moyens à mettre en oeuvre pour assurer la sécurité du système dépendront évidemment de ces choix et contraintes a priori.

Il faut enfin réfléchir aux **menaces** contre lesquelles il est raisonnable de se protéger : quelle est leur nature (ludique, avide, terroriste, stratégique, ...) ? Quels moyens un attaquant

pourrait-il déployer pour compromettre la sécurité du système, compte-tenu de l'enjeu que cela peut représenter pour lui ?

Le présent guide correspond à cette première étape du développement d'un système d'informations intégrant la sécurité. Il propose au responsable du système un cadre structuré pour définir ses objectifs de sécurité en répondant à trois séries de questions, sur les besoins de sécurité d'abord, sur les contraintes a priori ensuite et, enfin, sur les menaces.

Les réponses qu'apportera le responsable du système aux questions posées par cette fiche lui permettront de définir la *politique de sécurité* qu'il devra mettre en oeuvre, c'est-à-dire l'ensemble des mesures nécessaires pour satisfaire les besoins de sécurité, malgré les menaces prises en compte et en respectant les contraintes a priori. Les compromis qu'il sera peut-être nécessaire, au cours du cycle de vie du système, de faire sur ces spécifications de sécurité pourront alors être faits clairement et leurs conséquences appréciées de même.

Ce guide se décompose en quatre parties :

- - un guide, de rédaction du questionnaire,
- - le questionnaire proprement dit, organisé suivant le même plan que le guide,
- - un glossaire donnant, la définition officielle de divers termes relatifs aux systèmes d'information ; ces termes sont *écrits en italique et soulignés* à leur première apparition.
- - une annexe présentant les différentes menaces susceptibles d'être prises en compte pour un système d'informations donné, destinée à aider le responsable à définir précisément celles qui le concernent.

TITRE I : GUIDE

1˚) Les Besoins de sécurité

Avant de remplir ce paragraphe sur les besoins de sécurité, il convient d'avoir répertorié les informations qu'utilise le système.

Le terme 'information' pourra (selon le contexte et la définition particulière qui en sera donnée par le responsable du système) inclure aussi bien les données proprement dites que les traitements qui leur sont appliqués, ces deux groupes d'entités pouvant chacun faire l'objet de besoins de sécurité particuliers.

- 1.1˚) Obligations légales, réglementaires ou contractuelles

a) Indiquer, si c'est le cas, quels fichiers ou traitements ayant trait aux informations traitées par le système tombent sous le coup de la loi n˚ 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés.

Ces fichiers et traitements devant faire l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés, indiquer si cette démarche a déjà été entreprise.

Dans l'affirmative, préciser si les fichiers et traitements ont nécessité la promulgation d'une loi, ont été décidés par acte réglementaire après avis motivé de la C.N.I.L., ou ont fait l'objet d'une simple déclaration à la C.N.I.L.

b) Indiquer si certaines obligations particulières d'ordre réglementaire ou contractuel imposent des contraintes supplémentaires pour les informations ou le système et préciser les responsabilités des diverses parties prenantes.

- 1.2˚) Disponibilité

a) Indiquer le délai au-delà duquel l'indisponibilité des informations est insupportable.

b) Indiquer le délai maximal admissible d'indisponibilité du système lui-même et éventuellement les types de fonctionnement en mode dégradé admissibles.

- 1.3˚) Confidentialité

a) Indiquer si certaines informations tombent sous le coup du décret 81-514 du 12 mai 1981 relatif à l'organisation de la protection des secrets et des informations concernant la Défense nationale et la sûreté de l'État.

Dans l'affirmative, préciser, par type d'informations, le niveau de protection décidé par l'autorité ayant procédé à la classification.

Il est rappelé (Décret n° 81-514 du 12 mai 1981) qu'il existe trois niveaux de classification :

La mention **TRES SECRET DÉFENSE** est réservée aux informations dont la divulgation est de nature à nuire à la Défense nationale et à la sûreté de l'État et qui concernent les priorités gouvernementales en matière de Défense.

La mention **SECRET DÉFENSE** est réservée aux informations dont la divulgation est de nature à nuire à la Défense nationale et à la sûreté de l'État.

La mention **CONFIDENTIEL DÉFENSE** est réservée aux informations qui ne présentent pas en elles-mêmes un caractère secret, mais dont la connaissance, la réunion ou l'exploitation peuvent conduire à la divulgation d'un secret intéressant la Défense nationale et la sûreté de l'État.

