SUJET N° 4 :

Présentez le projet de construction à réaliser sur cette parcelle située en zone B du règlement d'urbanisme joint au sujet et exposez la problématique d'une telle réalisation.

DÉCIDE :

Article 1er.— Est autorisé le versement à la fondation Singer-Polygnac d'un fonds de concours de *Quatre cent mille* (400.000) francs représentant la participation du territoire à l'édification d'un mur de protection contre la mer aux abords du musée Paul Gauguin de Papeari.

Art. 2.— La dépense est imputable au budget local d'équipement, chapitre 44, article 1, exercice 1967.

Art. 3.— La présente décision sera enregistrée, communiquée et publiée partout où besoin sera.

Papeete, le 7 février 1967.

Pour le gouverneur en tournée :
Le secrétaire général,
R. LANGLOIS.

REGLEMENT D'URBANISME

ARTICLE 1

Champ d'application

Le règlement d'urbanisme fixe, dans les conditions prévues au livre 1 de la délibération n° 61-44 du 8 avril 1961 publié au J.O.P.F. du 3 juin 1961, les règles générales d'aménagement applicables sur le territoire :

— de la commune de Papeete
— du district de Pirae
— de la partie du district d'Arue limitée à l'Est par le ruisseau Puooro.

Ce règlement s'applique à toutes les opérations immobilières quelle qu'en soit la nature et l'importance à savoir :

— toutes constructions neuves, transformations ou agrandissements de bâtiments existants
— tous projets de lotissements ou de grands ensembles
— projets de l'administration ou des services publics
— tous travaux de terrassements (remblais, déblais, réalisation de terrasses,.....)
— tous tracés de voies nouvelles
— achat — échange — partage — remembrement — concession maritime, etc,. . . .).

Les situations existantes resteront acquises tant qu'elles ne tendent pas à se transmettre lors d'une des opérations ci-dessus, ou tant qu'elles ne représentent pas une gêne sérieuse pour l'intérêt public.

Dans ce cas, l'aliénation des privilèges pourra être effectuée mais devra être justement dédommagée par la puissance publique soit :

— par achat à la valeur vénale des immeubles frappés de servitude (construction + terrains)
— par échange à l'amiable à valeur et avantages égaux au choix du propriétaire.

Un décret précisera les modalités de ces acquisitions pour utilité publique.

ARTICLE 2

Division du territoire en zônes

Le territoire visé à l'article 1, comporte :

— une zône d'habitation
— une zône industrielle.

La zône d'habitation se divise en trois secteurs :

— Secteur A secteur du site portuaire
— Secteur B
— Secteur B'

Ces secteurs sont délimités de la façon suivante :

— Secteur A ligne pointillée avec des cercles
— Secteur B ligne pointillée avec des carrés.

La zône industrielle est constituée par l'ensemble des terrains figurés au plan d'aménagement au moyen de hâchures disposées en losanges.

Elle se divise en quatre secteurs :

— Secteur E vallée de Tipaerui
— Secteur F secteur du site portuaire
— Secteur G secteur artisanal et commercial
— Secteur H vallée de Fautaua.

Ces secteurs sont représentés de la façon suivante :

— Secteur E, F et H : hâchures doubles
— Secteur G : hâchures simples croisées.

CHAPITRE I

DISPOSITIONS RELATIVES AUX ZONES D'HABITATION

ARTICLE 3 H

Nature des constructions
Constructions interdites

La zône d'habitation est constituée par les parties du territoire visées à l'article 1 où le groupement des habitations, des commerces et des constructions destinés à abriter les activités qui sont le complément naturel de l'habitation, doit être maintenu, développé ou créé.

Sont autorisés entre autre :

— les magasins de vente
— les petits ateliers de réparations, petits entrepôts (ne dépassant pas 100 m2)
— les édifices religieux ou de loisirs
— les buvettes, etc, . . .
— les bureaux, agences, . . .

Dans cette zône, sont interdits les établissements et les constructions qui de par leur destination, leur nature, leur importance ou leur aspect, sont incompatibles avec la salubrité, la tranquillité, la sécurité ou la bonne tenue d'un quartier d'habitation.

L'agrandissement ou la transformation des établissements industriels ou dépôts existants dont la création serait interdite dans la zône d'habitation ne peuvent être autorisés qu'à titre exceptionnel, si leur importance ne modifie pas le caractère de la zône et lorsque les travaux envisagés doivent avoir pour effet de réduire la gêne ou le danger qui résultent de la présence de ces établissements ou dépôts.

En tout état de cause, les établissements industriels ou dépôts existants devront, dans un délai de 5 ans à compter de la promulgation du présent règlement, être transférés dans une zône à caractère industrielle.

ARTICLE 4 H

Forme et dimension des parcelles

Conditions d'utilisation du sol (surfaces couvertes)

Si la surface ou la configuration d'une parcelle est de nature à compromettre l'aspect ou l'économie de la construction

y édifier, ou la bonne utilisation des parcelles voisines, le permis de construire peut être refusé ou subordonné à un remembrement préable.

Les surfaces, dimensions minima ainsi que les maxima des *surfaces couvertes* autorisées (1) sont définies dans le tableau ci-dessous :

	Zône A	Zône B	Zône B'	Observation
— dimensions minima des lots		20 m	20 m	
— surface minima des lots		400 m2	400 m2	
Total des surfaces couvertes autorisées	~~40 %~~ ~~80 %~~	50 %	~~50 %~~ ~~20 %~~	lots de formes simples.

ARTICLE 5 H

Création d'ensembles — Remembrement — Lotissements

Dans les secteurs où existe une majorité de constructions vétustes et mal implantées, la construction ou l'extension de tout bâtiment existant peuvent y être interdites ou subordonnées à l'établissement d'un projet d'ensemble. Les projets d'ensembles feront l'objet d'études d'aménagement de détail. Jusqu'à l'approbation des plans d'urbanisme de détail correspondants, il peut être sursis à la délivrance des permis qui seraient de nature à compromettre ou à défavoriser l'aménagement des parties du territoire considérées.

Un remembrement parcellaire préable peut-être prescrit dans les conditions prévues aux articles 32 et 33 du code d'aménagement du territoire.

Les lotissements effectués après la promulgation du présent règlement devront respecter l'ensemble des prescriptions et notamment les dimensions et superficies minima, les largeurs des voies privées, l'assainissement, . . . la vente pouvant être annulée d'office en cas de non respect d'une de ces règles. (article 57 du code d'aménagement).

ARTICLE 5 H bis

Zône de parkings

La zône A' délimitée par les rues Colette, Bonnard et du Maréchal Foch est destinée à devenir une zône de parkings à rez-de-chaussée. A l'intérieur de cette zône des immeubles sur pilotis pourront être édifiés à condition que, exception faite des accès et des départs d'escaliers, etc,... la totalité du rez-de-chaussée soit réservée au parcage des voitures.

En dehors de cette servitude, les immeubles devront répondre aux règles d'édification spécifiques à la zône A.

ARTICLE 6 H

Desserte par les voies

Les emprises des voies principales et secondaires sont définies sur le plan d'urbanisme.

En dehors de ces voies, tous les logements ou lotissements doivent être correctement desservis.

Le permis de construire pourra être refusé pour les terrains qui ne seraient pas desservis par des voies publiques ou privées dans des conditions répondant à l'importance et à la destination de l'immeuble ou de l'ensemble d'immeubles qui y sont édifiés, notamment en ce qui concerne la commodité de la circulation et des accès, permettant notamment les manœuvres des voitures des services publics (pompiers, ramassage des ordures, . . .).

Les culs de sac devront être aménagés en rond point ou en Y pour permettre de faire facilement demi-tour ceci sans rentrer dans les propriétés privées.

L'ouverture de voies privées carrossables est soumise aux normes suivantes :

— voies de desserte secondaires :
(jusqu'à 10 logements)
— 6 m d'emprise : chaussée : 5 m)
accotement : 1 m)

— voies de desserte primaire :
(jusqu'à 50 logements)
— 8 m d'emprise : chaussée : 6 m)
accotements : 2 m)

— voie de liaison :
(au-dessus de 50 logements)
— 10 m d'emprise minima : chaussée : 8 m)
accotement : 2,00 m)

Toutes les routes doivent être exécutées suivant les règles de l'art, tant au point de vue du confort que de la sécurité et de l'hygiène. A cet effet la pente longitudinale maximum ne devra en aucun cas dépasser 16%. Les sections de raccordements de ces voies sur des voies principales devront être de faible pente (7 % sur au moins 30 m).

Des dérogations peuvent être accordées exceptionnellement et sur justification détaillée pour les routes de montagnes nécessitant des travaux trop importants.

ARTICLE 7 H

Réserve d'emplacements pour le stationnement des véhicules

La délivrance du permis de construire peut être subordonnée à la prévision d'aménagements permettant le stationnement hors des voies publiques des véhicules à deux ou à quatre roues, correspondant aux besoins de l'immeuble à construire.

Les parkings (1) nécessitant des manœuvres susceptibles de déborder sur les routes principales sont interdits. L'accès de ces parkings à la voie principale devra se faire normalement et toujours en marche avant.

1 — Zône A

Des parkings, garages, etc... devront être prévus et notamment pour les véhicules appartenant aux propriétaires ou locataires des constructions ainsi que pour les engins du personnel : on devra chercher à implanter ces emplacements dans les cours intérieurs, etc... et jamais sur la voie publique elle-même. Il sera utile que les constructeurs étudient des solutions avec les propriétaires voisins, notamment en ce qui concerne les sorties sur la voie, etc...

De toute manière il devra être prévue : 1 aire de stationnement par magasin plus 1 aire par logement ceci en dehors de la voie publique.

2 — Zône B et B'

21 — Habitations

Par logement : (quelque soit son importance) au minimum 1 aire de stationnement voiture (garage ou parkings). Pour

(1) *Surfaces couvertes* : ensemble des surfaces définies par le contour extérieur des toitures de toutes les constructions, y compris les annexes - projetées sur le plan horizontal.

(1) Dimensions normales des parkings : 2,20 x 5,00 m.

les habitations individuelles et villas, l'emplacement d'un garage devra être prévu dans le plan d'implantation, même s'il n'est pas réalisé tout de suite.

22 — Bureaux

1 emplacement de stationnement par bureau

3 — Commerces — divers

Minima 4 emplacements pour les clients - la surface de stationnement devra être égale ou supérieure à l'ensemble des surfaces commerciales, (magasin+annexes) - un garage au moins devra être prévu pour la ou les voitures personnelles du commerçant et le cas échéant des emplacements pour le personnel et les voitures de livraison.

4 — Edifices publics ou communautaires

des emplacements suffisants devront être prévus.
(1 parking pour 5 places assises.)

5 — Les garages collectifs

(box) à caractère commercial et les garages prévus pour les camions ne peuvent être établis en bordure d'une voie à grande circulation ou d'une voie de largeur égale ou supérieure à 10 m, sauf dispositions spéciales à prendre en vue de n'apporter aucun trouble à la circulation.

6 — Les groupes de garages individuels

doivent être disposés dans les parcelles de façon à ménager des possibilités d'évolution, et de ce fait ne présenter qu'un seul accès sur la voie publique ou commune.

7 — Les commerces ou autres établissements existants

recevant du public, et pour lesquels le stationnement des voitures crée une gêne même temporaire devront créer dans les 12 mois après l'approbation du présent règlement des emplacements de stationnement suffisants à leur bon fonctionnement.

ARTICLE 8 H

Implantation des constructions en bordure des voies

1) — Secteur A — Il y a obligation de recul sur alignement à rez-de-chaussée (formant galerie) dans tout le secteur.

recul sur alignement au R. de CH. 3,50 m.

— quai Bir Hackeim
— quai de l'Uranie
— quai du Commerce.

recul sur alignement au R. de CH. 3,00 m.

— toutes les autres voies, y compris la rue des Remparts.

La face externe des piliers des galeries devra se trouver à 0,25 mètre de l'alignement.

A l'intersection des voies, les bâtiments devront réserver un pan coupé de 5 mètres de longueur sur toute la hauteur du rez-de-chaussée.

2) — Secteurs B et B' — Il y a obligation de recul sur alignement de 5 mètres, le long de toutes les voies et chemins des secteurs B et B'.

Il est bien entendu que ces zônes de recul restent la propriété des riverains et peuvent être aménagées en jardin, pièces d'eau,... à l'exclusion de tout ouvrage important. Les haies et clôtures pourront être mises en place sur l'alignement même.

A l'intersection des voies, les constructions (zône A) ou les limites de propriétés zônes B et B' devront réserver un pan coupé de 5 mètres de longueur. Ce pan coupé sera tracé sur une perpendiculaire à la bisectrice formée par les 2 façades formant l'angle.

ARTICLE 9 H

Implantation des constructions par rapport aux limites séparatives.

La distance horizontale de tout point d'un bâtiment au point le plus proche de la limite parcellaire doit être au moins égale :

— à 4 mètres et jamais inférieure à la hauteur du bâtiment diminuée de 4 m, sous préjudice des dispositions particulières applicables aux bâtiments en matériaux inflammables

Toutefois :

Dans le secteur A

1) — la construction en limite de propriété *est obligatoire* en façade et notamment pour la galerie couverte qui ne devra en aucun cas présenter d'interruptions le long de la voie, et permettre un cheminement continu à l'abri du soleil et de la pluie.

2) — à l'intérieur d'une bande de 15 m de profondeur à partir de l'alignement ou de la limite de construction qui s'y substitue, la construction de bâtiments joignant la limite séparative est acquise d'office (aucune autorisation à obtenir des voisins). Si le bâtiment ne joint pas la limite séparative, les façades latérales percées de baies servant à l'éclairement des pièces d'habitations doivent être écartées d'une distance au moins égale à la moitié de leur hauteur au-dessus du sol. Si ces façades ne sont pas percées de baies servant à l'éclairement des pièces d'habitation, leur distance aux limites séparatives peut être réduite au tiers de leur hauteur. *Dans les deux cas, un minimum de 4 m sera exigé.*

3) — à l'extérieur de cette bande, la construction de bâtiments joignant la limite séparative est autorisée à condition que leur hauteur totale n'excède pas 4 mètres.

Dans les secteurs B et B'

La construction de bâtiments joignant la limite parcellaire peut être autorisée sous les deux réserves suivantes :

1) — lorsque les propriétaires voisins sont d'accord pour édifier des bâtiments jointifs ; les dimensions doivent alors être sensiblement équivalentes.

2) — s'il n'en résulte pas pour la parcelle voisine une privation d'ensoleillement, pour des bâtiments de faible importance dont la hauteur total n'excède pas 5 mètres.

Dans le cas où les constructions ne joignent pas la limite de propriété, le recul minimum sera de :

— 1 ou 2 niveaux : 4,00 m
3 niveaux : 6,00 m

ARTICLE 10 H

Implantation des constructions sur un terrain appartenant à un même propriétaire

Cet article ne concerne que les projets de construction sur des terrains non destinés à être morcelés ultérieurement quelle que soit la forme de la division (partage, lotissement,...).

Dans le cas où les constructeurs prévoient un morcellement ultérieur éventuel, ils devront respecter l'ensemble de la réglementation et notamment les surfaces minima des lots etc...

1) — Entre un bâtiment principal et ses annexes non contigus, doit toujours être ménagée une distance suffisante

pour permettre l'entretien facile des marges d'isolement et des bâtiments eux-mêmes et, s'il y a lieu, le passage et le fonctionnement du matériel de lutte contre l'incendie.

Cette distance sera au moins égale aux reculs par rapport aux limites de propriétés énoncés à l'article *9 H*.

	1 niveau	2 niveaux	3 niveaux
Zône B	4.00 m	4.00 m	6.00 m
Zône B'	4.00 m	4.00 m	6.00 m

2) — Entre un bâtiment et un bâtiment voisin, principal ou non, doit toujours être ménagée une distance suffisante pour assurer un minimum d'isolement aux vues, bruits, etc...

Cette distance sera au moins égale à 2 fois le recul par rapport à la limite de propriété énoncé à l'article *9 H*. C'est l'immeuble le plus élevé qui détermine la distance séparative minimum dans le tableau ci-dessous.

Immeubles	1 niveau	2 niveaux	3 niveaux
Zône B	8.00 m	8.00 m	12.00 m
Zône B'	8.00 m	8.00 m	12.00 m

3) — Les constructions qui ne sont pas à usage d'habitation, telles que magasins, bureaux, annexes, etc.... sont soumises aux mêmes règles d'espacement.

4) — Les logements jumelés sont tolérés mais ne pourront en aucun cas être vendus séparément ou appartenir à deux propriétaires différents au moment de la construction.

ARTICLE 11 H

Implantation des constructions par rapport au bord de mer

Le recul des constructions sur le bord de mer (ligne de séparation entre les terres et le lagon en période des plus hautes eaux) devra être :

— immeuble à 1 niveau : 10 m
— immeuble à 2 ou 3 niveaux : 15 m

Seules les constructions ayant un caractère communautaire et touristique, et pour lesquelles existe une nécessité justifiable, pourront être implantées sur le bord de mer (clubs nautiques....).

Les accessoires directement liés à la mer tels que jetées, marinas, bassins, plongeoirs, etc... sont autorisés sur la limite même.

ARTICLE 12 H

Hauteur des constructions

1°) Hauteur des constructions par rapport à la largeur des voies :

dans les secteurs A et A'

La différence de niveau entre tout point d'un bâtiment et tout point de l'alignement opposé ne doit pas excéder la distance comptée horizontalement entre ces deux points augmentée de la moitié de ladite distance, sans que ce supplément puisse excéder 5 mètres.

$$(H = L + \frac{L}{2} \text{ : } L \text{ inférieur ou égal } 5 \text{ m.})$$

dans les secteurs B et B'

La différence de niveau entre tout point d'un bâtiment et tout point de l'alignement opposé ne doit pas excéder la distance comptée horizontalement entre ces deux points (H=L). Une tolérance de 2 mètres est admise lorsque la hauteur calculée comme il est indiqué au paragraphe 1er et 2e ci-dessus ne permet pas d'édifier un nombre entier d'étages droits. La même tolérance est admise pour les murs pignons, ventilations, saillies et autres éléments de la construction reconnus indispensables.

S'il existe l'obligation de construire en retrait de l'alignement, la limite de ce retrait se substitue à l'alignement.

Dans le cas de voies privées, la limite effective de la voie privée se substitue à l'alignement.

Lorsque les voies sont en pente, les façades des bâtiments sont divisées, pour le calcul de la hauteur en sections dont aucune ne peut excéder 30 m de longueur. La cote de hauteur de chaque section est prise au milieu de chacune d'elle.

Si la distance entre deux voies d'inégale largeur ou de niveaux différents est inférieure à 15 m la hauteur de la construction édifiée entre les deux voies est régie par la voie la plus large ou de niveau le plus élevé.

Lorsque la construction est édifiée à l'angle de deux voies d'inégale largeur, il est admis que, sur une longueur qui n'excède pas 15 m le bâtiment édifié sur la voie la plus étroite puisse avoir la même hauteur que sur la voie la plus large.

2°) Limitation absolue de la hauteur des constructions.

La hauteur des constructions, non comptés les toitures, murs pignons, ventilations, saillies et autres éléments de la construction reconnus indispensables, ne peut excéder :
dans les secteurs A et B, 11 mètres+1 étage en retrait suivant H=L
dans le secteur B', 7 mètres+1 étage en retrait suivant H=L.

Toutefois dans les programmes de constructions groupées, dans les projets de lotissement et dans les projets d'ensemble visés à l'article 7 H, la hauteur des constructions peut excéder cette limite ; elle est alors fixée, après avis de la section spéciale du projet de construire en considération de l'environnement général et des nécessités d'architecture propres au groupe et à l'ensemble considéré.

Dans le secteur A, certaines constructions sont soumises à une servitude spéciale d'architecture. Elles sont indiquées au plan d'aménagement par une bande continue de triangles noirs (cf art. *17 H*).

ARTICLE 13 H

Alimentation en eau et assainissement

L'alimentation en eau potable et l'assainissement de toute construction à usage d'habitation et de tout local pouvant servir, de jour et de nuit, au travail, au repos et à l'agrément, ainsi que l'évacuation, l'épuration et le rejet des eaux résiduaires industrielles, doivent être assurés dans des conditions conformes aux règlements en vigueur aux prévisions des avant-projets d'alimentation en eau potable et d'assainissement, et aux prescriptions particulières ci-après :

— Les lotissements et ensembles d'habitations doivent être desservis par un réseau de distribution d'eau potable sous pression et par un réseau d'égoûts évacuant directement et sans aucune stagnation les eaux usées de toute nature.

— Ces réseaux sont raccordés aux réseaux publics du quartier où est établi le lotissement ou l'ensemble d'habitation.

— En l'absence de réseaux publics :

1) le réseau de distribution d'eau potable est alimenté par un seul point d'eau ou, en cas d'impossibilité démontrée, par le plus petit nombre possible de points d'eau.

2) le réseau d'égoûts aboutit à un seul dispositif d'épuration et de rejet au milieu naturel ou, en cas d'impossibilité démontrée, au plus petit nombre possible de ces dispositifs.

POLYNESIE FRANCAISE — ILE DE TAHITI — COMMUNE DE PAPEETE

AVENUE GEORGES CLEMENCEAU
TERRE TETARAORUE /PARTIE/ SCIE. : 351.00M2

COURRIER ARRIVÉE/CCL
N° 133
DATE 13 JUIN 2001

AMENAGEMENT DU SHOW-ROOM AUTOMOBILES

COMAB
Dossier n° 01-43
Examiné en séance
du 24 OCT. 2001

POLYNESIE FRANÇAISE
Section UCC
- 5 OCT. 2001
N° AU
URBANISME

AVIS FAVORABLE
OPT/CÔLIENSIM
Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise admise par l'OPT

13 JUIN 200

MAI 2001

1. SITUATION

Le projet est situé dans la commune de Papeete, quartier MAMAO , Tahiti, Polynésie Française dans un immeuble existant, sur une parcelle de 351 m².