Indiquer si les informations, bien que non classifiées, concernent notre patrimoine scientifique, technique, industriel, économique ou diplomatique et doivent donc rester de **DIFFUSION RESTREINTE.**

Préciser, si le niveau de protection doit évoluer dans le temps, l'instant à partir duquel l'information peut être déclassifiée et le niveau retenu après déclassification.

b) Indiquer si certaines informations relèvent de l'Instruction Interministérielle n° 2100/ SGDN/SSD du 1er décembre 1975 relative à l'application en France du système de sécurité de l'Organisation du Traité de l'Atlantique Nord (OTAN).

Dans l'affirmative, préciser, par type d'informations, le niveau de protection décidé par l'autorité ayant procédé à la classification.

Il est rappelé qu'il existe quatre degrés de classification :

- **TRES SECRET COSMIC** (en anglais : **COSMIC TOP SECRET**) : Informations dont la divulgation non autorisée aurait des conséquences exceptionnellement graves pour l'Organisation du Traité de l'Atlantique Nord.
- **SECRET OTAN** (en anglais : **NATO SECRET**) :
  Informations dont la divulgation non autorisée aurait des conséquences graves pour l'OTAN.
- **CONFIDENTIEL OTAN** (en anglais : **NATO CONFIDENTIAL**) : Informations dont la divulgation non autorisée serait préjudiciable aux intérêts de l'OTAN.
- **DIFFUSION RESTREINTE OTAN** (en anglais : **NATO RESTRICTED**) : Informations nécessitant une protection inférieure à celle qui est assurée aux informations CONFIDENTIEL OTAN.

Préciser, si le niveau de protection doit évoluer dans le temps, l'instant à partir duquel l'information doit être déclassifiée et le niveau retenu après déclassification.

c) Pour les informations sensibles non classifiées de défense, indiquer, conformément à l'Instruction Générale Interministérielle n° 900/SGDN, le niveau de protection qu'il convient de leur assurer.

Il est rappelé qu'il existe trois niveaux de protection :

- **- SECRET**
- **- CONFIDENTIEL**
- **- DIFFUSION RESTREINTE**

Chacun de ces niveaux est assorti d'une mention spécifique, caractéristique du domaine protégé ; cette mention peut être :

- **- PERSONNEL**
- **- MÉDICAL**
- **- INDUSTRIE, COMMERCIAL, NOM d'une Société**
- **- NOM** d'un programme
- - etc...

Préciser, si le niveau de protection doit évoluer dans le temps, l'instant à partir duquel l'information doit être déclassifiée et le niveau retenu après déclassification.

- 1.4˚) Intégrité

Pour l'ensemble des informations (données et traitements), indiquer quels contraintes d'intégrité sont à prendre en compte.

On procédera, par analogie avec la confidentialité, en définissant différentes classes correspondant à des besoins d'intégrité divers ; par exemple :

La mention **INTÉGRITÉ MAXIMALE** s'appliquera aux informations dont la modification illicite pourrait avoir des conséquences très graves pour les intérêts vitaux du système ou de ses utilisateurs.

La mention **FORTE INTÉGRITÉ** s'appliquera aux informations dont la modification illicite pourrait avoir des conséquences non négligeables sur les intérêts vitaux du système ou de ses utilisateurs

Les autres informations recevront la mention **INTÉGRITÉ NORMALE.**

2˚) Les contraintes a priori

Cette partie regroupe toutes les contraintes connues, relatives à la mise en place du système d'information, que celles-ci découlent d'obligations incontournables, ou bien, suivant la phase de définition du projet, de choix définitivement arrêtés.

- 2.1˚) Calendrier

Indiquer les grandes dates prévues ou souhaitées ; dans le cas où la mise en service doit être effectuée de manière progressive, induisant alors un fonctionnement dégradé ou limité, définir aussi précisément que possible les différentes phases de montée en puissance.

- 2.2˚) Budget

En cas de mise en place progressive des éléments du système, indiquer les contraintes budgétaires liées à chacune des phases.

- 2.3˚) Flux d'informations

a) Indiquer, si cela a déjà pu être déterminé, les types de communications prévus (réseau téléphonique commuté, lignes spécialisées, ...), les réseaux nationaux ou internationaux utilisés (Transpac, Infonet,...).

b) Préciser l'implantation géographique probable des différents sites constitutifs du système ainsi que le volume prévisible des informations transitant entre eux.

c) Indiquer si le système doit être en relation avec d'autres systèmes présents ou à venir et si certaines contraintes, d'interopérabilité en particulier, en résultent.

- 2.4˚) Bâtiments et accès

Indiquer s'il est prévu d'utiliser des bâtiments déjà existants pour abriter le(s) site(s), ou si des locaux seront spécialement construits à cet usage.

Préciser, lorsque cela est possible, les contraintes liées à l'implantation physique du ou des sites et portant tant sur la périphérie immédiate (permettant ou non une approche non détectable, la mise en place permanente ou occasionnelle d'une station d'écoute des signaux parasites compromettants, etc...) que sur les accès.

- 2.5˚) Spécifications techniques

Suivant l'avancement de la phase de définition du système, indiquer les contraintes techniques qui ont déjà pu être dégagées : type et caractéristiques des matériels, performances, normes à respecter,...

Dans le cas d'un système réparti, il est utile de donner la configuration prévue dans chacun des sites.

- 2.6˚) Évolutions

Dans le cas où une évolution du système est prévue ou possible à plus ou moins long terme, indiquer les contraintes qui peuvent en résulter (accès à des réseaux, interopérabilité, compatibilité et évolutivité des matériels,...).

- 2.7˚) Personnels

a) Si le système traite d'informations relevant du secret de Défense ou de la sûreté de l'Etat, indiquer pour quels personnels y ayant accès (conception, exploitation, maintenance, utilisateurs,...) il est prévu une habilitation telle que définie dans l'Instruction Générale Interministérielle n˚ 1300/SGDN/SSD du 12 mars 1982, et à un niveau correspondant à celui des informations auxquelles ils peuvent avoir accès.

b) Pour toutes les informations, autres que celles relevant du paragraphe ci-dessus, indiquer si les personnels y ayant accès sont (ou seront) soumis à une clause contractuelle de confidentialité, matérialisée, par exemple, par la signature d'une attestation de reconnaissance de responsabilité.

c) Indiquer s'il existe au sein de l'organisme une fonction de sécurité des systèmes d'information et, dans l'affirmative, préciser sa dépendance hiérarchique vis-à-vis de la direction, sa structure, ses domaines d'action et ses principales prérogatives.

d) Indiquer si les personnels font l'objet de séances régulières de sensibilisation aux problèmes de sécurité des systèmes d'information et, dans l'affirmative, préciser quels sujets sont généralement abordés.

e) Indiquer si possible, par catégorie (direction, cadres, personnels d'exécution,...), le senti-

ment des personnels face au problème de la sécurité des systèmes d'informations (adhésion, hostilité,...).

3˚) Les menaces

Il est illusoire de vouloir dresser une liste exhaustive de toutes les menaces qui planent sur un système d'information, l'"état de l'art" en la matière étant en perpétuelle évolution.

Le responsable devra néanmoins s'efforcer, dans cette partie, de déterminer le plus objectivement possible les menaces qui lui semblent pouvoir s'appliquer au système dont il a la charge, en précisant leur nature, les vulnérabilités du système sur lesquelles elles s'appuient et les moyens d'attaque, techniques ou non, nécessaires à leur réalisation effective et, compte-tenu du profit que peut escompter l'attaquant, les moyens qu'il acceptera de consacrer à cette attaque.

Pour faciliter sa tâche, le responsable trouvera dans l'annexe intitulée "Menaces-types" un certain nombre de renseignements utiles, comprenant notamment une définition des quatre types de menaces principales, des éclaircissements sur les vulnérabilités susceptibles d'être rencontrées dans tout système d'information et quelques modes d'attaque parmi les plus couramment utilisés.

TITRE II
QUESTIONNAIRE

Présentation du système

Nom du système[1] : _____.

Services rendus[1] : _____.

Nom du responsable[1] : _____.

1˚) Les besoins de sécurité

- 1.1˚) **Obligations légales, réglementaires ou contractuelles**
  Obligations liées aux informations
  VOIR FORMULAIRE "BESOINS DE SÉCURITÉ DES INFORMATIONS"
  Obligations liées au système[1]:

- 1.2˚) **Disponibilité**
  Délai maximal d'indisponibilité tolérable pour les informations
  VOIR FORMULAIRE "BESOINS DE SÉCURITÉ DES INFORMATIONS"
  Délai maximal d'indisponibilité tolérable pour les services rendus par le système[1] :

- 1.3˚) **Confidentialité**
  VOIR FORMULAIRE "BESOINS DE SÉCURITÉ DES INFORMATIONS"

---

1. Compléter

- 1.4˚) **Intégrité**
  VOIR FORMULAIRE "BESOINS DE SÉCURITÉ DES INFORMATIONS"

2˚) <u>Les contraintes a priori</u>

- 2.1˚) **Calendrier**[1]

Expression du besoin : de _____ à _____.
Spécifications fonctionnelles : de _____ à _____.
Conception : de _____ à _____.
Tests : de _____ à _____.
Validation : de _____ à _____.
Certification : de _____ à _____.