Le terrain se trouve en section

2. DESTINATION – PROGRAMME

L'objet des présent travaux est la réhabilitation de la charpente et de la couverture du bâtiment existant et le remplacement de la façade.
Les volumes et surfaces restent inchangées à l'exception d'une surélévation de 60 cm afin de réaliser les travaux en conservant la couverture actuelle pour la pérennité du bâtiment.
Les autres travaux sont des travaux de remise en état de second œuvre.
L'assainissement existant est en état de fonctionnement sera conservé.
Le locataire est conscient du projet d'alignement sur la voirie principale à venir.

3. REPARTITION DES SURFACES

- ***Niveau rez-de-chaussée***

– salle d'exposition ..... 191,60 m²

– sanitaires..... 3,20 m²

4. NATURE DES TRAVAUX

- ***Démolition***

- Dépose de la façade principale
- Démontage de la porte d'entrée et des menuiseries.
- Dépose de la charpente et couverture existante

- ***Gros œuvre***

Sans objet

- ***Cloison***

- Réalisation de cloisons légères

- ***Charpente et couverture***

- Mise en place d'une charpente métallique et d'une couverture en tôle nervurée pré laquée.

- ***Menuiseries extérieures***

- Châssis aluminium vitré en remplacement pour la façade principale.

- ***Peinture***

- Peinture extérieure et intérieure sur enduit ciment

- ***Plomberie, sanitaires et <u>assainissement</u>***

L'installation comprend un bloc sanitaire (WC, lavabo), le tout raccordé au système d'épuration existant.

- ***Revêtements scellés et collés***

- Revêtements de sols : carrelage grès cérame

- ***Equipements électriques***

- L'installation générale répondra à la norme C 15.100

- Les canalisations seront réalisées en conducteurs isolés sous conduits isolants encastrés. Les conduits passeront par le sol et remonteront en murs cloisons et faux plafonds.

- Le local est desservi par une ligne téléphonique.

- ***Gaines***

- Les descentes des eaux pluviales seront regroupées dans une gaine verticale.

- ***Climatisation***

- Le local sera ventilé mécaniquement.

- Ventilation des espaces communs par châssis persiennes

PAPEETE

N

PORT DE PAPEETE

Motu Uta

Gare Maritime

Fare Ute

Quai des Ferries

BOULEVARD POMARE

RUE DES REMPARTS

Vaininiore

Patutoa

Taunoa

Puea

Fariipiti

Temae

Manuhoe

Orae

Mamao

Vaiete

Farimata

Tarahoï

Orovini

Mission

Vaiami

Paofai

Ste Amélie

CHEMIN VICINAL DE TAUNOA

CHEMIN VICINA DE PATUTOA

AVENUE DU CHEF VAIRAATOA

AVENUE DU PRINCE HINOI

AVENUE DU COMMANDANT CHESSE

AVENUE GEORGES BAMBRIDGE

RUE PAUL GAUGUIN

RUE FRANCOIS CARDELLA

RUE DU 22 SEPT

RUE JEANNE D'ARC

RUE DU MARECHAL FOCH

RUE CHARLES VIENOT

RUE DU PONT NEUF

RUE DE LEVECHER

ROUTE DE LA MISSION

RUE DUMONT D'URVILLE

RUE DU COMMANDANT DESTREMEAU

ROUTE DE L'OUEST

Clinique Paofai

Clinique Cardella

Cathédrale

Temple

Mairie

Hôpital Mamao

CPS

CMAR

Dossier n° 07-43

Examiné en séance

du 24 OCT. 2001

-5 OCT. 2001

AVIS FAVORABLE

OPT-COMENOM

Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise admise par l'OPT

13 JUIN 2001

C.M.T. - C.O.M.

No 986 - 070 - 22 - 5846

Cellule Topographie

GOUVERNEMENT DE LA POLYNESIE FRANCAISE

MINISTERE de l'EQUIPEMENT, de l'AMENAGEMENT et de l'URBANISME, de l'ENERGIE et des PORTS

DIRECTION DE L'EQUIPEMENT - ARRONDISSEMENT INFRASTRUCTURE

ILE DE TAHITI

COMMUNE DE PAPEETE.
Avenue Georges CLEMENCEAU.

TERRE TETARAORUE."Partie"
Parcelle.

- ○ DELIMITATION DU DOMAINE PUBLIC
- ◉ ALIGNEMENT
- ◉ ROUTIER
- ○ FLUVIAL
- ○ MARITIME

DEMANDE DU 26.11.91

DE Mme. VAIRAAROA Frida.née TIMIONA.

ECHELLE ○ 1/200 ◉ 1/500 ○ 1/1000 ○

PAPEETE, le 29.11.91

DIRECTION EQUIPEMENT INF/TOPO POLYNESIE FRANCAISE

G. GUIDO

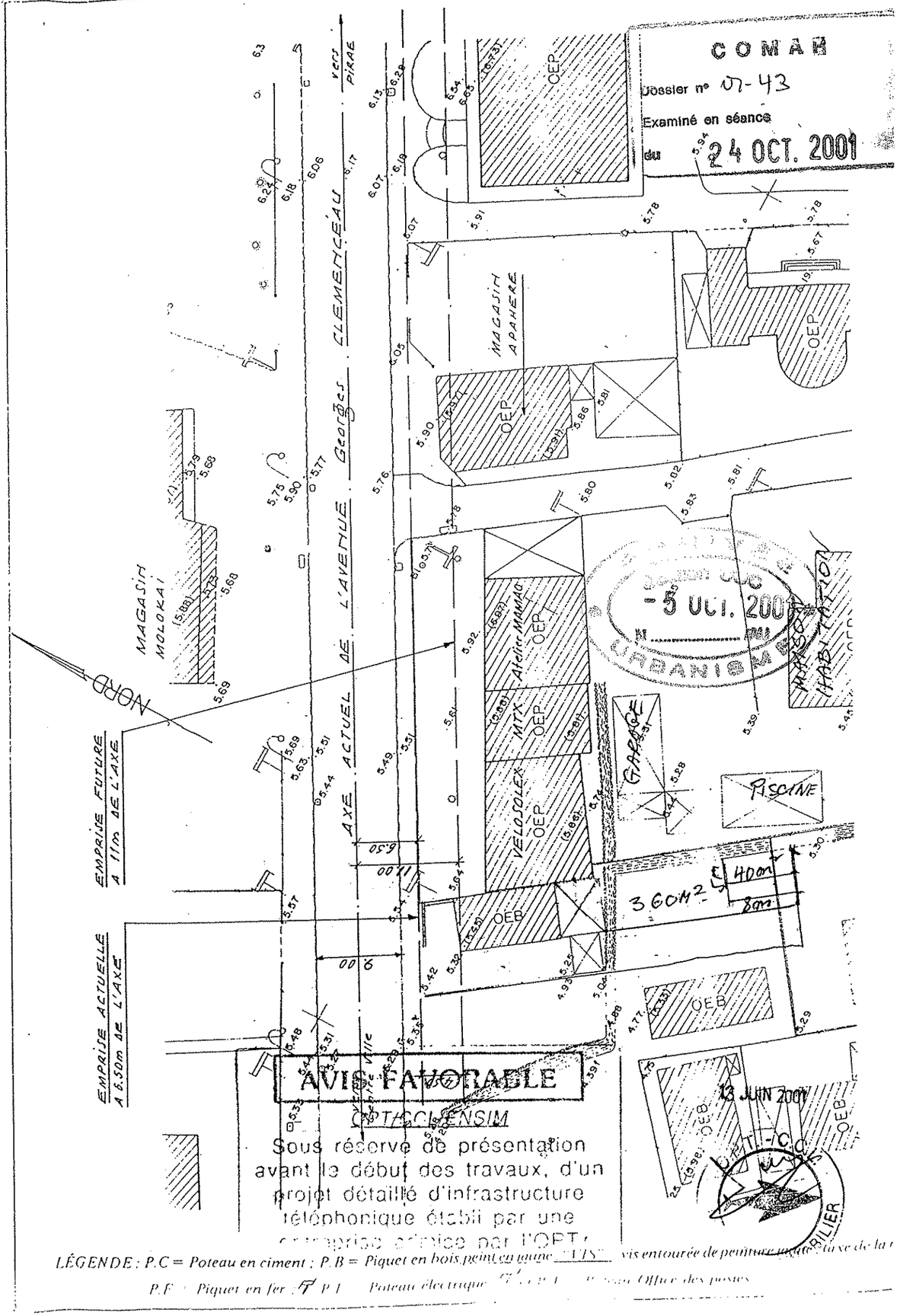
	Visa	Date
Levé		28.11.91

COMAR
Dossier n° 07-43
Examiné en séance
du 24 OCT. 2001

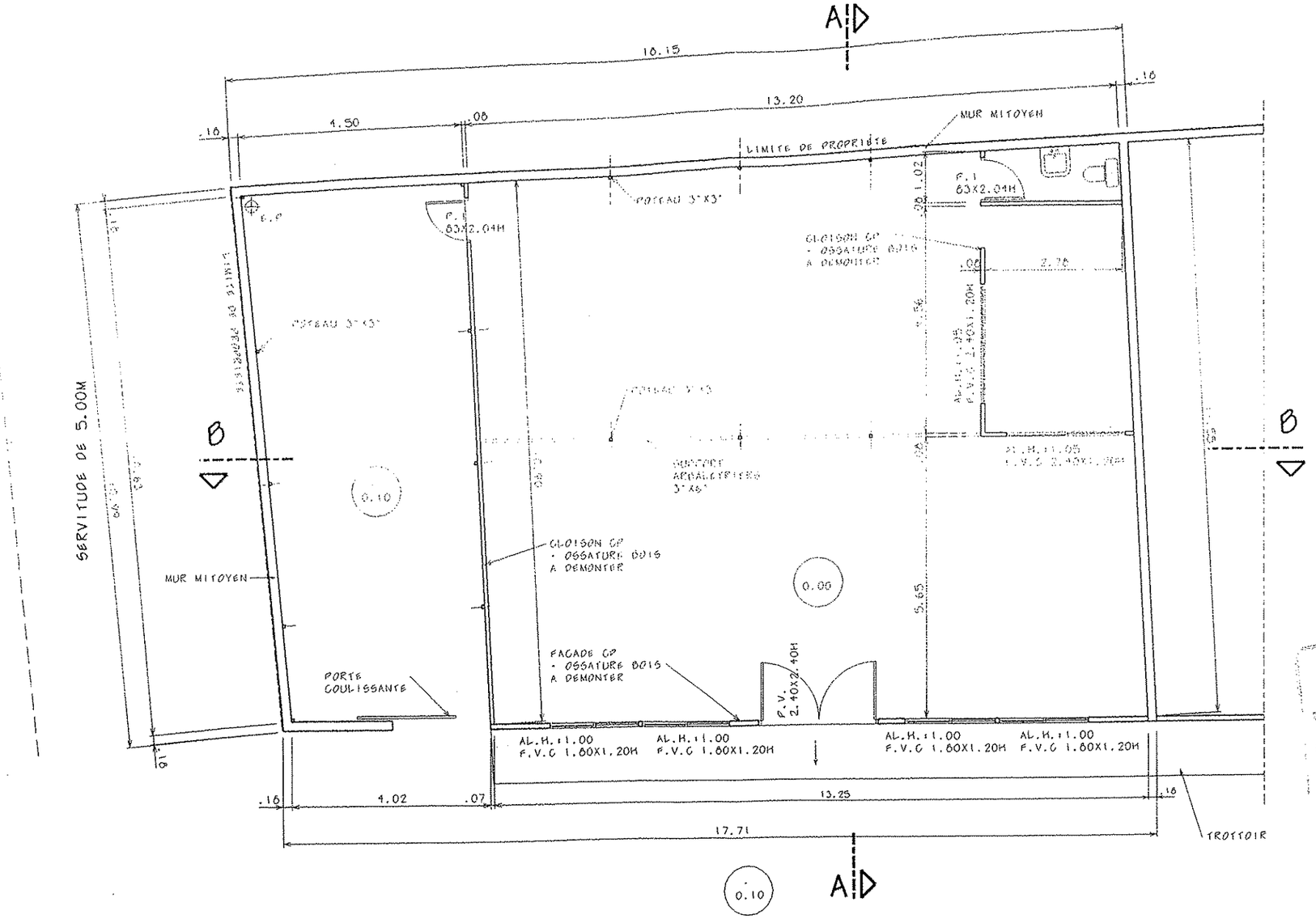
-5 OCT. 2001
PRESIDENT DE LA COMMISSION D'URBANISME

13 JUIN 2001

AVIS FAVORABLE
OPT/ACI/ENSIM
Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise agréée par l'OPT.



LÉGENDE : P.C = Poteau en ciment ; P.B = Piquet en bois peint en jaune "OPT" vis entourée de peinture jaune à la tête de la ; P.F = Piquet en fer ; P.T = Poteau électrique ; P.O = Poteau Office des postes



VUE EN PLAN /ETAT DES LIEUX/

ECH. 1:100

COMAB
Dossier n° 01-43
Examiné en séance
du 24 OCT. 2001

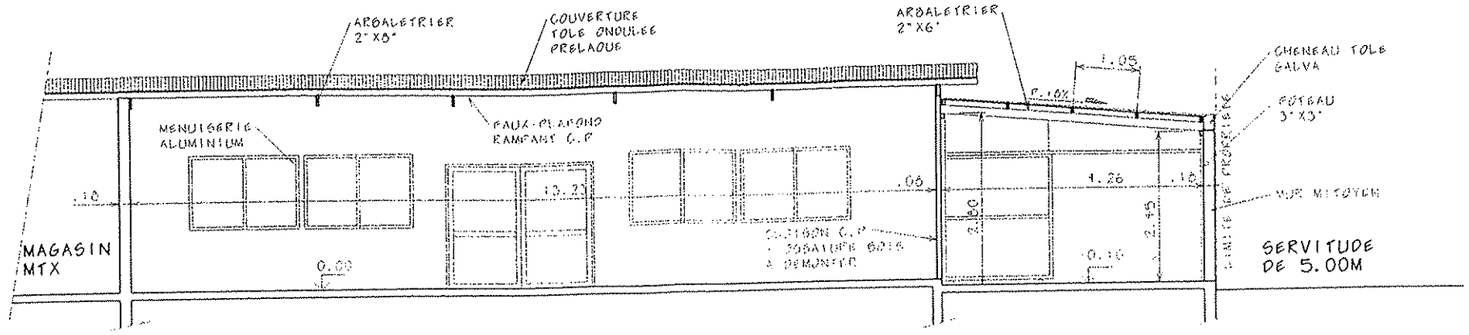
-5 OCT. 2001

AVIS FAVORABLE

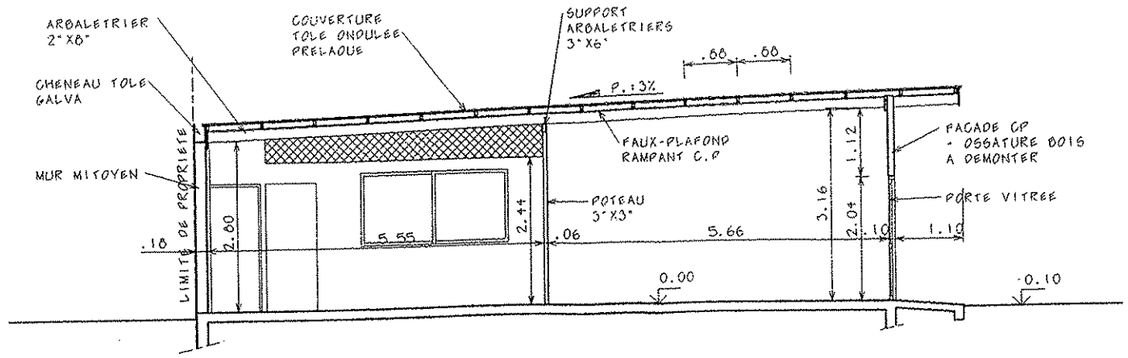
OPT/CCL/ENSIM

Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise admise par l'OPT

13 JU



COUPE BB
/ETAT DES LIEUX/

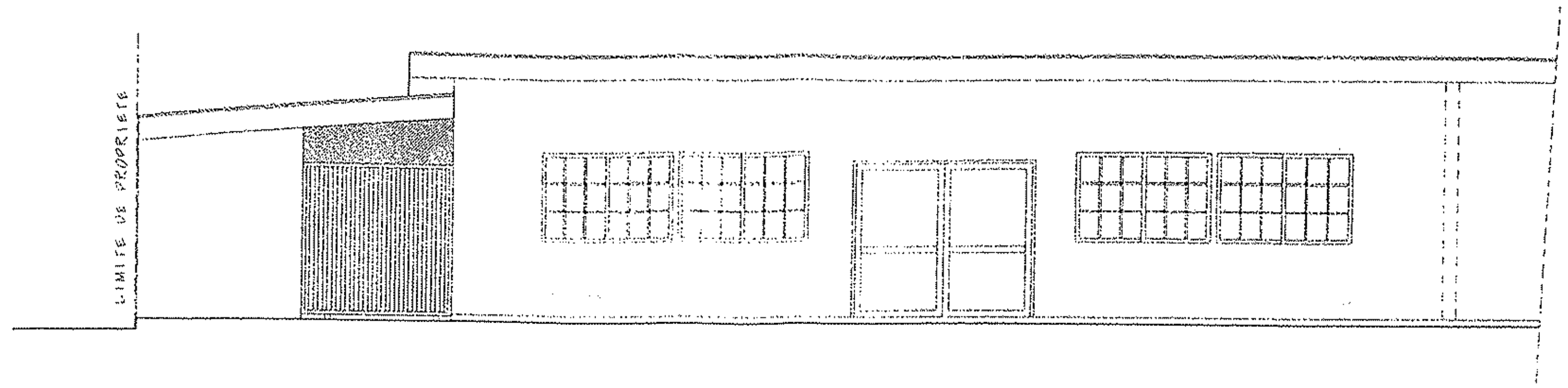


COUPE AA
/ETAT DES LIEUX/

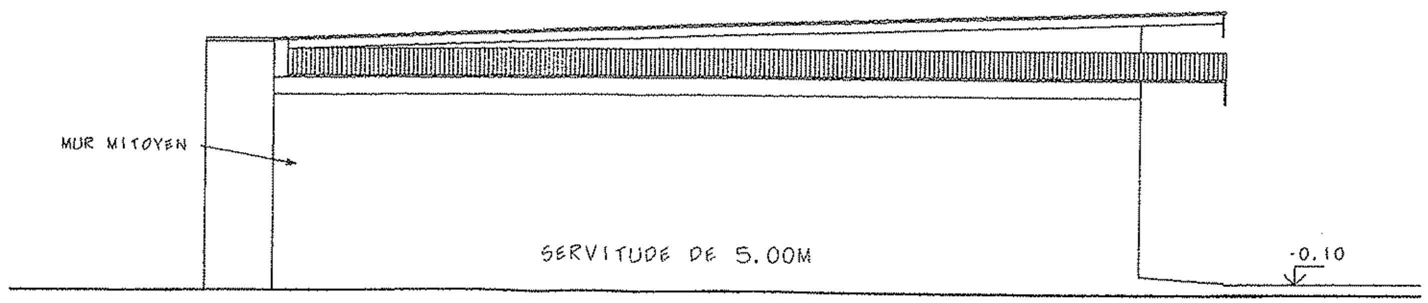
COMAR
Dossier n° 07-43
Examiné en séance
du 24 OCT. 2001

-5 OCT 2001
URBANISME

AVIS FAVORABLE
OPT/COUVENSIM
Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise admise par l'OPT



FACADE NORD-OUEST
/ETAT DES LIEUX/ ECH.:1/100



FACADE NORD-EST
/ETAT DES LIEUX/ ECH.:1/100

COMAR
Dossier n° 01-43
Examiné en séance
du 24 OCT. 2001

5 OCT. 2001
N ...... MJ
URBANISME

AVIS FAVORABLE
OPT/CCI/ENSIM
Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise admise par l'OPT

13 JUIN 200
O.P.T. - C.C.

VELOSOLEX

MAGASIN
MTX

12.94

16.15

17.65

EMPRISE FUTURE A 11.00M DE L'AXE

EMPRISE ACTUELLE A 6.50M DE L'AXE

AXE DE L'AVENUE GEORGES CLEMENCEAU

VERS CENTRE VILLE

TERRE TETARAORUE
/PARTIE/
SCIE.: 351.00M2

12.09

SERVITUDE DE 5.00M

MAGASIN
APAHERE

VERS PIRAE

COMAR
Dossier n° 01-43
Examiné en séance
du 24 OCT. 2001

DIRECTION DES SERVICES TECHNIQUES
- 5 OCT. 2001
URBANISME

AVIS FAVORABLE

OPT/CCI/ENSIM

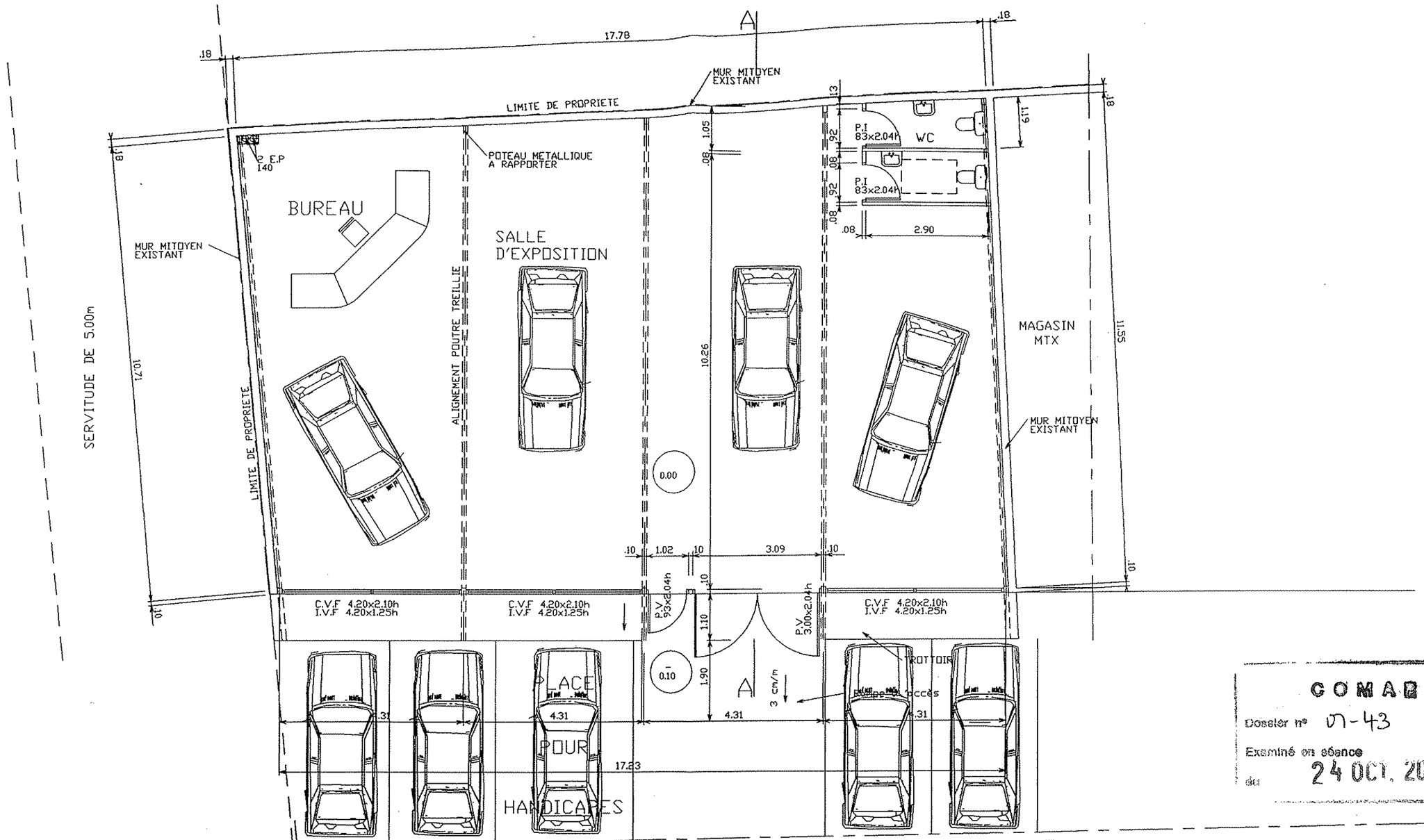
Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise admise par l'OPT

13 JUIN 2001

O.P.T. - C.C.I.

PLAN DE MASSE

ECH. 1/250

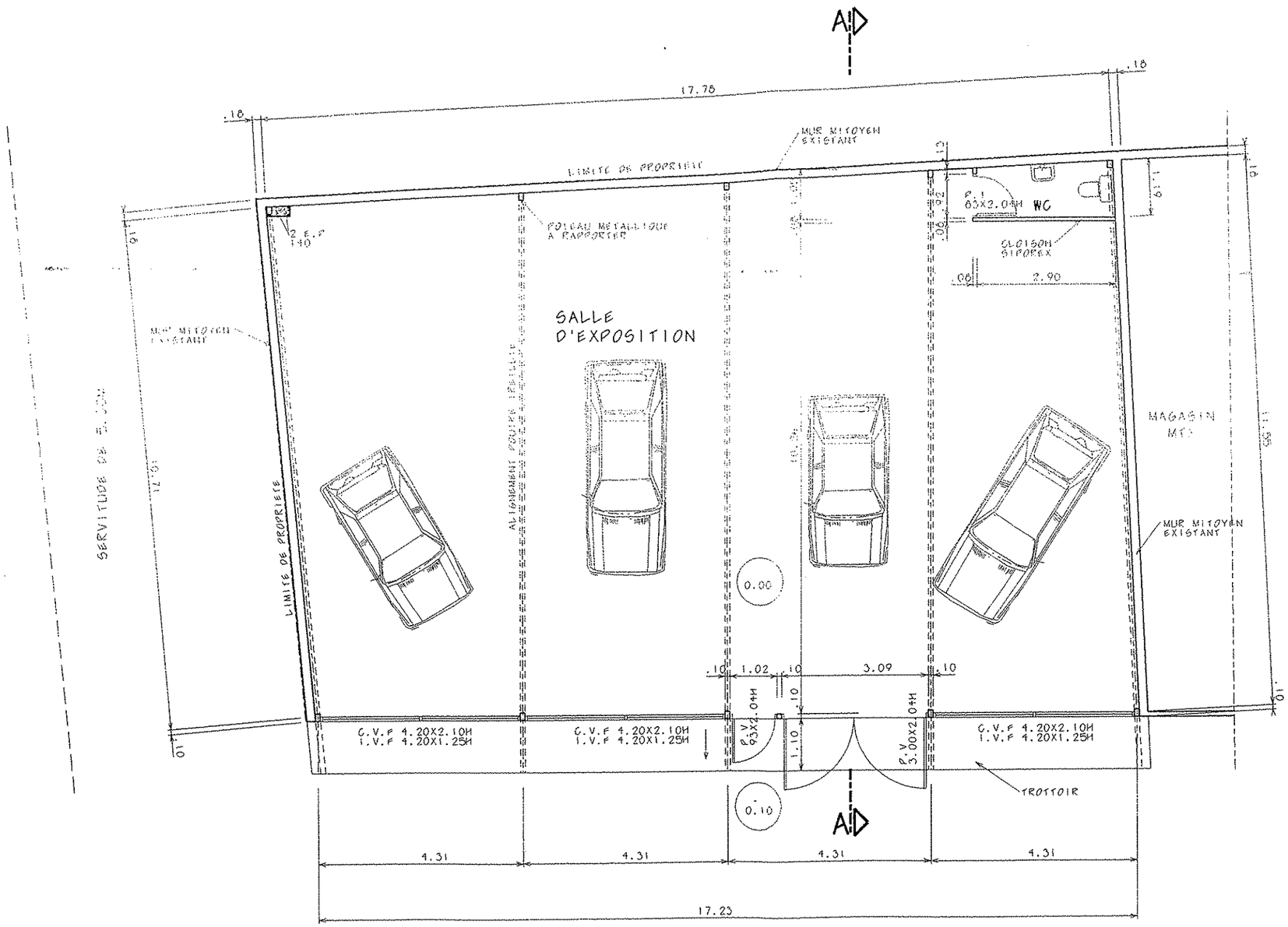


COMAB
Dossier n° 07-43
Examiné en séance du 24 OCT. 2001

5 OCT 2001
ABANDONNE

VUE EN PLAN

Echelle 1/100

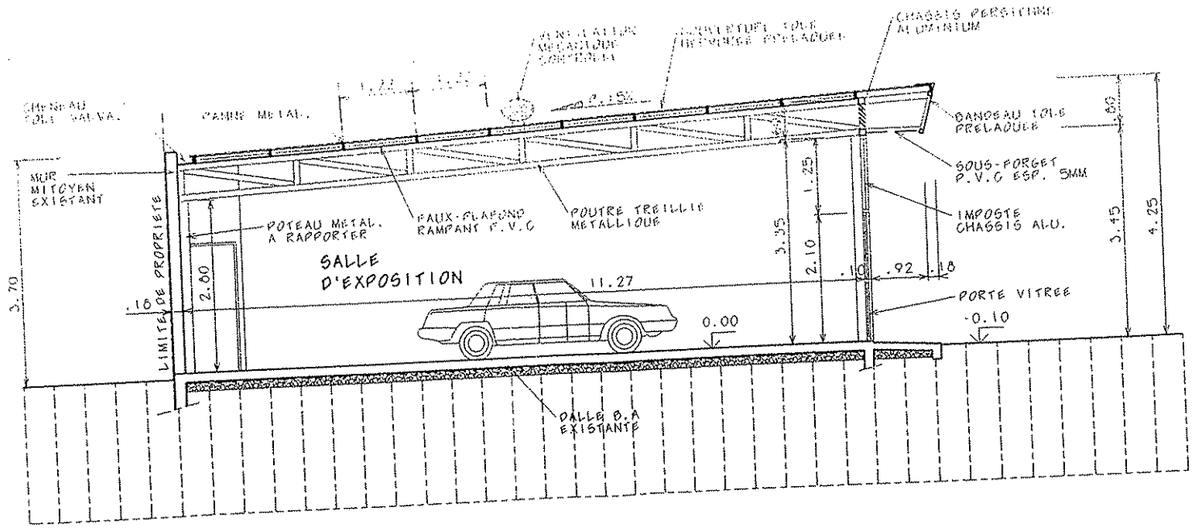


VUE EN PLAN

ECH. : 1/100

COMAR
Dossier n° 07-43
Examiné en séance
du 24 OCT. 2001

- 5 OCT. 2001



COUPE AA

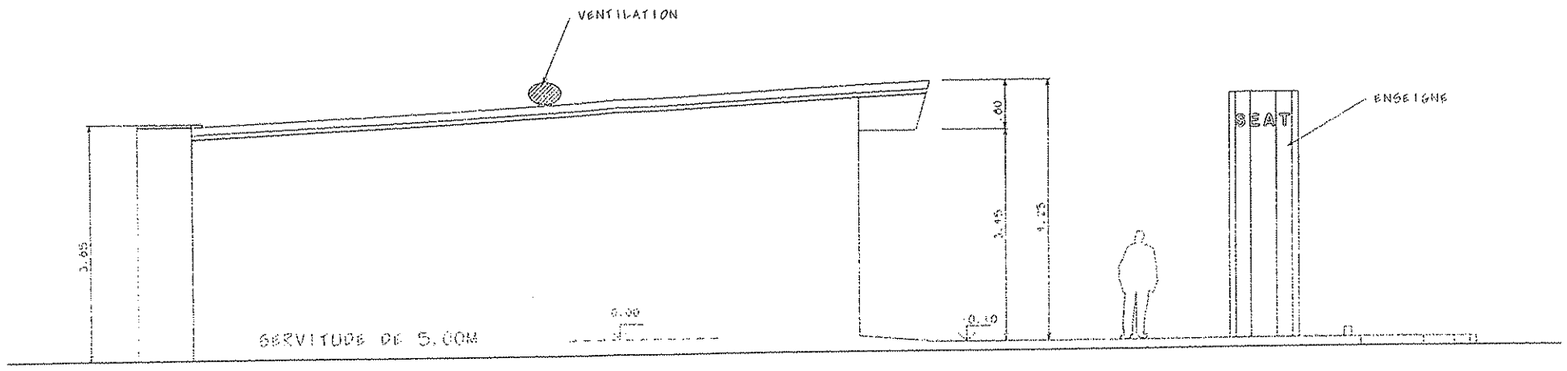
ECH. 1/100

COMAB
Dossier n° 07-43
Examiné au bureau
du 24 OCT. 2001

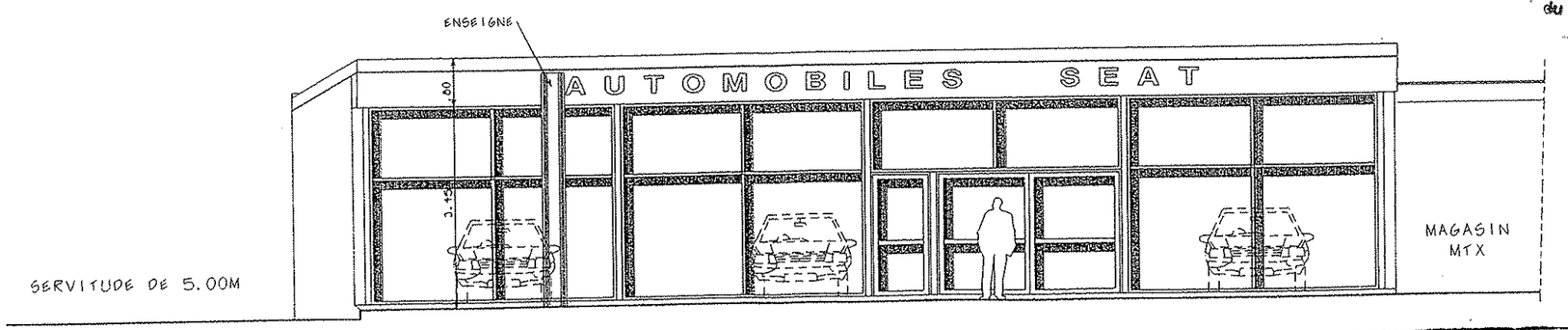
- 5 OCT. 200
au
COMMUNE

AVIS FAVORABLE
OPT/OCI/ENSIM
Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise agréée par l'OPT

13 JU



FACADE NORD-EST ECH. 1:1/100



FACADE NORD-OUEST ECH. 1:1/100

COMAB
Dossier n° 07-43
Examiné en séance
du 24 OCT. 2001

5 OCT. 2001
ORGANISME

AVIS FAVORABLE
OPT/CCL/ENSIM
Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise admise par l'OPT

13 JUIN 2001

SUJET N° 1 :

Le projet concerne la transformation et l'aménagement de salle de classe dans un bâtiment existant.
Indiquez les dispositions qui doivent être vérifiées à la demande de travaux immobiliers pour ce type d'établissement.
Dans quelles mesures ce projet peut-il être réalisé en respectant les dispositions du Code de l'Aménagement de la Polynésie Française.

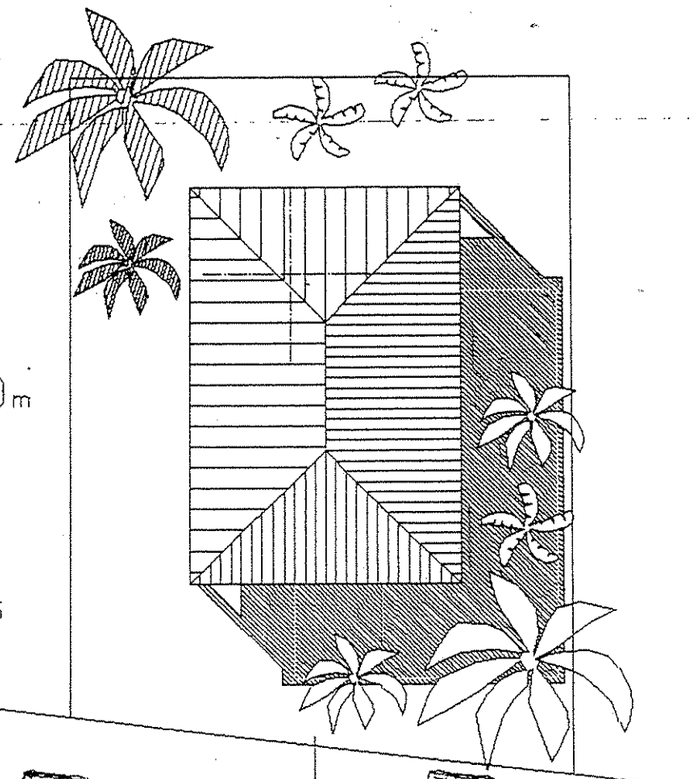
Plan de Masse

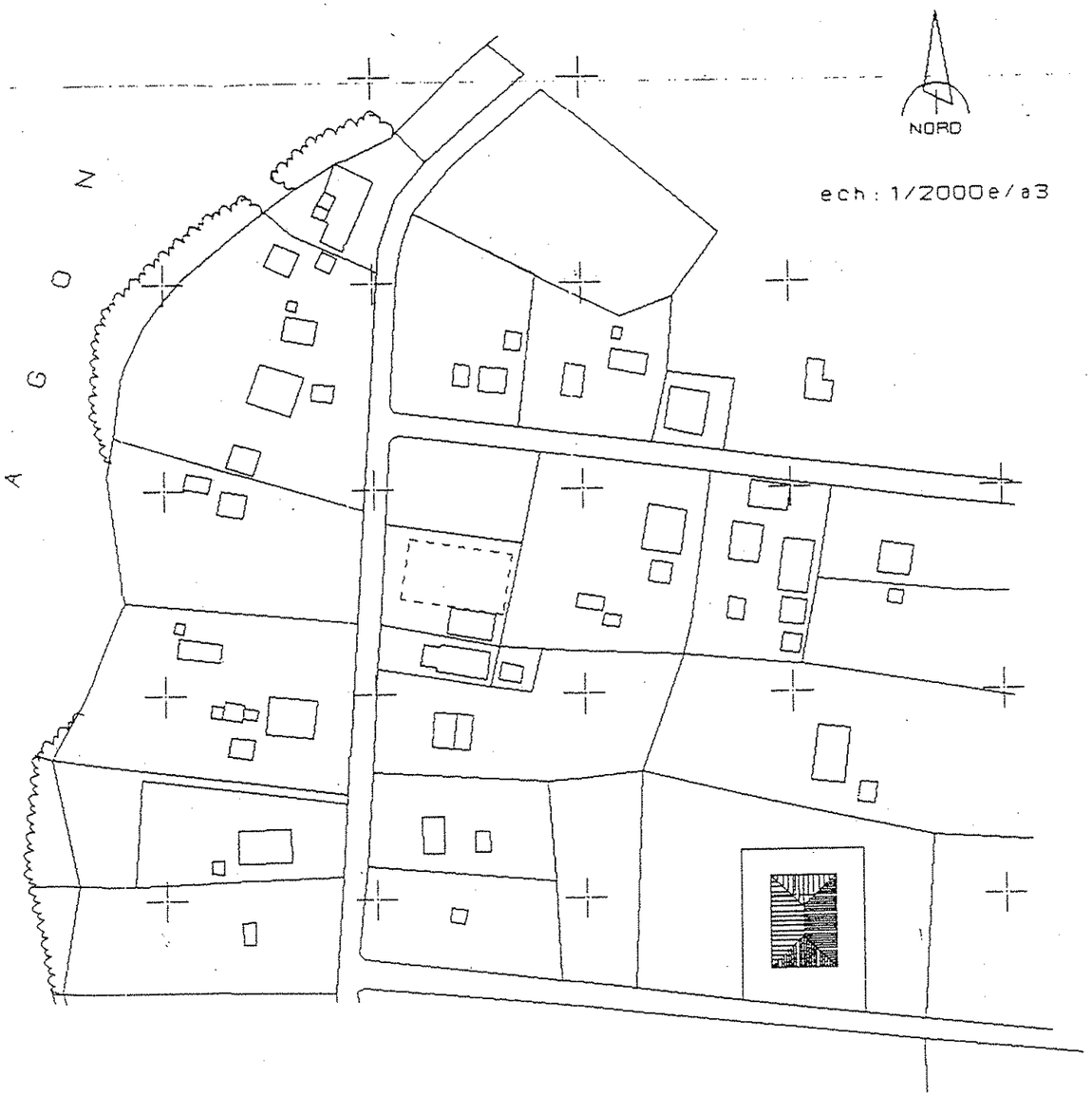
ech : 1/500e/a3

0 10 20m

Terre:TEVAIROA

Parcelle:44 et 45





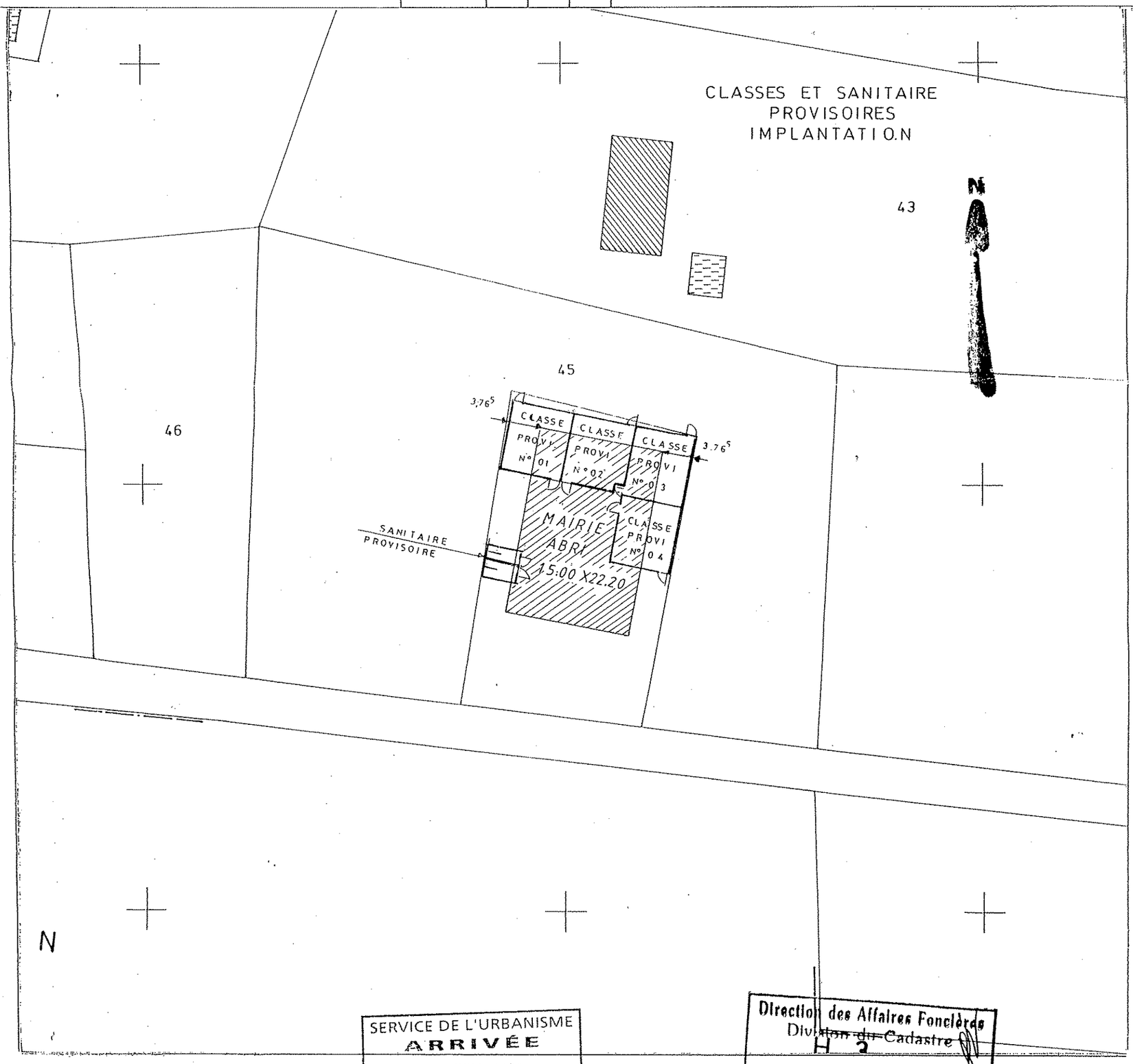
ech : 1/2000e/a3

0 25 50 75 100m

D.A.F. :