Mise en service globale : _____.
Retrait du service : _____.
Mise en service progressive :

Phase 1 : de _____ à _____ : _____.[1]
Phase 2 : de _____ à _____ : _____.[1]
Phase 3 : de _____ à _____ : _____.[1]
Phase 4 : de _____ à _____ : _____.[1]
Phase 5 : de _____ à _____ : _____.[1]

- 2.2˚) **Budget**[2]

Budget global : _____.
Budget phase 1 : _____.
Budget phase 2 : _____.
Budget phase 3 : _____.
Budget phase 4 : _____.
Budget phase 5 : _____.

- 2.3˚) **Flux d'informations** ***(****Ne pas utiliser le § 2.3 si le système ne comporte pas de composante télécommunications)*

a) <u>Supports des communications</u>
Type[3]: _____.
Réseaux[3]: _____.

b) <u>Implantation géographique et volume des échanges</u>

- 1) <u>Implantation géographique</u>

Centre de gestion du système[3]: _____.
Centre de gestion de secours[4]: _____.

---

1. Désignation de la phase
2. Compléter
3. Compléter

Lieu d'implantation

Centres régionaux[1]: _____.
Centres locaux[5]: _____.
Installations terminales[5]_____.
Divers[3]

- 2) Volume des échanges

Entre centre de gestion et régionaux :_____ _____.
Entre centres régionaux et locaux : _____.

c) Liaisons avec d'autres systèmes[2] :
Sans objet
Contraintes particulières[3] :

- 2.4˚) **Bâtiments et accès**
  VOIR FORMULAIRE "CONTRAINTES PAR SITE"

- 2.5˚) **Spécifications techniques**
  VOIR FORMULAIRE "CONTRAINTES PAR SITE"

- 2.6˚) **Évolutions**[3]
  Date envisagée : _____.
  Évolutions prévues :

- 2.7˚) **Personnels**

a) Habilitations(s) :
Oui / Non

b) Clause contractuelle de confidentialité[3] :
Oui / Non

c) Fonction de sécurité des systèmes d'information[7]
Non :

Oui[4] : Dépendance hiérarchique : _____.
Structure :
Domaines d'action :
Prérogatives :

1. Nombre
2. Rayer les mentions inutiles
3. Rayer les mentions inutiles
4. Compléter

3˚) <u>Les menaces</u> *(Le §3 est destiné à être reproduit en un nombre suffisant pour traiter la totalité des menaces pesant sur le système.)*

- 3.1˚) **Nature**[7]

Stratégique / Terroriste / Ludique / Avide
Autre : _____.[8]

- 3.2˚) **Vulnérabilités utilisées**[8]

Personnels
Organisation
Matériels
Traitements
Télécommunications

- 3.3˚) **Moyens nécessaires**

Financiers
Connaissances techniques
Connaissance du système
Accès physique au système

BESOINS DE SÉCURITÉ DES INFORMATIONS

Ce § est destiné à être reproduit en un nombre suffisant pour traiter toutes les informations (données et traitements) dépendant du système.

Nature de l'information

<u>Nom</u>[1] : _____.

<u>Type</u>[2] : Donnée / Traitement

Obligations légales, réglementaires ou contractuelles

a) <u>Déclaration C.N.l.L.</u>[10] :

- Sans objet
- En cours
- Terminée
  - Promulgation d'une loi
  - Acte réglementaire
  - Simple déclaration

---

1. Compléter
Compléter
2. Rayer les mentions inutiles

b) Autres obligations :[9]

Disponibilité
Délai maximal d'indisponibilité tolérable[9] : _____.
Modes dégradés admissibles[9]

Confidentialité
a) Secret de Défense[10] :

- Sans objet
- Classification[9] :
- Durée[9] :
- Déclassification[9] :

b) OTAN[10] :

- Sans objet:
- Classification[9]:
- Durée[9] :
- Déclassification[9]:

c) Autres[10] :

- 1) Classification spécifique
  - Niveau[10]
    - SECRET
    - CONFIDENTIEL
    - DIFFUSION RESTREINTE
  - Mention[10]
    - **PERSONNEL**
    - **COMMERCIAL**
    - **MÉDICAL**
    - **INDUSTRIE**
  - Autres[9] :
    Durée[9] :
    Déclassification[9]:
- 2) Sans classification

Intégrité[1]
MAXIMALE
FORTE
NORMALE

---

1. Compléter
Rayer les mentions inutiles

CONTRAINTES PAR SITE

Ce § est destiné à être reproduit en un nombre suffisant pour traiter tous les sites du système.

Nature du site[11]
Centre de gestionCentre de gestion de secours
Centre régionalCentre local

Installation terminale ou autre[1] : _____.

Bâtiments et accès[11]
Bâtiments :à construire / existants
Périphérie : dégagée / non dégagée
Voisinage : contrôlable / non contrôlable
Accès illicite : impossible / très difficile / difficile / facile

Spécifications techniques
Normes à respecter :
Compatibilité de matériels :
Contraintes diverses :

TITRE III GLOSSAIRE

Besoins de sécurité : Définition précise et non ambiguë des niveaux de confidentialité, d'intégrité et de disponibilité qu'il convient d'assurer à une information.