EXTRAIT DE PLAN CADASTRAL

Nom de la terre	parc. N°	ha	a	ca	Propriétaire à la matrice cadastrale
TEVAIROA	44		07	87	DOMAINE



SERVICE DE L'URBANISME
ARRIVÉE
20 NOV. 2003
N°_____ / AU
Section UOC

Direction des Affaires Foncières
Division du Cadastre
H 2

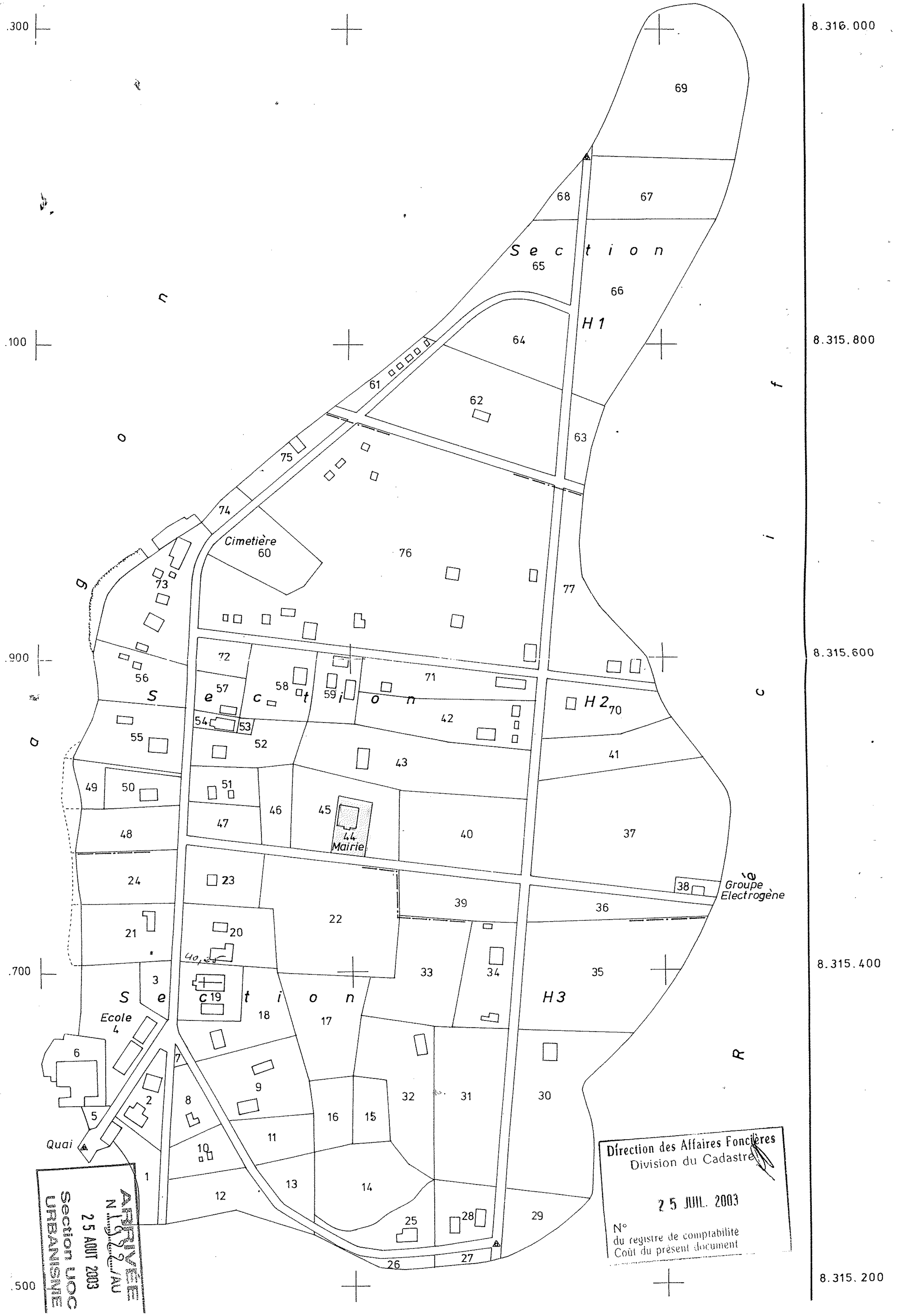
Reçu N°

Coût du présent extrait

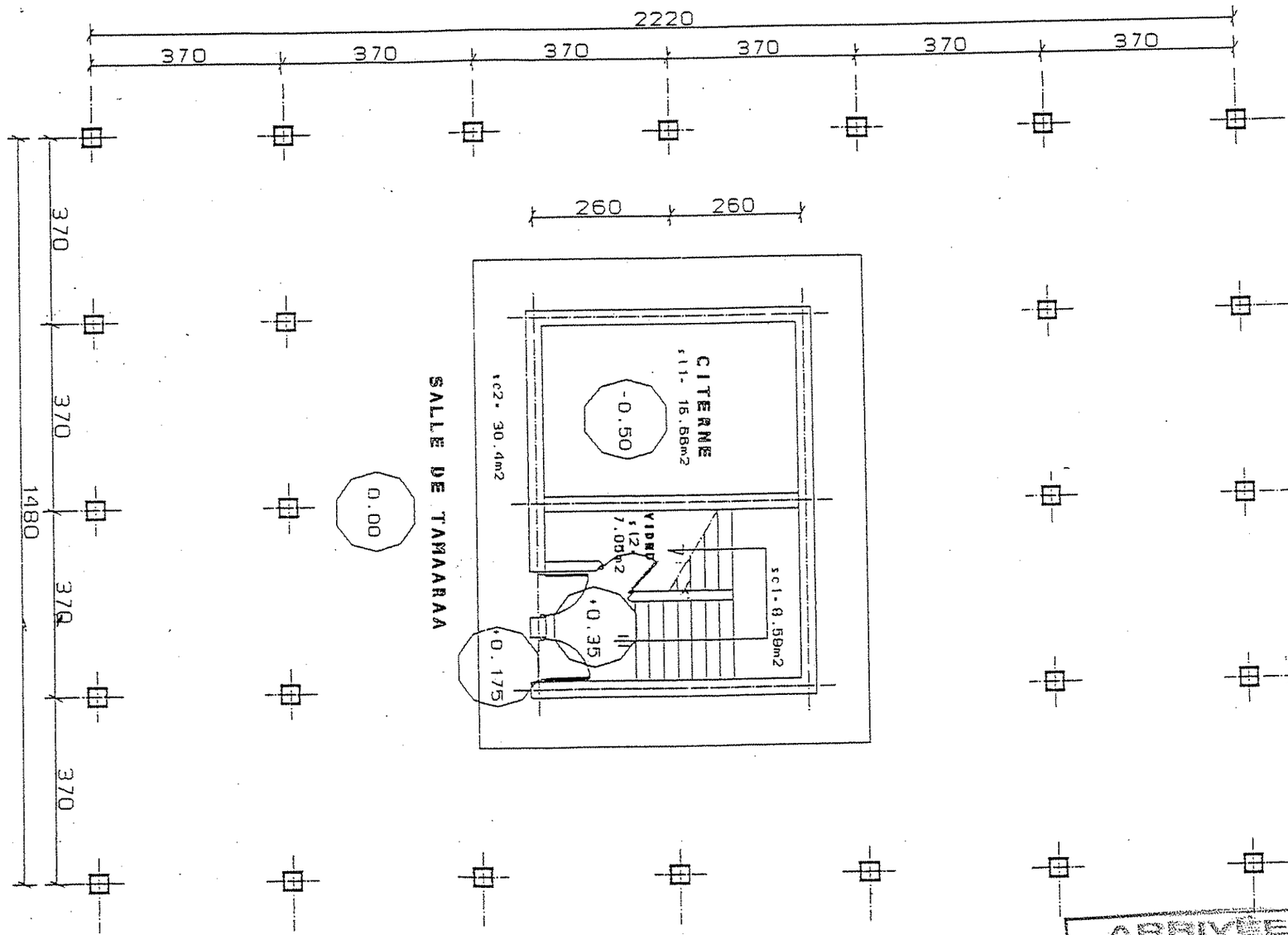
Papeete, le 25 JUIL. 2003

N°

Pour le Ministre et par délégation, le Chef de Division


8.316.000
8.315.800
8.315.600
8.315.400
8.315.200
.300
.100
.900
.700
.500
Section H1
Section H2
Section H3
Section
Cimetière
Mairie
Groupe Electrogène
Ecole
Quai
Direction des Affaires Foncières
Division du Cadastre
2 5 JUIL. 2003
N°
du registre de comptabilité
Coût du présent document
ARRIVÉE
N 1922 /AU
25 AOUT 2003
Section UOC
URBANISME

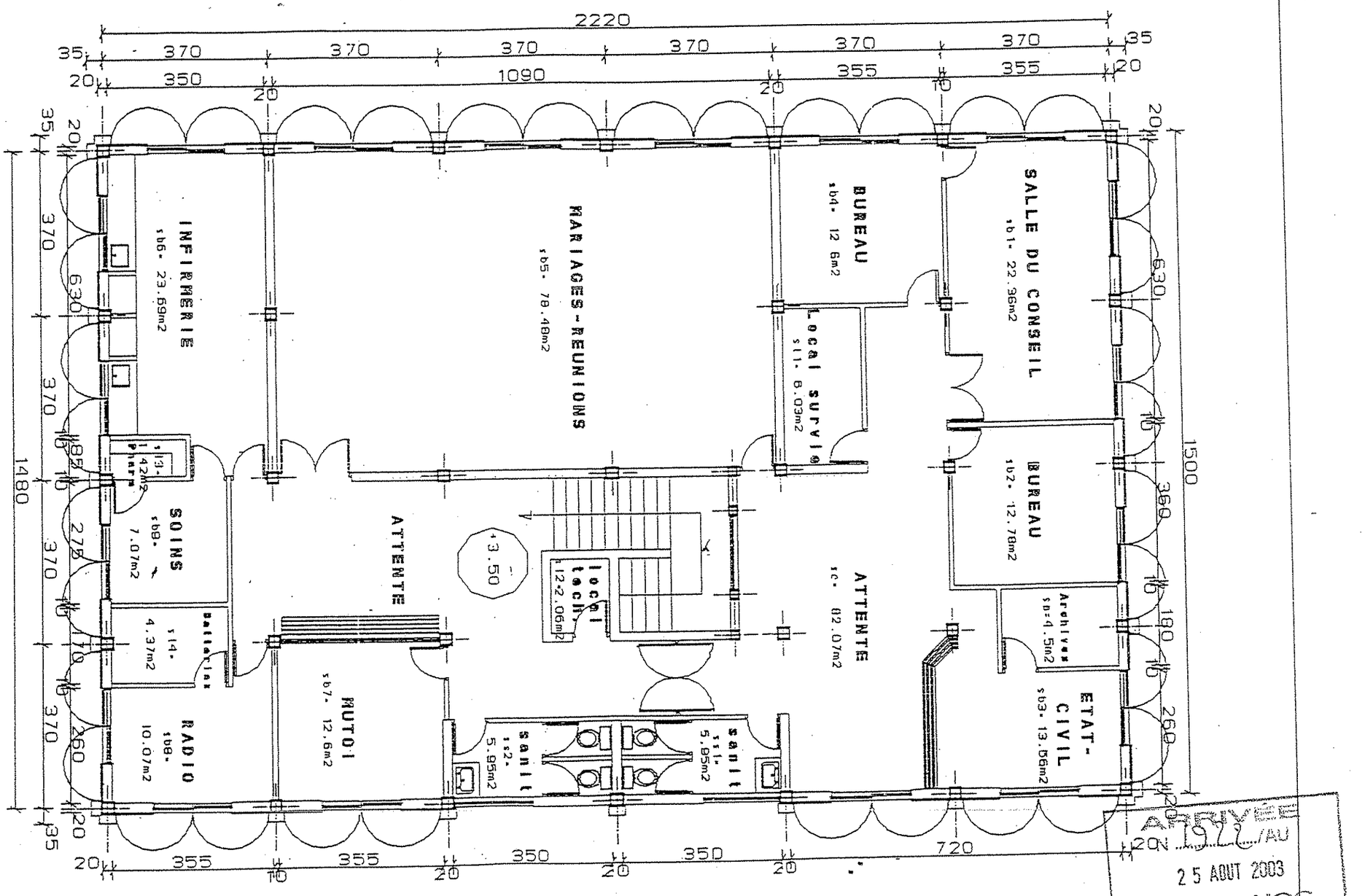
VUE EN PLAN RDC BATIMENT EXISTANT



PLAN D'OCCUPATION DU NIVEAU	
Decomposition des Surfaces	
1: CIRCULATIONS	s1cir= 38.99m2
2: LOC.TECNIQUES	s1s.p= 23.71m2
Surface du Rez de Chaussee	
SDO=62.69m2	SHO= 341.63m2

ARRIVEE
N 1992/AU
25 AOUT 2009
Section UO6
L'URBANISME

VUE EN PLAN ETAGE BATIMENT EXISTANT

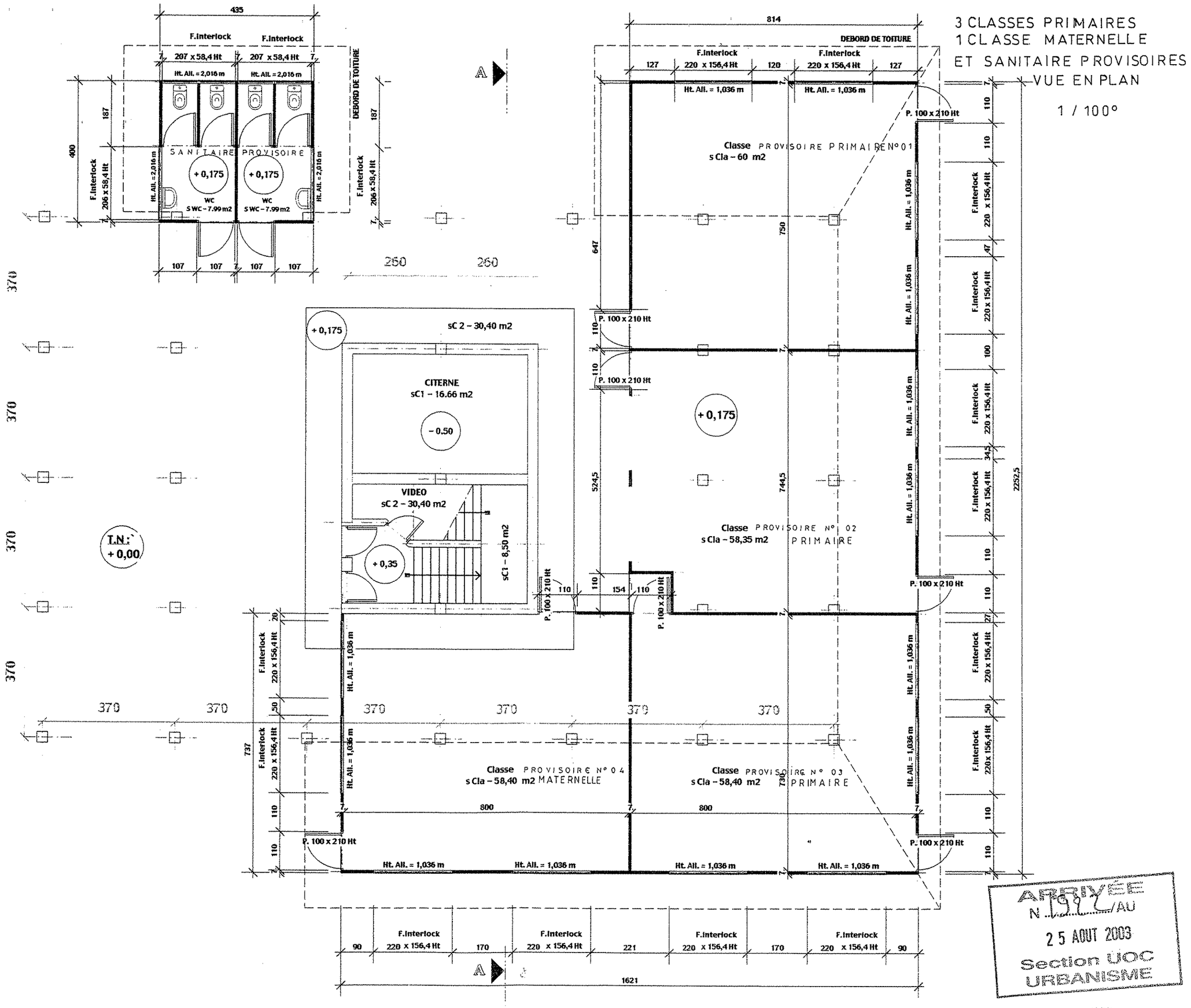


PLAN D'OCCUPATION DU NIVEAU	
Decomposition des Surfaces	
1: ARCHIVES	s1er= 4.5m2
2 BUREAUX	s1bur= 193.21m2
3 CIRCULATIONS	s1cir= 82.07m2
4: SANITAIRES	s1san= 11.9m2
5: LOC.TECNIQUES	s1s.o= 13.85m2
Surface du 1eme Etage	
SDO= 305.57m2	SHO= 337.87m2

ARRIVEE
AU
25 AOUT 2003
Section UOC
URBANISME

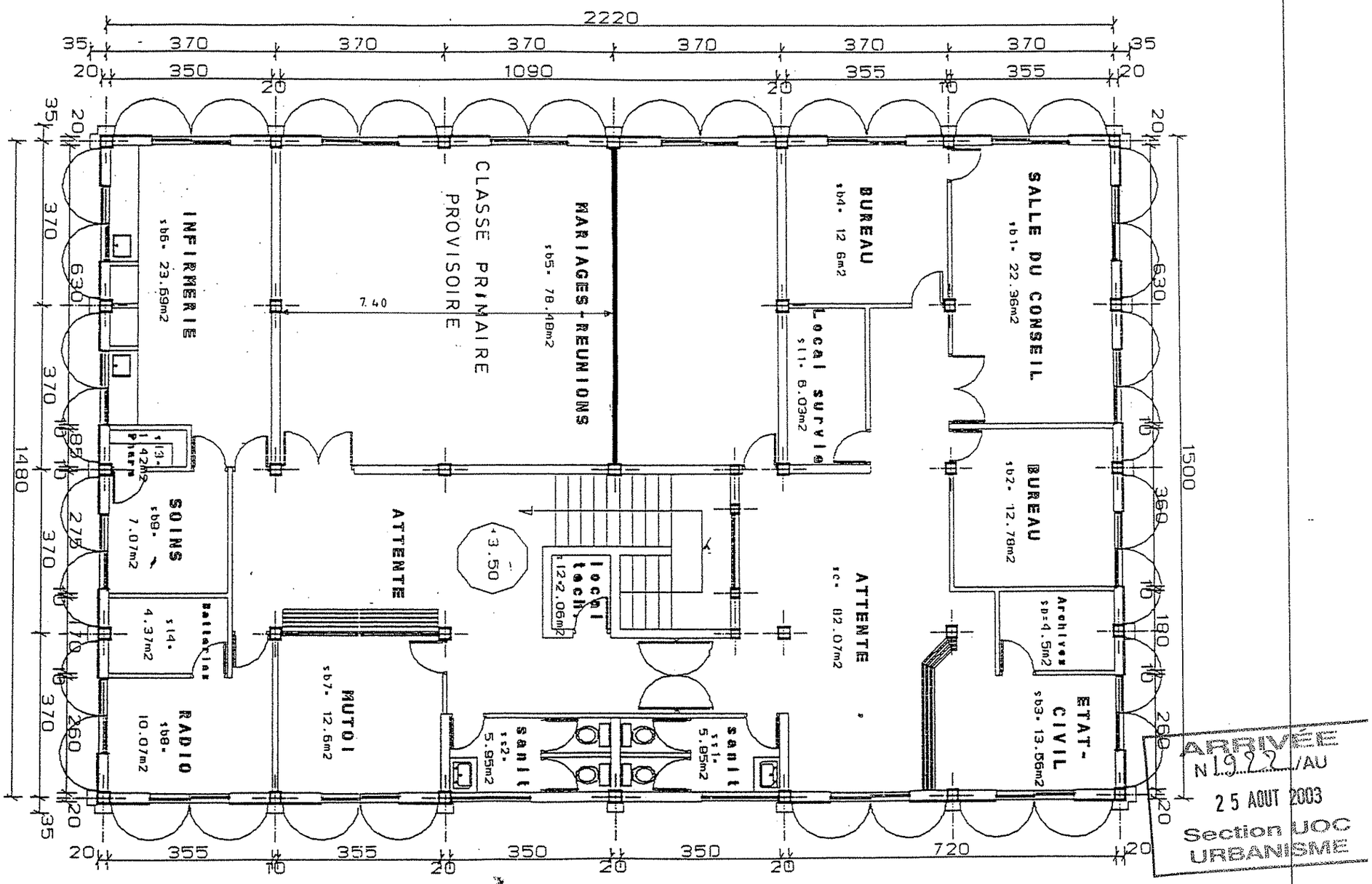
3 CLASSES PRIMAIRES
1 CLASSE MATERNELLE
ET SANITAIRE PROVISOIRES
VUE EN PLAN

1 / 100°



ARRIVÉE
N° 1992 /AU
25 AOUT 2003
Section UOC
URBANISME

CLASSE PRIMAIRE PROVISOIRE
A L'ETAGE ECH 1/100°



PLAN D'OCCUPATION DU NIVEAU

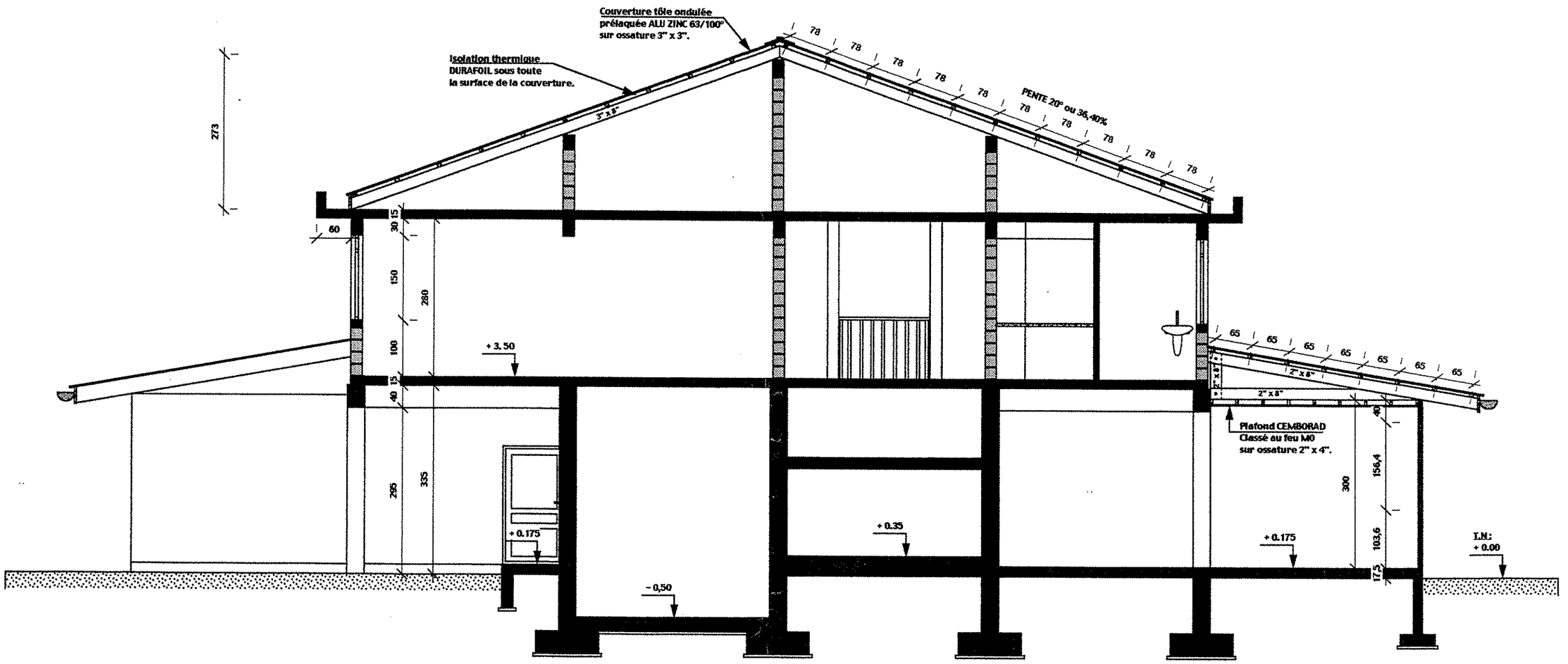
Decomposition des Surfaces		
1: ARCHIVES	s1arch=	4.5m2
2 BUREAUX	s1bur=	193.21m2
3 CIRCULATIONS	s1cir=	82.07m2
4: SANITAIRES	s1san=	11.9m2
5: LOC.TECNIQUES	s1s.p=	13.85m2

Surface du 1eme Etage
SDO= 305.57m2 SHO= 337.87m2

ARRIVÉE
N 1922 /AU
25 AOUT 2003
Section UOC
URBANISME

5 CLASSES ET SANITAIRE PROVISOIRES

COUPE A.A ECH 1 / 75°



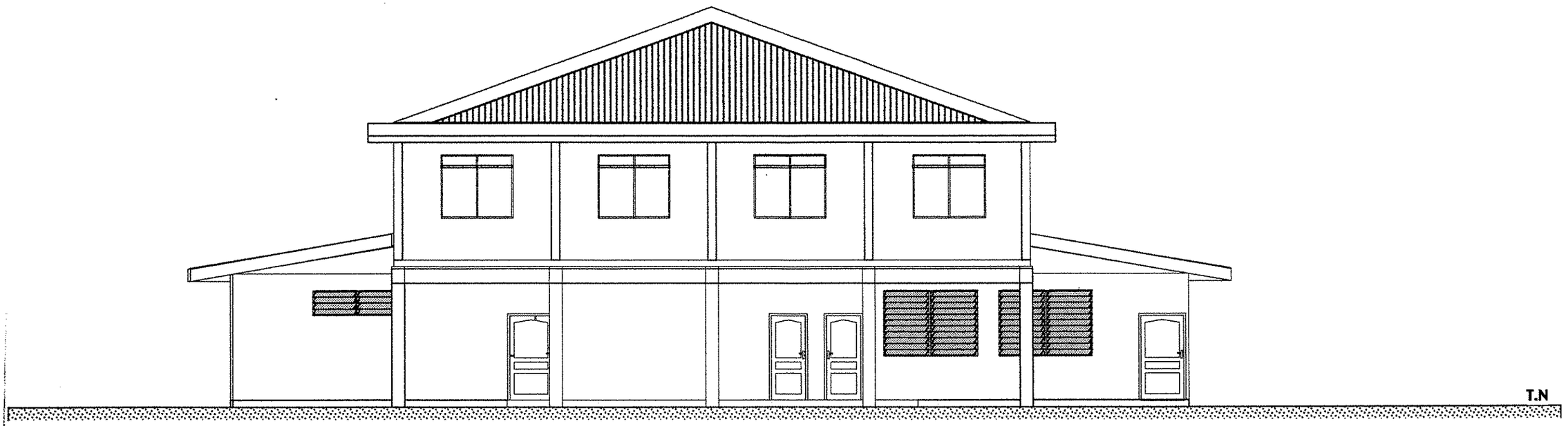
ARRIVEE
N 1922 /AU
25 AOUT 2003
Section UOC
URBANISME

NOTA :

- **Les sols seront constitués d'un revêtement carrelages Grès Cérames (anti-dérapants) classés UPEC.**
- **Les murs intérieurs des salles d'eaux sont à une hauteur de 1,80 m et revêtus de carreaux de faiences 15 x15 sur une hauteur de 2,00 m .**
- **L'alimentation en eau se fera par la citerne d'eau de à l'aide de pompes à eau.**

5 CLASSES ET 1 SANITAIRE PROVISOIRES

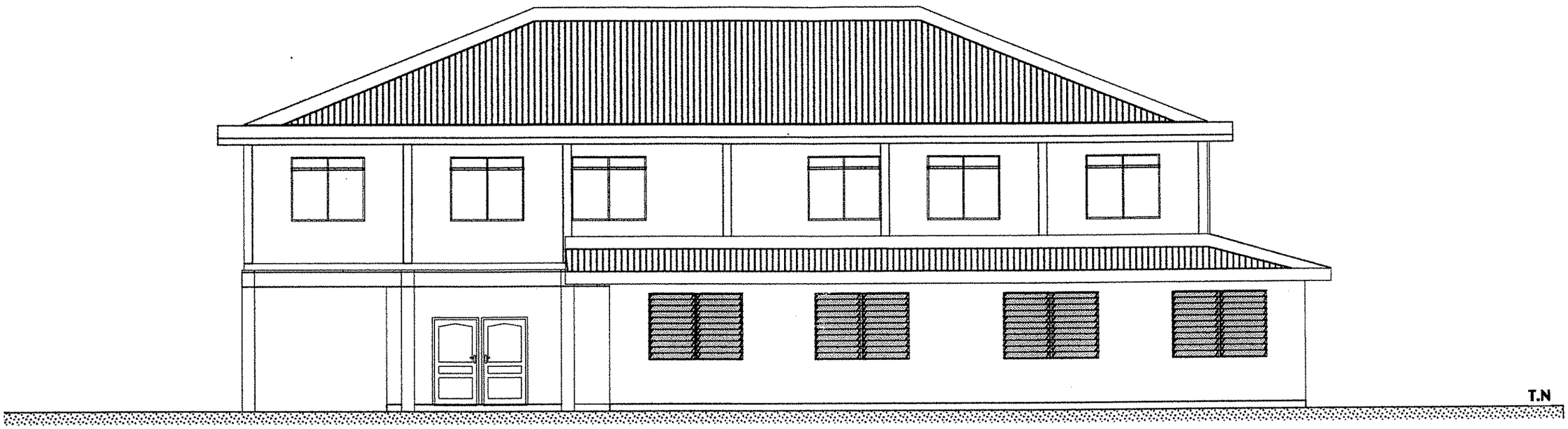
FACADE AVANT ECH 1/100°



ARRIVÉE
N. 1922/AU
25 AOUT 2003
Section UOC
URBANISME

5 CLASSES ET UN SANITAIRE PROVISOIRES

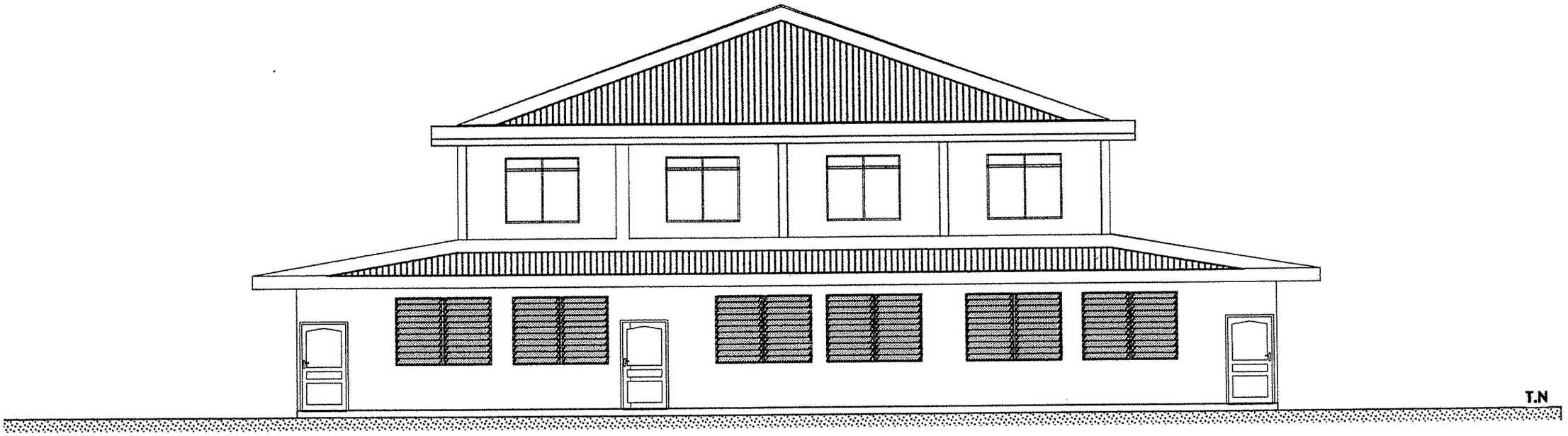
FACADE LATERALE DROITE ECH 1 / 100°



ARRIVÉE
N 1922 /AU
25 AOUT 2003
Section UOC
URBANISME

5 CLASSES ET 1 SANITAIRE PROVISOIRES

FACADE ARRIERE 1/ 100°



ARCHIVÉE
N DLK AU
25 AOUT 2003
Section UOC
URBANISME

SUJET N° 2 :

Compte tenu des documents qui vous sont présentés, indiquez la problématique de la réalisation de cette opération de viabilisation et de construction au titre d'une demande de travaux immobiliers.

Nota : le projet n'est pas situé sur une commune dotée d'un plan général d'aménagement.

POLYNESIE FRANCAISE
Ile de TAHITI
Commune de ARUE

Office Polynésien de l'Habitat
O.P.H.
B.P. 1705 - 98713 PAPEETE TAHITI

ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME

OPERATION TAHIPU

- 19 LOGEMENTS -

- Avant Projet Détaillé -

Le Maire
Boris LEONTIEFF

PLAN DE SITUATION

Archives : 351 E

Date : Janvier 2001

A.P.D

Plan N°

01

Echelle : 1/5000

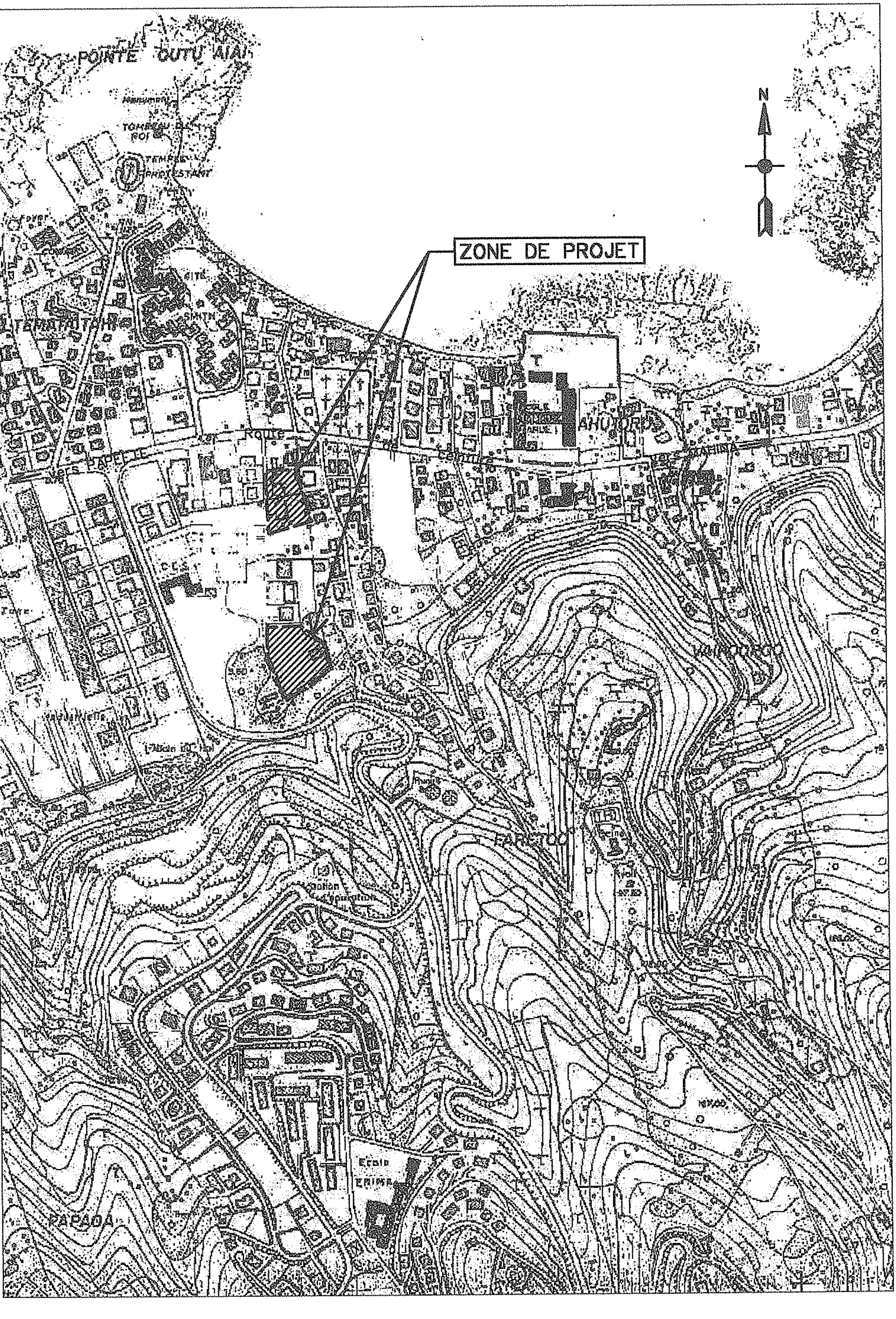
Bureau d'études :

PACIFIQUE
B.P. 1756 - 98713 Papeete - TAHITI
Tel: 54-47-47 / Fax: 41-94-42
Email: topopac@mail.pf

Maitre d'ouvrage :

S.C.I. TAHIPU

BP 973 Papeete Tahiti
Polynésie Française
Tel: 58 27 23
Fax: 58 37 93



POINTE OUTU AIAI
TOMBEAU DU ROI
TEMPLE PROTESTANT
N
ZONE DE PROJET
Route
vers PAPEETE
Ceinture
vers MAHINA
AHUTORU
C.E.S.
PAPAOA
Ecole

POLYNESIE FRANCAISE
Ile de TAHITI
Commune de ARUE

Office Polynésien de l'Habitat
O.P.H.
B.P. 1705 - 98713 PAPEETE TAHITI

ARRIVÉE
N .....
26 JAN. 2001
Section UOC
URBANISME

OPERATION TAHIPU

- 19 LOGEMENTS -

- Avant Projet Détaillé -

Le Maire
Boris LEONTIEFF

PLAN TOPOGRAPHIQUE ET PARCELLAIRE

Archives : 351 E

Date : Janvier 2001

A.P.D

Plan N°

02

Echelle : 1/250

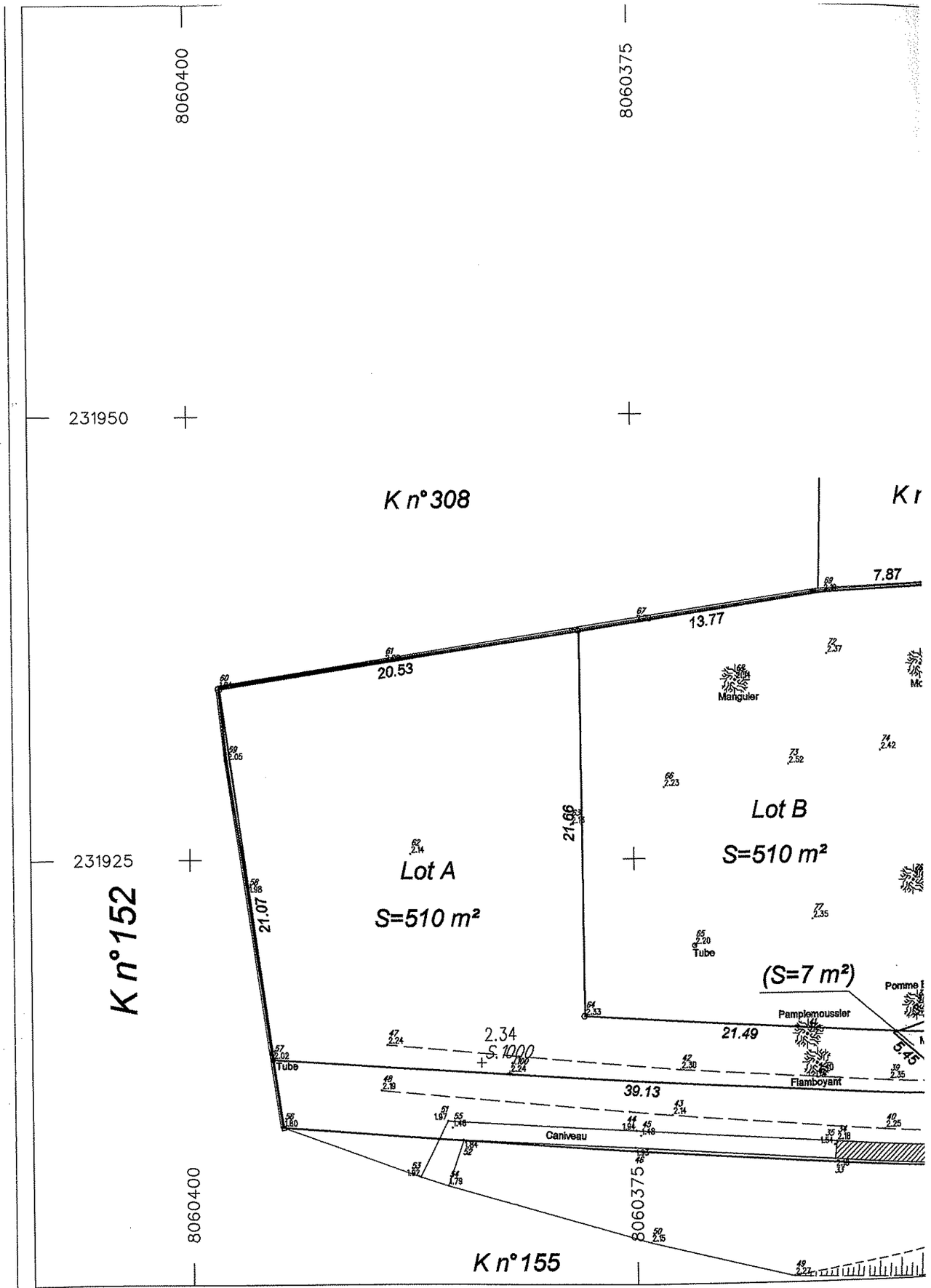
Bureau d'études :