Confidentialité : Qualité d'une information de n'être connue que par les personnes ayant besoin de la connaître.

Disponibilité : Qualité d'une information d'être, à la demande, utilisable par une personne ou un système.

Donnée : Représentation d'une information sous une forme conventionnelle, destinée à faciliter son traitement.

Information : Élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué.

Intégrité : Qualité d'une information de ne pouvoir être altérée, détruite ou perdue par accident ou malveillance.

Objectifs de sécurité d'un système : Document, approuvé par l'autorité responsable d'un système en projet, définissant explicitement les besoins de sécurité de ce système, les contraintes auxquelles il est soumis et les menaces contre lesquelles il doit pouvoir se prémunir.

Politique de sécurité : Ensemble des lois, règles et habitudes réglementant la gestion, la pro-

1. Compléter

tection et la distribution des biens, informations sensibles comprises, d'un organisme, au sein de celui-ci.

Système d'information : Ensemble des moyens dont le fonctionnement fait appel d'une façon ou d'une autre à l'électricité et destinés à élaborer, traiter, stocker, acheminer ou présenter l'information.

ANNEXE MENACES-TYPES

1˚) Nature de la menace

Suivant les missions du système et les informations qu'il traite, la nature de la menace peut être fort différente ; on distingue généralement quatre natures de menaces :

- **1.1 La menace stratégique**

La menace stratégique s'intéresse par essence à toute information concernant le secret de Défense et la sûreté de l'État, tels qu'ils sont définis par le décret 81-514 du 12 mai 1981, mais également à celles appartenant à notre patrimoine national, qu'il soit d'ordre scientifique, technique, industriel, économique ou diplomatique ; la menace stratégique peut également attenter à la disponibilité de systèmes d'information, dont le fonctionnement continu est nécessaire au fonctionnement normal des institutions.

Elle est généralement le fait d'organismes gouvernementaux ou para-gouvernementaux, structurés et organisés pour la recherche du renseignement et disposant de moyens financiers et techniques très importants, leur permettant d'envisager tous types d'attaque sur un système.

- **1.2 La menace terroriste**

On définira la menace terroriste comme regroupant toutes les actions concourant à déstabiliser l'ordre établi ; les actions entrant dans cette catégorie peuvent avoir un caractère violent (destruction physique de systèmes) ou plus insidieux (intoxication et désinformation par détournement ou manipulation d'informations, sensibles ou non, perturbations engendrées dans un système et susceptibles d'envenimer des troubles sociaux présents à l'état latent,...).

Les groupes, susceptibles de commettre ce genre de forfaits, disposent généralement de moyens financiers importants, leur permettant d'envisager pratiquement tous types d'attaque sur un système.

- **1.3 La menace ludique**

Les nouvelles techniques de traitement de l'information ont créé cette nouvelle menace, qui procède davantage, dans l'esprit de ceux qui en sont les auteurs, d'un jeu ou d'un sport que d'un réel forfait (intrusion de systèmes, développement de virus ou de vers informatiques,...).

Les moyens financiers et techniques dont disposent les personnes, agissant souvent isolément, qui commettent de telles actions, sont généralement modestes, et seule leur bonne connaissance du système visé leur permet de s'y introduire de façon efficace.

- **1.4 La menace avide**

Cette nouvelle forme de délinquance, engendrée par l'apparition des procédés de traitement de l'information, et parfois dite "en col blanc", peut avoir deux différents buts, parfois concomitants :

Le premier se traduit par un gain pour l'attaquant ; ce gain peut être financier (détournement de fonds), lié à un savoir-faire (concurrence déloyale), sentimental (vengeance), ou de tout autre ordre.

Le second occasionne une perte pour l'attaqué ; ce peut être la destruction de son système ou de ses informations, une perte de crédibilité ou de prestige vis-à-vis d'une tierce personne, etc...

Il est impossible de définir, même succinctement, le profil-type d'un fraudeur de ce genre, tant les applications susceptibles d'être attaquées sont multiples ; néanmoins, les statistiques à ce sujet permettent de souligner que dans un grand nombre de cas, la menace a été initiée et mise en œuvre à l'intérieur même de l'organisme abritant le système et a été le fait d'employés, dont les antécédents ne permettaient pas de supposer qu'ils commettraient un forfait de ce type.

2˚) Vulnérabilités des systèmes d'information

Un système d'informations est composé de manière indissociable de personnels et de matériels, effectuant des traitements donnés sur les informations, selon des règles d'organisation prédéfinies ; chacune de ces composantes possède intrinsèquement des vulnérabilités, dont la connaissance est indispensable pour imaginer les parades nécessaires à la réduction du risque qu'elles engendrent.