TOPO PACIFIQUE
B.P. 1756 - 98713 Papeete - TAHITI
Tel: 54-47-47 / Fax: 41-94-42
Email: topopac@mail.pf

Maitre d'ouvrage :

S.C.I. TAHIPU

BP 973 Papeete Tahiti
Polynésie Française
Tel: 58 27 23
Fax: 58 37 93



8060350

8060325

8060300

8060275

K. 314

312

K n° 241

K n° 242

K n° 243

K. 269

(S=2 m²)

Dalle

Dalle

Poubelle

Poubelle

Poubelle

Route

K. 155

K. 350

Caniveau

Tube

Split

8060250
8060225
8060200
8060175
231950
231925
K. 315
K. 317
K. 348
K. 415
K. 351
K. 347
K. 416
K. 349
K. 345
K. 159
K. 346
K. 158
limite par application cadastrale
Tube
Tube existant

POLYNESIE FRANCAISE
Ile de TAHITI
Commune de ARUE

Office Polynésien de l'Habitat
O.P.H.
B.P. 1705 - 98713 PAPEETE TAHITI

ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME

OPERATION TAHIPU

- 19 LOGEMENTS -

Le Maire
Boris LEONTIEFF

- Avant Projet Détaillé -

PLAN DES TERRASSEMENTS

Archives : 351 E

Date : Janvier 2001

A.P.D

Plan N°

03

Echelle : 1/250

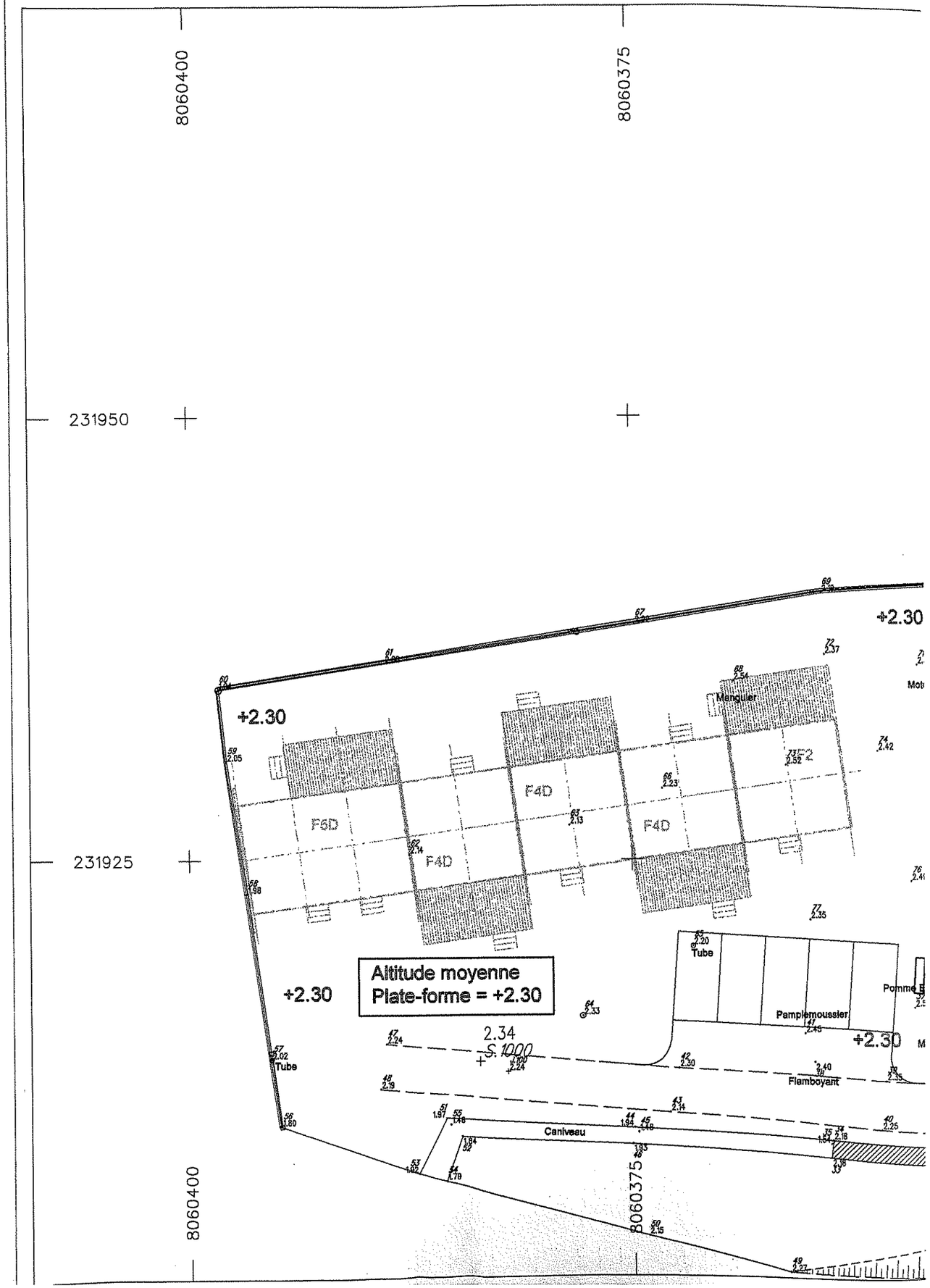
Bureau d'études :

PACIFIQUE
B.P. 1756 - 98713 Papeete - TAHITI
Tel: 54-47-47 / Fax: 41-94-42
Email: topopac@mail.pf

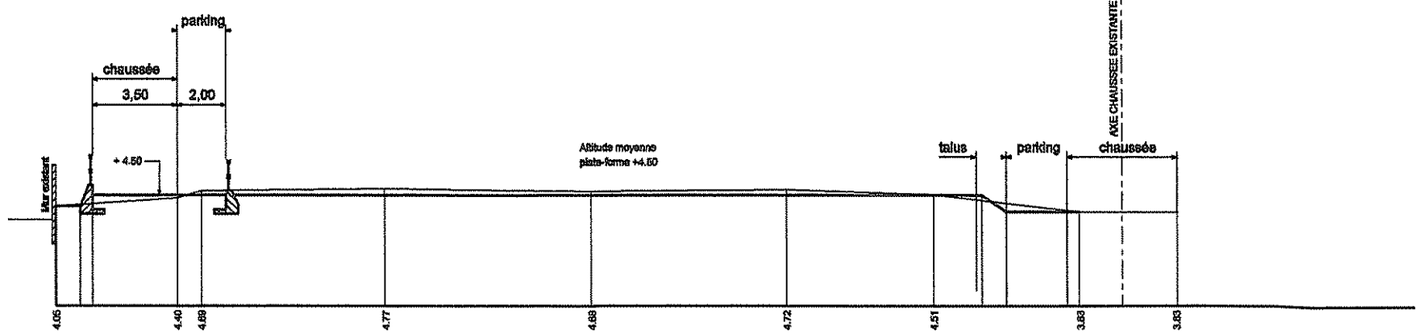
Maitre d'ouvrage :

S.C.I. TAHIPU

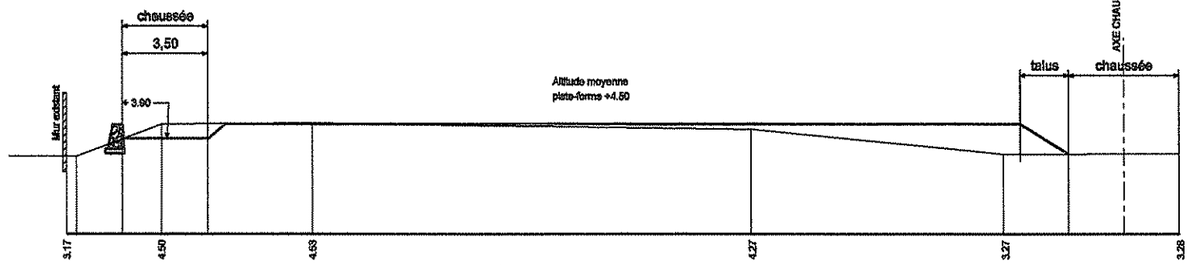
BP 973 Papeete Tahiti
Polynésie Française
Tel: 58 27 23
Fax: 58 37 93



8060350 8060325 8060300 8060275



COUPE YY'



COUPE XX'

- LEGENDE -

4.04 Altitude tn

+4.50 Altitude projet

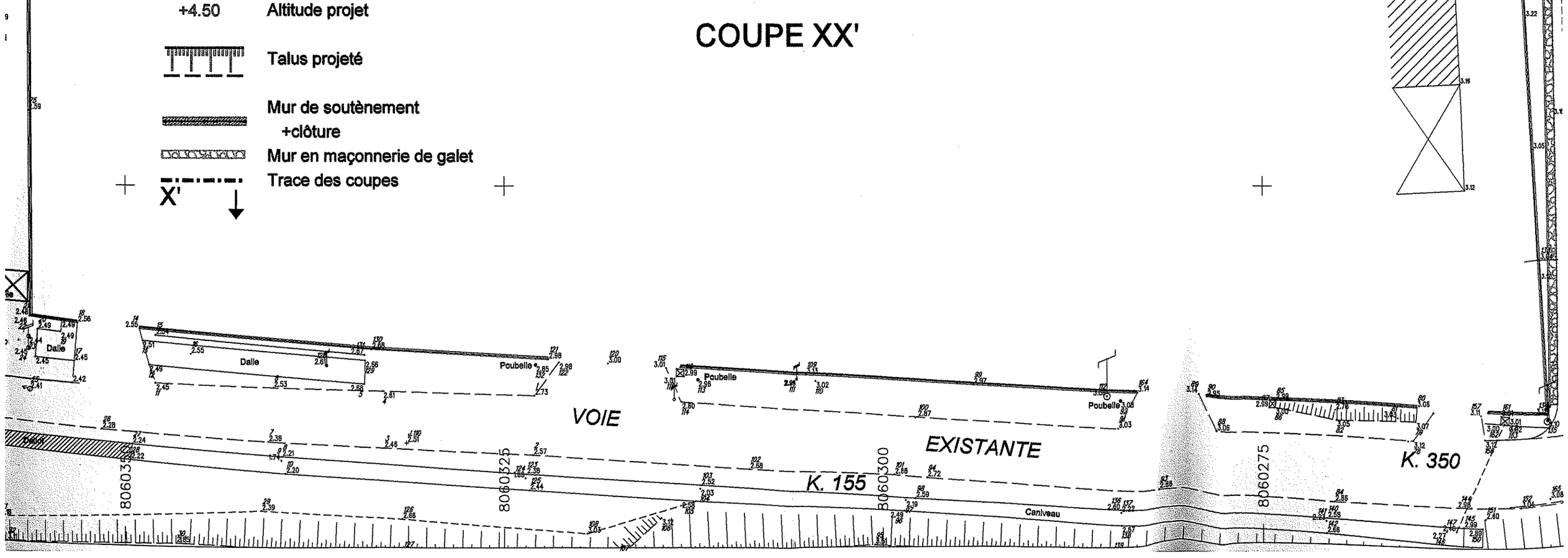
Talus projeté

Mur de soutènement
+clôture

Mur en maçonnerie de galet

Trace des coupes

X'



8060250

8060225

8060200

8060175

231950

231925

X

X'

Y

Y'

+6.00

+4.50

+3.20

3.70

DESSERTE

VOIE DE

VOIE

EXISTANTE

F5D

F4D

F3D

Altitude moyenne
Plate-forme = +4.50

POLYNESIE FRANCAISE

ARRIVEE
N ...../AU
26 JAN. 2001
Section LOC
URBANISME

OFFICE POLYNESIEN DE L'HABITAT

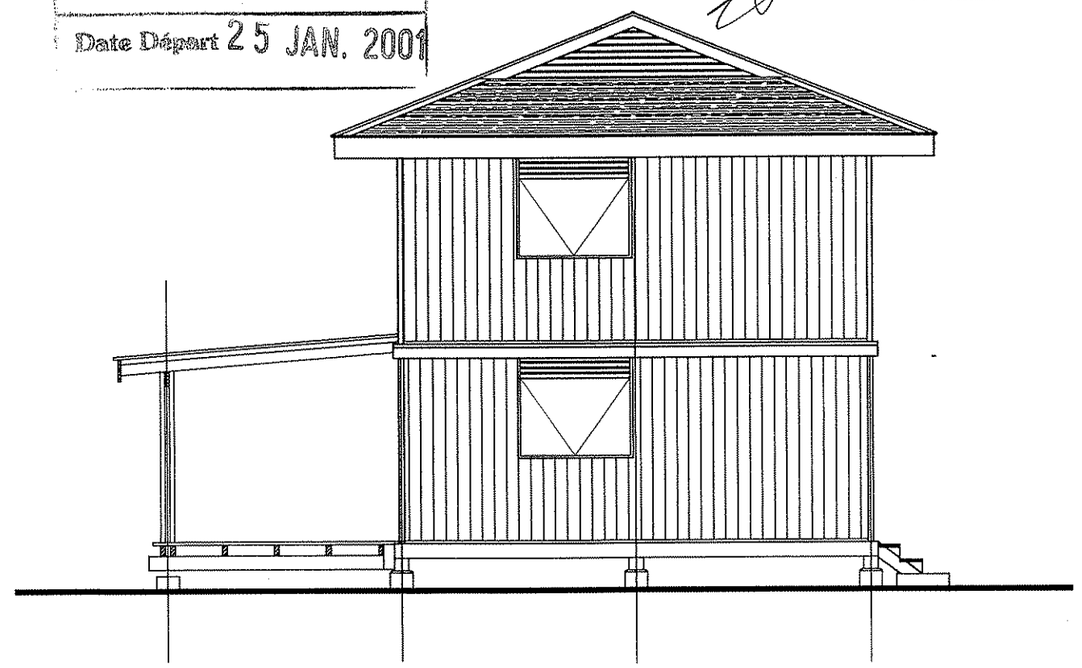
B.P : 1705 - 98713 PAPEETE - Tél : 54 28 80 / 50 38 50 Fax : 41 25 05 / 45 03 47

OPERATION TAHIPU

ARUE

Mairie d'ARUE
N° 06-2001
Date Arrivée 19 JAN. 2001
Date Départ 25 JAN. 2001

MAIRIE D'ARUE
TAHITI
Polynésie Française
Le Maire
Boris LEONTIEFF



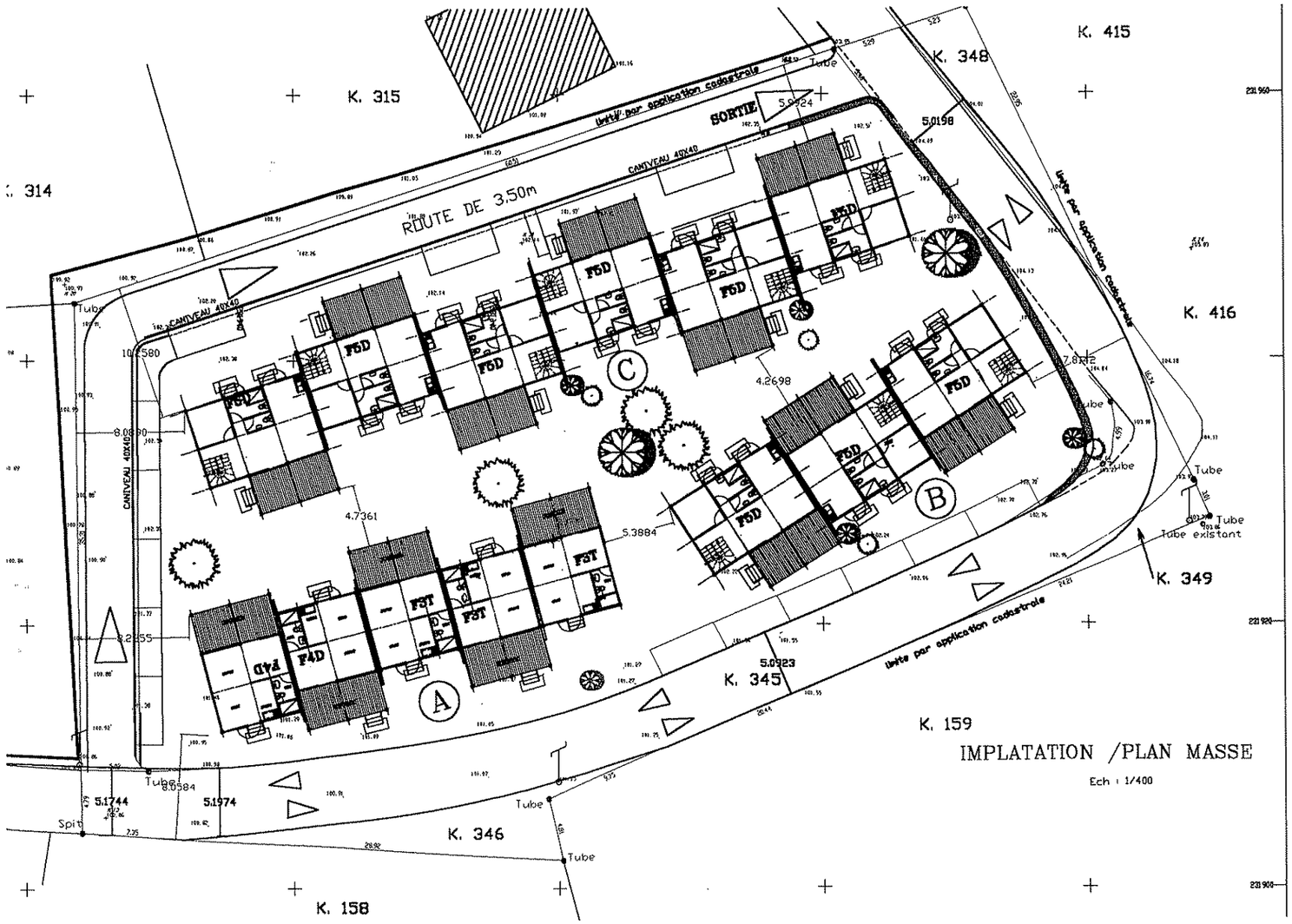
IMPLANTATION

VUE EN PLAN - FACADES - COUPE

TYPE DU FARE

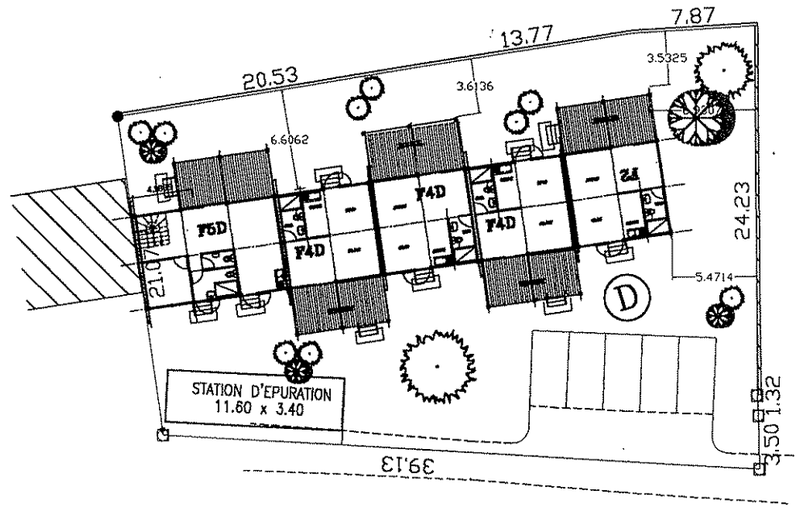
F2 / F3D / F4D / F5D

ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME



IMPLATATION /PLAN MASSE

Ech : 1/400



IMPLATATION /PLAN MASSE

Ech : 1/400

ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME

3.0500

PAVC

FAVP -All. H =100

2.9500

1.9500

7.1000

2.9500

Chambre 1

P83/204

P73/204

W/C

SDB

2.9543

FAVC -All. H =100

REPAS

2.9500

2.9500

P73/204

SDB

P73/204

W/C

2.9543

SEJOUR

7.1000

FAVP -All. H =100

PAVC

TERRASSE

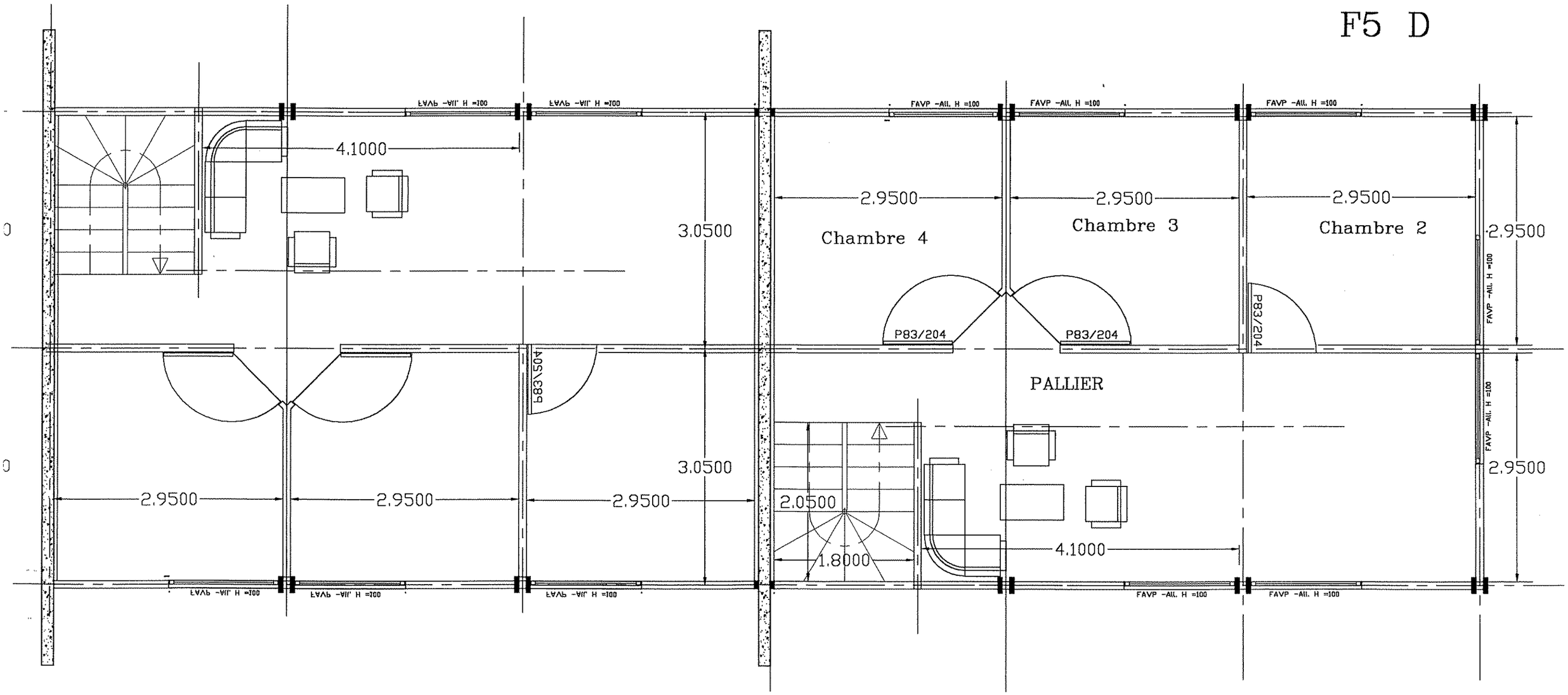
3.0500

6.1000

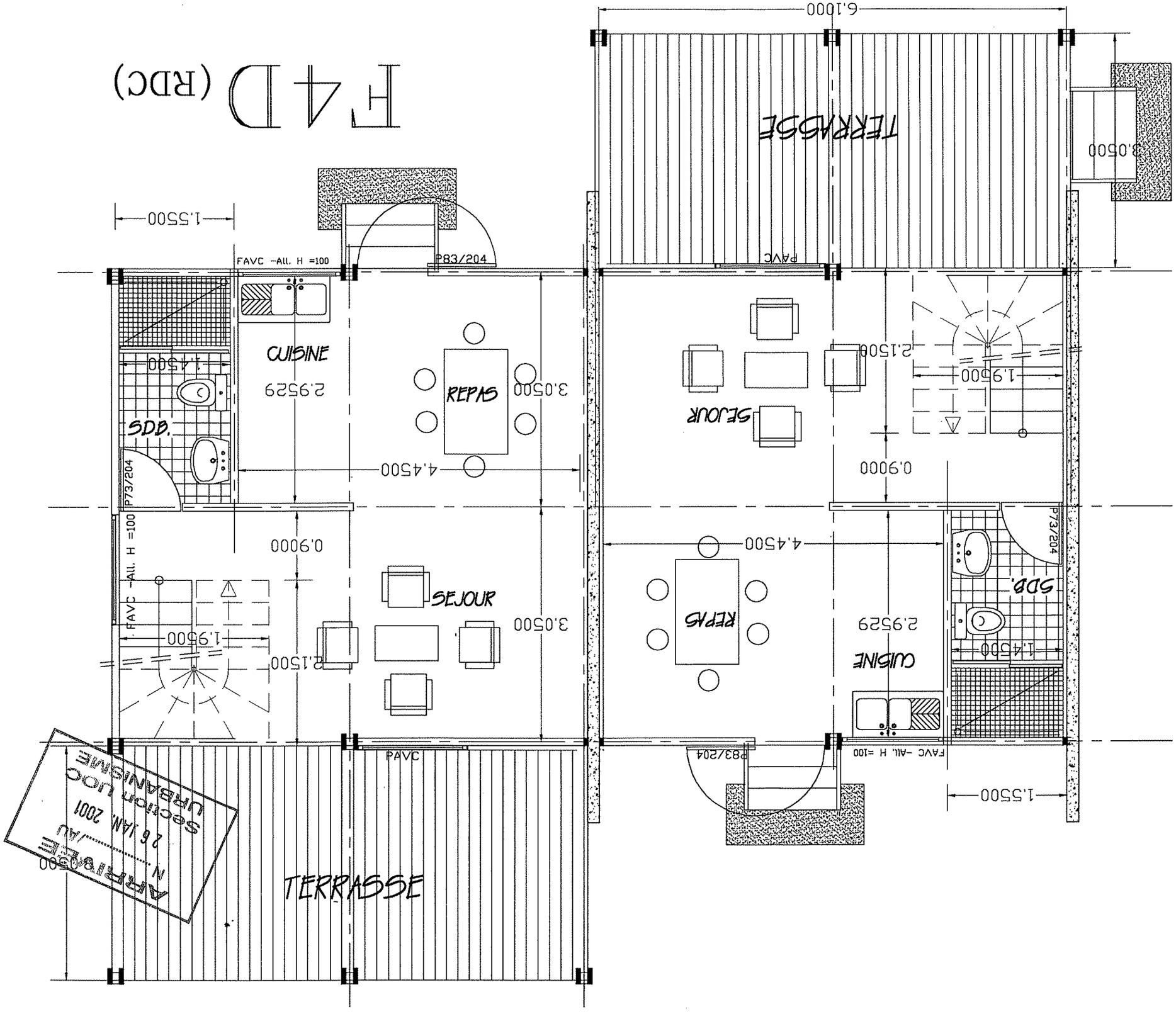
F5D (RDC)

ARRIVÉE
N...../AU
26 JAN. 2001
Section UOC
URBANISME

ETAGE
F5 D



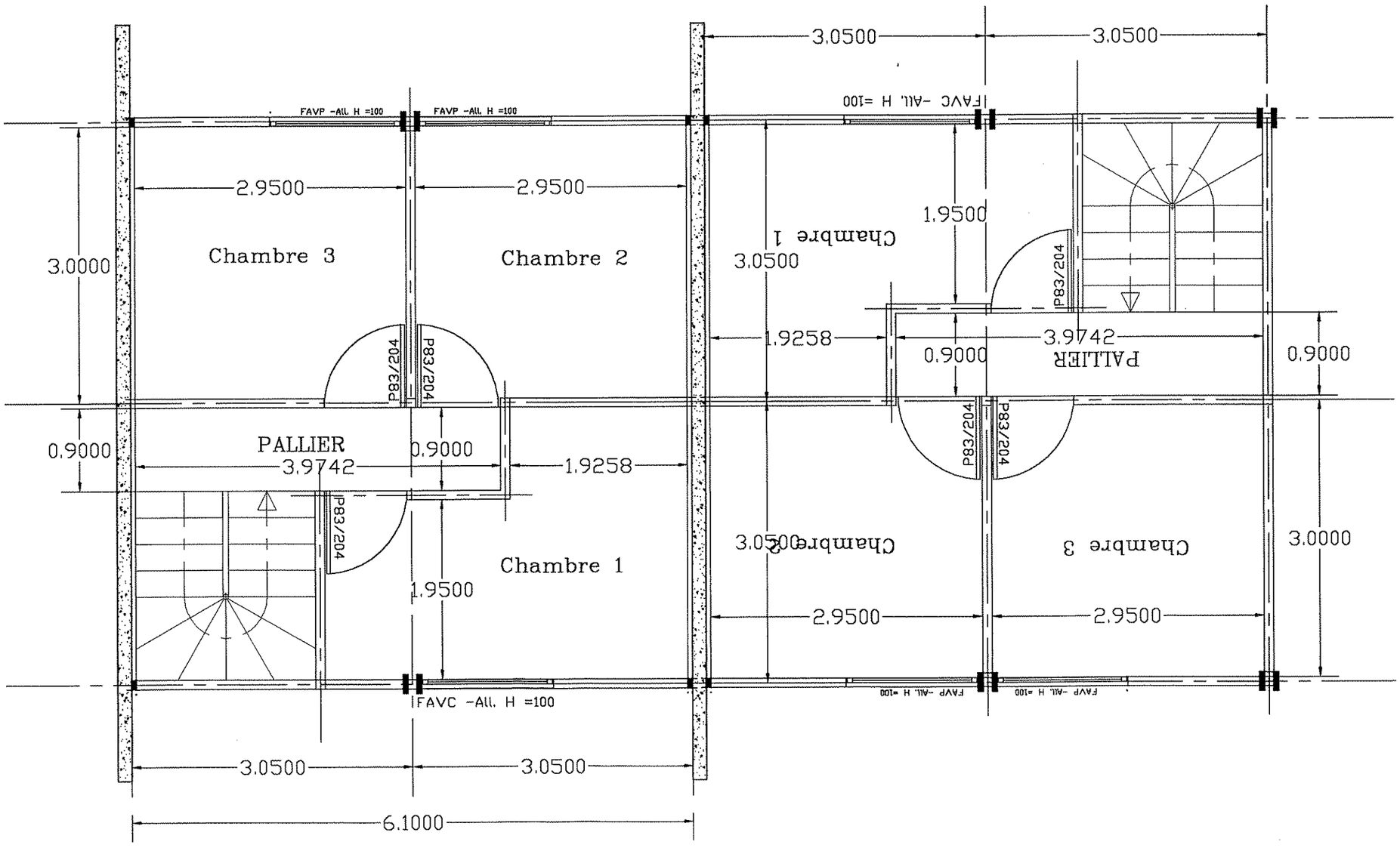
F4D (RDC)

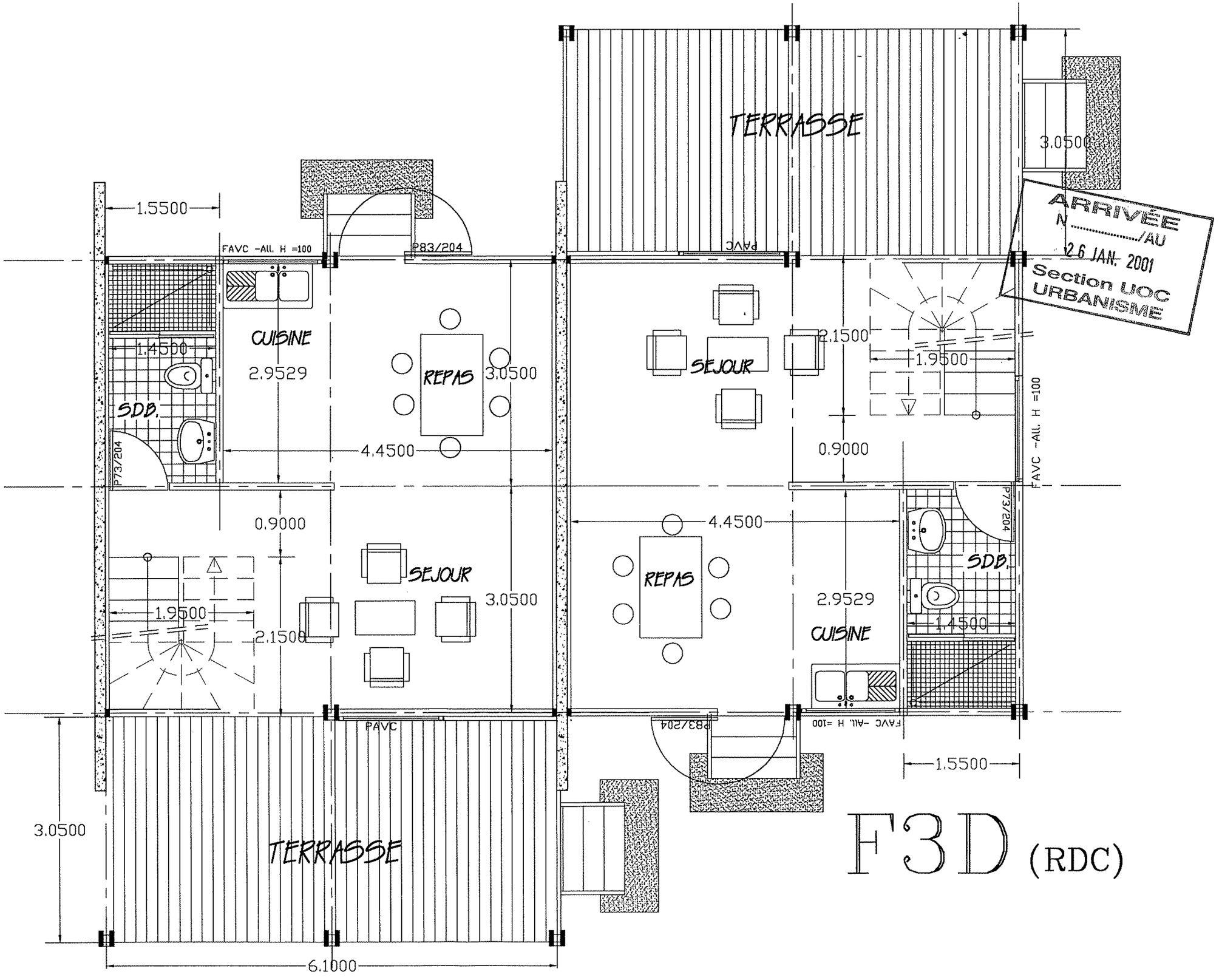

6.1000
TERRASSE
3.0500
PAVC
1.5500
FAVC -All. H =100
P83/204
CUISINE
2.9529
1.4500
SDB.
P73/204
REPAS
3.0500
4.4500
2.1500
SEJOUR
1.9500
0.9000
PAVC
TERRASSE
Section UOC
26 JAN. 2001
AU
N
APPARTEMENT
URBANISME

ARRIVÉE
N° ...../AU
26 JAN. 2001
Section UOC
URBANISME

ETAGE

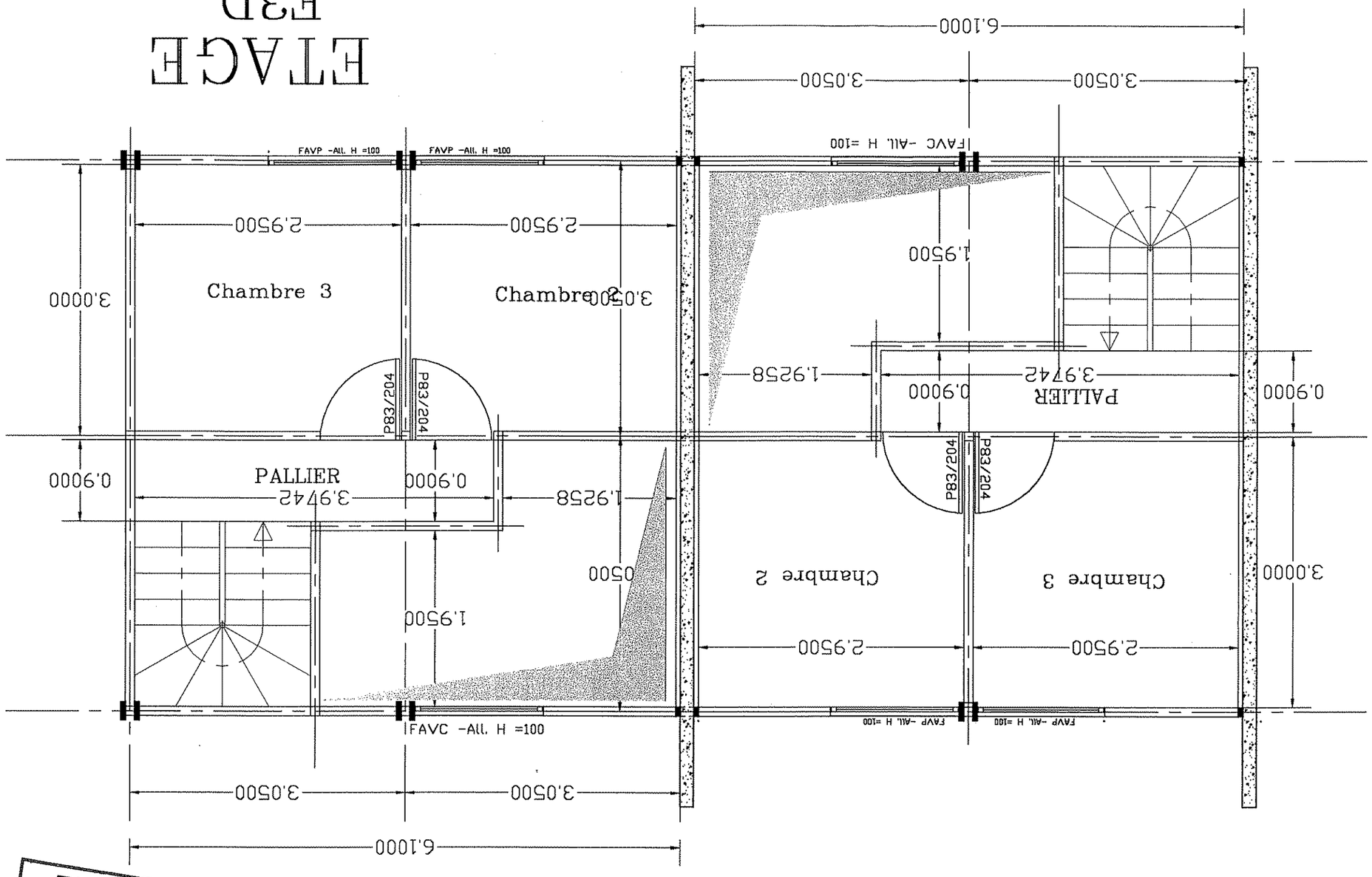
F4D



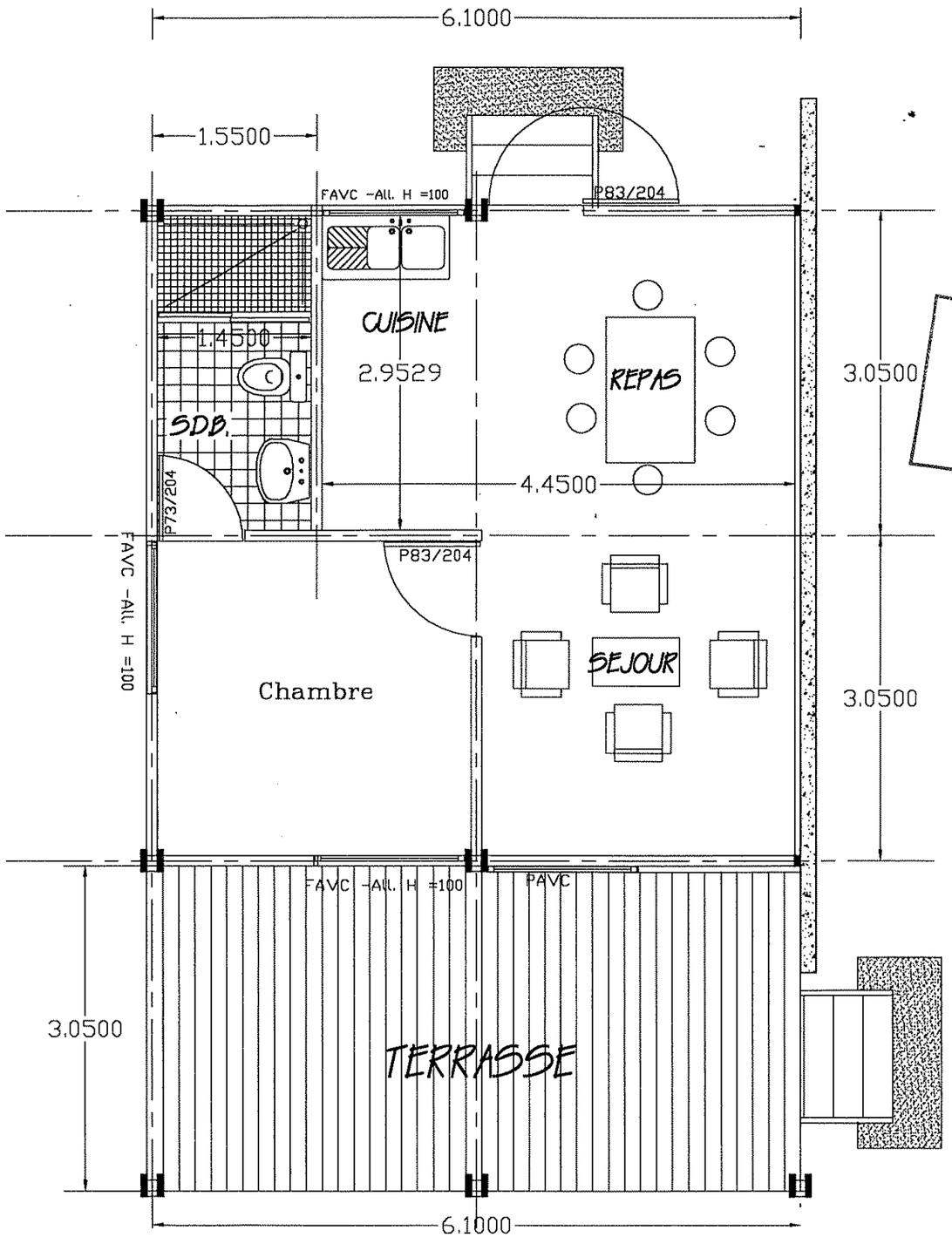

TERRASSE
3.0500
ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME
1.5500
FAVC -All. H =100
P83/204
CUISINE
2.9529
1.4500
SDB.
P73/204
REPAS
3.0500
4.4500
SEJOUR
2.1500
1.9500
0.9000
FAVC -All. H =100
P73/204
4.4500
REPAS
SDB.
2.9529
CUISINE
1.4500
P83/204
FAVC -All. H =100
1.5500
PAVC
SEJOUR
3.0500
1.9500
2.1500
0.9000
3.0500
TERRASSE
6.1000