Il est à noter que le succès d'une attaque nécessite souvent l'exploitation en série de plusieurs vulnérabilités : l'attaquant devra, par exemple, tirer parti d'une faille de l'organisation du système avant de pouvoir utiliser les vulnérabilités des traitements.

- **2.1 Vulnérabilités des personnels**

Un système d'informations est toujours servi par des hommes et pour des hommes ; que ceux-ci aient accès aux informations pour les créer, les manipuler, les détruire, ou au système pour le concevoir, permettre son exploitation, l'utiliser, ils présentent tous un risque potentiel élevé.

Outre les erreurs involontaires qu'ils peuvent commettre dans le cadre de leurs attributions, ils peuvent également se prêter à des

actions de malveillance, soit de leur propre fait, soit suite à une incitation extérieure, leurs faiblesses naturelles pouvant être mises à profit par un agresseur éventuel ; on peut, dans ce cadre, citer :

- - Erreurs commises par excès de routine, laxisme, fatigue, manque de conscience professionnelle ou de formation ; ces erreurs peuvent intervenir lors de la conception du système (erreurs dans l'expression du besoin ou les spécifications) ou pendant sa phase opérationnelle.
- - Divulgation d'informations sensibles ou de renseignements sur le système par bavardage inconsidéré, vantardise, provocation, au cours de réunions professionnelles, familiales, ou associatives, ou par des personnels licenciés ou démissionnaires,
- - Actions diverses entreprises sous la pression (menaces de violence, chantage, dettes,...), par idéologie politique ou volonté de nuire, sous l'effet de produits divers (alcool, drogues,...),
- - Perturbations diverses en cas de mouvements sociaux,...

- **2.2 Vulnérabilités de l'organisation**

La structure et les procédures de tous ordres qui existent dans l'organisme abritant le système ont une influence directe sur celui-ci ; des déficiences en ce domaine peuvent entraîner des défauts de fonctionnement du système et des fautes exploitables par un agresseur éventuel ; on citera :

- - Mauvaise connaissance des textes légaux ou réglementaires en vigueur,
- - Absence de références hiérarchiques définies,
- - Extension abusive des privilèges, par laxisme ou complaisance, allant au-delà du "besoin d'en connaître",
- - Procédures inefficaces ou inapplicables,
- - Pertes de compétences ou de savoir-faire, suite au départ de personnels cumulant diverses fonctions "stratégiques",

- **2.3 Vulnérabilités des matériels**

Les matériels utilisés par le système sont techniquement vulnérables à certains événements, parmi lesquels il convient de citer :

- - Mauvaise conception ou industrialisation des composants du système, non-respect du cahier des charges,
- - Perturbations dues à la présence d'ondes électromagnétiques dans le milieu ambiant (radars, radio,...),
- - Émission de signaux parasites compromettants par des matériels ne respectant par les normes dites "TEMPEST",
- - Piégeage des matériels (dispositifs d'enregistrement ou de réémission des données),
- - Modification ou substitution des composants du système,...
- - Incendie, destruction mécanique, inondation,...
- - Défaillances de l'alimentation électrique, de la climatisation,...

- **2.4 Vulnérabilités des traitements**

Quels que soient sa nature et la manière dont il est effectué (personnel, logiciel, micro-code,...), tout traitement est vulnérable dans sa logique même, c'est-à-dire dans le contrôle de l'enchaînement successif des tâches élémentaires qui le composent ; si, de plus, ce traitement est confié à des processus automatiques, certaines vulnérabilités supplémentaires sont introduites ; parmi les vulnérabilités les plus souvent rencontrées, on peut citer :

- - Mauvaise conception ou implantation physique de la logique de traitement,
- - Modification illicite ou non contrôlée, utilisation de versions périmées de la logique de traitement,
- - Mauvaise cohésion des algorithmes utilisés,...

- **2.5 Vulnérabilités des télécommunications**

Lorsque, parmi les traitements appliqués aux informations, des transferts ont lieu à travers des lignes de télécommunications, les vulnérabilités du système sont bien évidemment accrues ; suivant le type de support utilisé, elles peuvent être quelque peu différentes, mais certaines constantes existent :

- - Écoute sur la ligne de télécommunication,
- - Rejeu d'informations déjà transmises,
- - Brouillage ou saturation de la ligne de télécommunication,
- - Intrusion active par usurpation d'identité du destinataire ou de l'expéditeur d'informations,
- - Destruction physique ou logique de la ligne de transmission.

3˚) Attaques possibles

Bien qu'il soit bien difficile de savoir où et sur quoi l'attaque portera, il est primordial que les diverses attaques possibles aient été au moins une fois évoquées, puisque c'est à partir d'elles que l'on définira les mesures de prévention et de protection qu'il convient de mettre en place.

Suivant leur mode d'action, on distingue divers types d'attaque, nécessitant des moyens matériels, humains et des délais que l'on s'efforcera d'apprécier.

- **3.1 Attaques cryptologiques**

Les attaques d'ordre cryptologique consistent, lorsqu'une information est chiffrée, à retrouver l'information claire, ainsi que les éléments secrets qui ont servi à son chiffrement ; ces éléments une fois connus, la confidentialité et l'intégrité des informations ne peuvent être conservées.

Certaines fautes de chiffrement sont parfois à l'origine de failles mises à profit pour décrypter telle ou telle information particulière ou groupe d'informations ; les moyens à mettre en œuvre sont alors généralement minimes, la durée nécessaire, de l'ordre de quelques heures, mais une bonne connaissance du système (ou la compromission des personnes concernées) est obligatoire pour avoir connaissance des fautes de chiffrement et pouvoir les exploiter utilement.

Une autre attaque cryptologique consiste en une analyse mathématique des algorithmes de chiffrement eux-mêmes, permettant parfois de découvrir des failles, utilisables pour le décryptement ; les moyens à mettre en œuvre sont alors considérables (très grosse puissance de calcul, mathématiciens chevronnés,...) pour des études qui peuvent s'étaler sur de nombreuses années.

- **3.2 Attaques TEMPEST, piégeages**

Le terme «TEMPEST» regroupe l'ensemble des mesures prises ou à prendre pour éviter que la connaissance par écoute ou interception de certains des signaux parasites émis par un matériel électronique quelconque ne permette de remonter aux informations qui sont à l'origine de leur création ; les rayonnements dits «compromettants» dont il est question se propagent de deux manières différentes dans l'environnement dans lequel ils sont situés :

- - par rayonnement dans l'atmosphère, avec une portée de l'ordre de quelques dizaines de mètres.
- - par induction puis conduction dans des matériaux métalliques situés à proximité des équipements en cause, les distances pouvant alors être de plusieurs centaines de mètres.

L'attaque par piégeage des équipements est associée à l'aspect TEMPEST, car les deux procédés sont souvent employés simultanément ; le piégeage consiste, par exemple, à installer dans ou à proximité d'un matériel «sain» des composants particuliers dont le but peut être l'enregistrement et le stockage illicite d'informations, la réémission vers des équipements

d'écoute, le brouillage ou la saturation des télécommunications.

Le piégeage peut également consister à introduire subrepticement un équipement pirate au sein d'un système, en supplément ou en lieu et place d'un matériel existant.

Ce type d'attaques peut se faire moyennant un investissement important et nécessite la possibilité d'accéder physiquement (au moins un fois) à l'un des éléments du système ainsi la possibilité d'accéder physiquement (au moins une fois) à l'un des éléments du système ainsi que de bonnes connaissances et en théorie du signal ; ces attaques semblent encore réservées aux "professionnels" de la fraude, mais le prix des matériels, en constante diminution et leur facilité d'utilisation grandissante permettent de penser qu'ils seront prochainement à la portée d'un grand nombre.

- **3.3 Attaques informatiques**

Tout système d'information comporte peu ou prou une partie informatique, évidente (ordinateur, centre de calcul,...) ou plus subtile (microprocesseurs, microcodes,...), également susceptible de devenir une cible.

A ce niveau, l'exploitation de faiblesses connues est essentielle ; il peut s'agir du contournement d'un contrôle effectué par un logiciel ou un mécanisme quelconque, l'usurpation d'une identité offrant des privilèges accrus, ou toute autre action ; une liste exhaustive ne peut être envisagée, tant les systèmes sont multiples et différents, et tant l'imagination des attaquants et leurs connaissances en la matière sont importantes.

Les moyens nécessaires sont bien évidement en relation directe avec l'importance de la faiblesse exploitée, mais l'on s'aperçoit que l'investissement consenti n'est jamais très important ; la connaissance du système en place est en revanche primordiale, ainsi que la possibilité d'y accéder physiquement ou logiquement.

- **3.4 Attaque par virus, bombes, etc...**

Parmi les attaques informatiques, certaines ont un caractère particulier qu'il convient d'analyser plus précisément ; tout d'abord, il convient de bien différencier les diverses attaques dont il est question :

Les «portes dérobées» consistent en une possibilité d'accès privilégié à un système en cours de développement pour, par exemple, en faciliter la mise au point ; certaines peuvent subsister en phase d'exploitation, soit par erreur ou oubli, soit à dessein, dans un but légitime (faciliter la maintenance ultérieure) ou malveillant.

Un «cheval de Troie» est un module de programme, non documenté, permettant d'effectuer de manière détournée des opérations non prévues ; typiquement, il s'agit d'opérations non destructrices, visant à s'approprier des informations auxquelles l'on n'a pas accès (mots de passe en particulier) ; ce module logiciel s'effectue à chaque fois que le programme qui le supporte est lancé.

Une bombe logique est également un module de programme non documenté, mais dont le but est essentiellement destructif (informations et parfois matériels) ; cette bombe logique ne se déclenche que lorsque certaines conditions, bien définies par le programmeur, sont remplies ; son action est brève et généralement définitive.

Virus et ver sont similaires sous de nombreux aspects ; tous deux sont des modules logiciels non documentés, porteurs d'une bombe logique ; ils ont la faculté soit de se reproduire en de nombreux exemplaires (virus) soit de se déplacer d'un programme à un autre (ver) ; après une phase d'installation, de reproduction ou de déplacement, durant laquelle ils passent généralement inaperçus, et lorsque les conditions définies pour l'«explosion» de la bombe logique qu'ils ont en leur sein sont remplies, virus et ver deviennent alors actifs ; l'action de la bombe logique est également généralement brève et définitive.

Quel que soit le type du système d'information dont il est question, la «contamination» initiale par des programmes de ce type peut se faire de deux manières différentes :

- - par programmation directe, ce qui impose que l'attaquant dispose d'un accès logique au système et de bonnes connaissances en programmation,
- - par l'introduction dans le système, accidentelle ou volontaire, à l'aide d'un support matériel (média) ou par le biais des réseaux, de logiciels déjà infestés, ce qui impose là également de disposer d'un accès physique ou logique au système.

Dans l'un et l'autre cas, les moyens à mettre en œuvre sont négligeables, et le temps nécessaire faible, pour des effets qui peuvent être dévastateurs.

- **3.5 Attaques sur les réseaux**

A cause de leur ouverture sur le monde extérieur, les réseaux constituent une voie de pénétration privilégiée ; ils peuvent, ainsi qu'il a déjà été dit, être l'objet d'attaques de type TEMPEST ou être le moyen initial d'introduction de logiques infestées.

Outre ces deux aspects, il faut également insister sur le fait que l'attaque par le réseau permet d'une part d'agir à distance, et donc de conserver l'anonymat, et, d'autre part, d'utiliser les faiblesses connues d'un système pour attaquer un système différent connecté au premier ; les média se sont fait l'écho de telles actions où des systèmes interconnectés ont été l'objet d'intrusions effectuées ainsi de proche en proche.

On distingue deux types d'intrusion selon les effets attendus par l'attaquant : l'intrusion passive, qui affecte la confidentialité des informations et consiste à écouter ce qui transite sur le réseau, et l'intrusion active, dans laquelle le but est de se faire passer pour un utilisateur autorisé, de modifier ou détruire des informations ou d'attenter à la continuité de service du système.

Les moyens nécessaires peuvent nécessiter, suivant le cas un investissement négligeable (minitel) minime (enregistreur ou réémetteur) ou plus important (analyseur de fréquences) ; en tout état de cause, une bonne connaissance des systèmes visés est nécessaire et un temps non négligeable peut être utilisé par l'attaquant pour aboutir à ses fins.

- **3.6 Attaques sur les systèmes de conception**

L'attaque sur les systèmes de conception consiste à intervenir dès que possible sur tout ou partie du système ; les phases qui se succèdent (définition du besoin, spécifications, conception, industrialisation, tests fonctionnels, validation,...) peuvent être l'objet d'attaques diverses.

Pour un logiciel, il peut s'agir de l'introduction d'un «Cheval de Troie» ou d'une bombe logique, mais également d'une mauvaise définition des besoins, en particulier ceux de la sécurité, réduisant le nombre de mécanismes à implanter.

En ce qui concerne les matériels, la modification du masque d'un circuit intégré, par exemple, peut entraîner l'implantation de fonctions cachées, utilisables ensuite par un complice ; une erreur

d'industrialisation peut, malgré les tests, induire des erreurs, dont l'effet ne se fera ressentir que lorsque le système sera opérationnel.

- **3.7 Attaques physiques**

Les attaques physiques enfin regroupent toutes celles relevant du banditisme traditionnel ou du terrorisme et qu'il est inutile de rappeler, mais également certaines spécifiques aux particularités des systèmes d'information.

Parmi celles-ci, le vol de supports d'informations, se répand de plus en plus, soit pour divulguer leur contenu à une firme concurrente, à la presse,..., soit pour effectuer des menaces de divulgation ou de destruction, tant il est vrai que les informations représentent actuellement une valeur des plus importantes.