F3D (RDC)

ETAGE F3D



AFFIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME



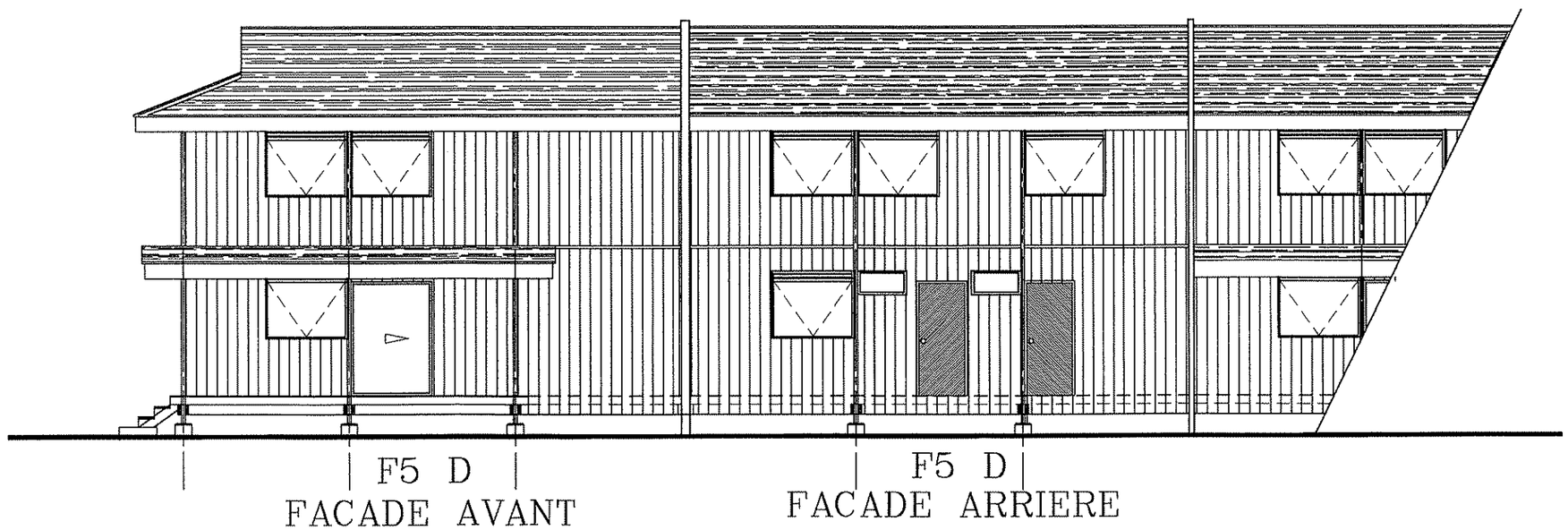
ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME

F2 (RDC)

ARRIVÉE
N ..... /AU
26 JAN. 2001
Section UOC
URBANISME

FACADE TYPE DES F5 D

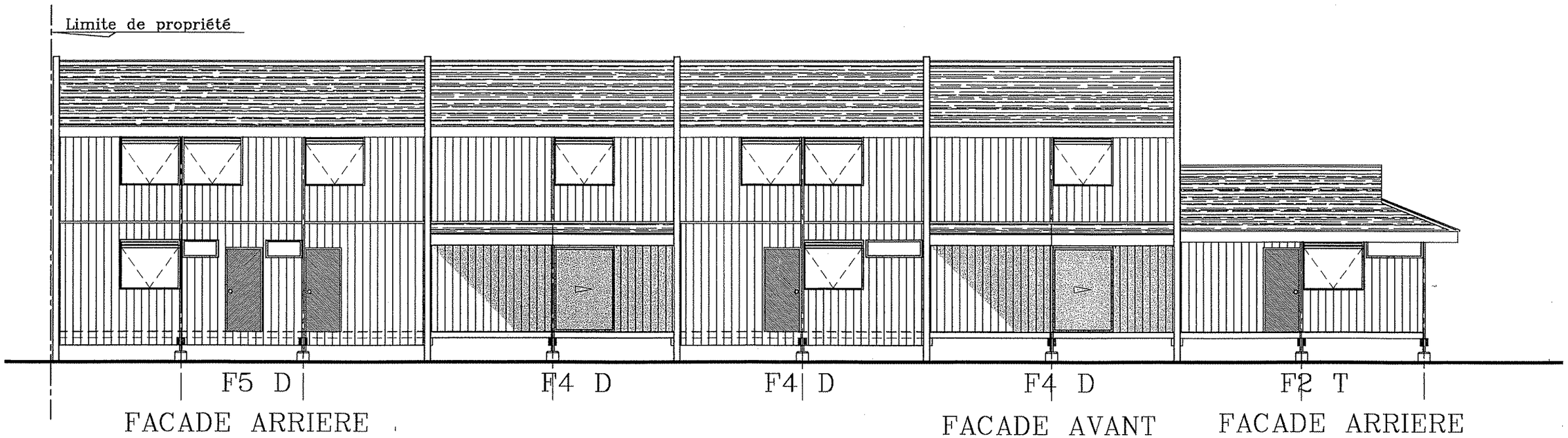
Ech : 1/100



ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME

FACADE Ilot: D de 5 FARE

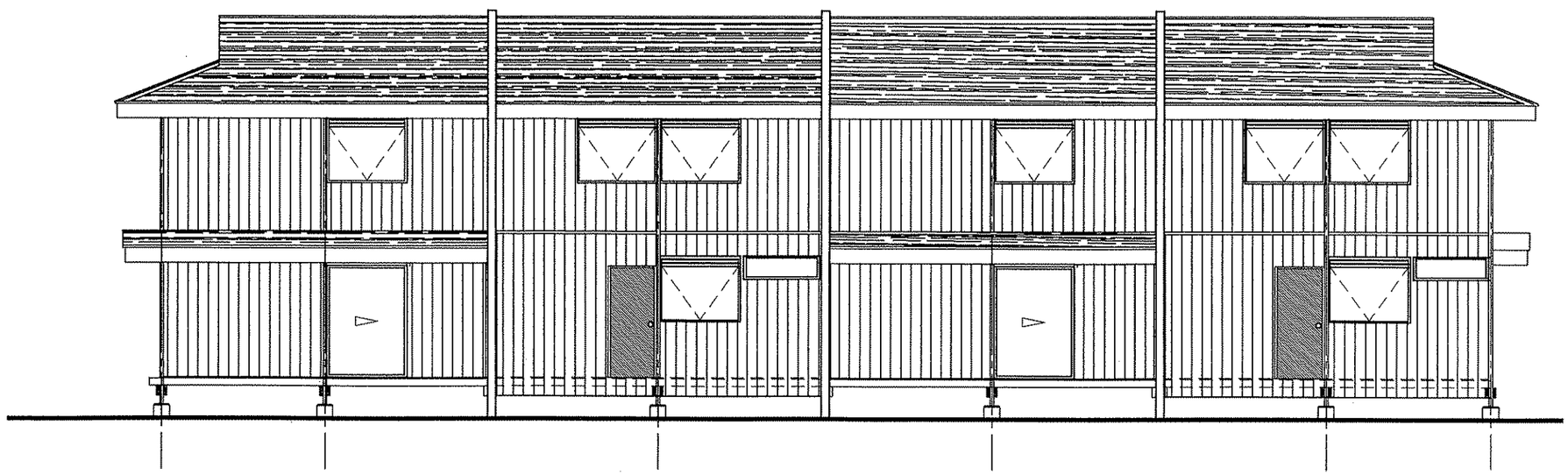
Ech : 1/100



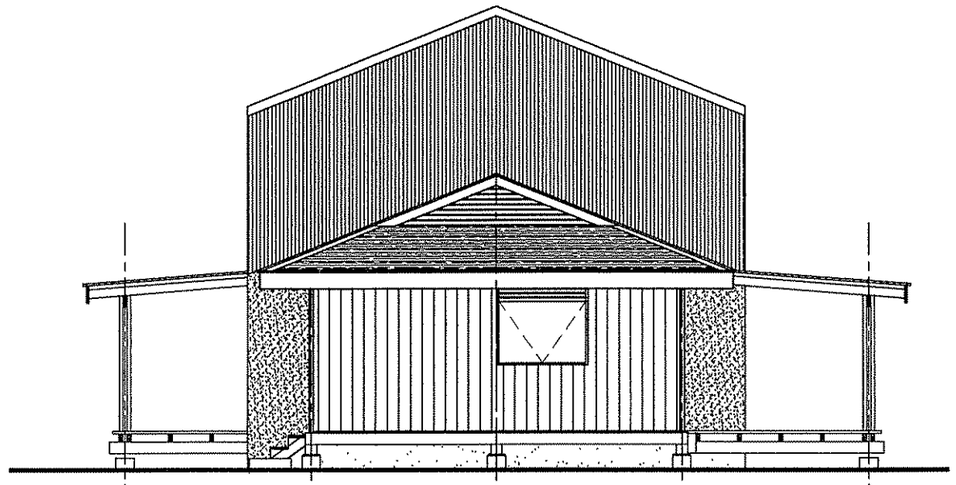
ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME

FACADE TYPE

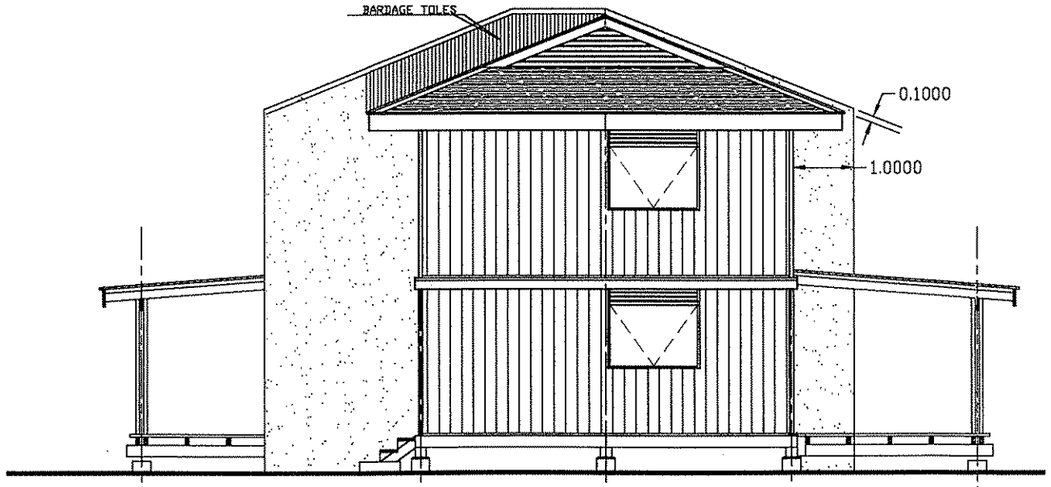
Ech : 1/100



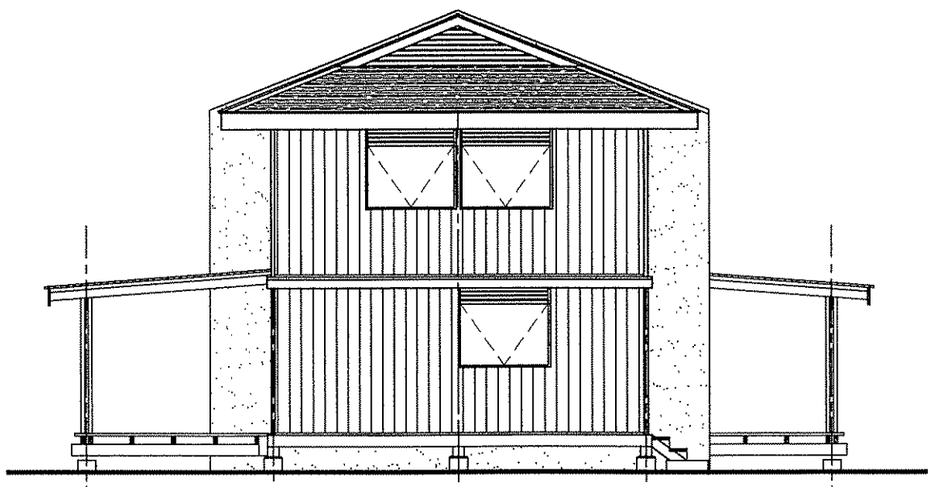
ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME



PIGNON ℄AUCHE F2

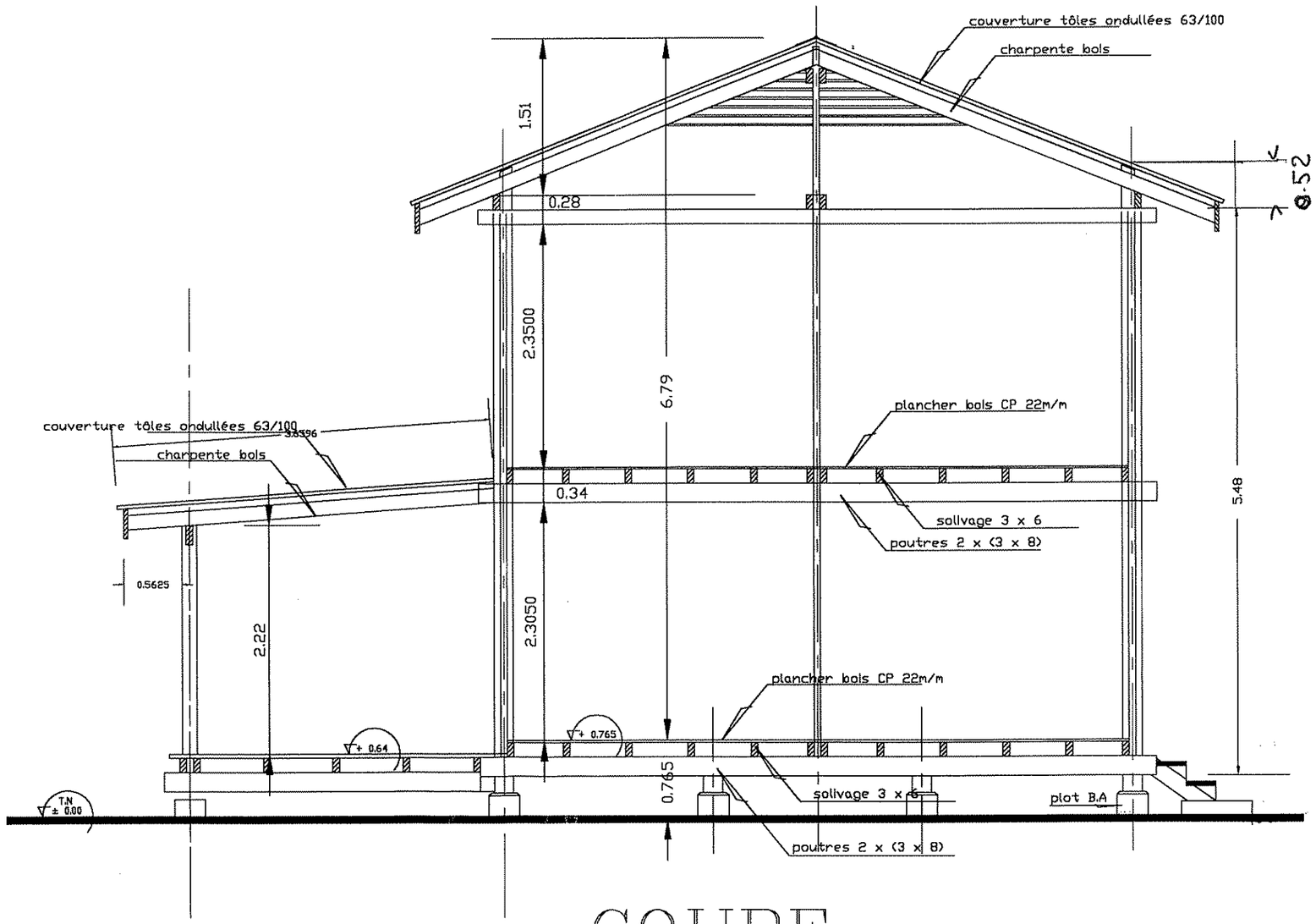


PIGNON ℄AUCHE



PIGNON DROIT

ARRIVÉE
N ...../AU
26 JAN. 2001
Section UOC
URBANISME



COUPE

ARRIVÉE
N ...../AU
26 JAN. 2001
Section Plans
Urbanisme

AVIS FAVORABLE
OPT/CCL/ENSIM
Sous réserve de présentation avant le début des travaux, d'un projet détaillé d'infrastructure téléphonique établi par une entreprise admise par l'OPT

17 JANV. 2001
O.P.T. - C.C.L.
IMMOBILIER

K. 314
K. 315
K. 348
K. 415
K. 416
K. 349
K. 345
K. 346
K. 159
69
5.0198
5.3706
5.0923
7.2524
6.6258
8.0043
5.1744
5.1974
4.6427
1.2580
8.0890
SORTIE
ROUTE DE 3.50m
CANIVEAU 40X40
Limite par application cadastrale
Tube
Tube existant
Tubg
Spit
F5D
F4D
F3T

IMPLATATION
Ech : 1/250

CONCOURS D'INGENIEUR EN CHEF 1ère CATEGORIE 2ème CLASSE
Spécialité halieutique

VENDREDI 15 FEVRIER 2002 DE 8H00 A 12H00 (4 HEURES)

Sujet :

Etablissez en 4 pages maximum une note de synthèse sur les possibilités de développement de la pêche aux îles Marquises : quelles opportunités pour la pêche artisanale locale (petites unités basées aux Marquises), la pêche semi-industrielle (bateaux opérant aux Marquises mais qui débarquent à Papeete) et la pêche industrielle (bateaux pêchant ou non aux Marquises mais qui peuvent tirer partie d'une présence dans la zone) ?
A partir des informations que vous trouverez dans les documents , rédigez une note de synthèse sur la situation actuelle de la pêche aux Marquises et dégagez les options possibles pour le développement des trois types de pêche cités précédemment en donnant pour chacun votre appréciation de la faisabilité économique et technique des options.

Dossier :

Service de la Pêche

Coopérative de Pêcheurs MOKAI

Taiohae

Nuku Hiva

Iles Marquises

Etude d'un projet de développement

De l'activité de la flottille

Création d'une unité de Mareyage à Taiohae

Dossier P.A.S. n° 151
Juin 2001

SOMMAIRE

Préambule

La morphologie de ses îles et son relatif éloignement de Tahiti font que l'archipel des îles Marquises doit faire face à de fortes contraintes techniques et économiques pour assurer son développement, en particulier dans la filière pêche.

Il semble opportun de rappeler q'une étude (*) financée par le Fond Européen de Développement (FED) et réalisée en 1998 par la société COFREPECHE à mis en évidence :

- que l'archipel des Marquises se situait dans une zone ayant un fort potentiel de ressources halieutiques,

- que jusque dans un récent passé, une partie de ces ressources a été exploitée par des flottilles industrielles étrangères (Japon, Corée),

- que l'exploitation de cette ressource, hauturière par les Marquisiens, nécessitait la mise en œuvre d'un important programme d'investissements (infrastructures terrestres, flottille).

Dans les années 90, plusieurs coopératives de pêcheurs ont exploité la ressource thonière de proximité.
Utilisant alors des moyens de captures artisanaux (pirogues, kau), et en valorisant localement le poisson par la production de longes de thon congelées qui étaient commercialisées sur le marché tahitien.
Cette filière a expédié jusqu'à 16 tonnes par mois vers Tahiti.

La montée en puissance de la flottille des palangriers congélateurs basée à Tahiti a fait rapidement péricliter cette activité, par la mise sur le marché de produits de meilleure qualité (surgélation bord) et à des prix plus compétitifs.

L'activité de pêche qui subsiste actuellement, pourrait être qualifiée de vivrière, sans une réelle visibilité de développement .

Forte de ce constat, la Coopérative des Pêcheurs et Aquaculteurs de MOKAI , basée à Taiohae, a sollicité le concours du Service Territorial de la Pêche, afin d'analyser les possibilités de dynamiser cette activité et d'examiner les perspectives de développement sur le moyen, voir le long terme.

La présente étude, à pour objectif de répondre à cette attente.

(*) Etude de faisabilité de la commercialisation des produits de la Mer à partir des îles Marquises.

Chapitre 1

Situation actuelle

Chapitre 1 – Situation actuelle

1 – La ressource humaine

Le nombre d'adhérents à la Coopérative MOKAI est de 56 à fin juin 2001. (cf liste nominative jointe en annexe)

Il convient cependant de distinguer trois catégories :

- **Les pêcheurs professionnels** au nombre de 14, tous propriétaires de leur bateau (Kau, Poti Marara, Bonitier), ont une licence de pêche qui leur permet de bénéficier des exonérations réglementaires dont l'exonération de taxe sur le carburant.
- **Les pêcheurs amateurs** au nombre de 12, n'ont pas de licence de pêche.
  Ils n'exercent pas à proprement parler une activité professionnelle dans la filière pêche, mais cependant commercialisent leur captures à des tiers.
  La plus part des membres de cette catégorie, ont un emploi stable dans l'administration.
- **Les adhérents sympathisant** au nombre de 30, dont la quasi totalité n'ont pas d'embarcations .

Il est clair que les pêcheurs professionnels ne sont pas majoritaires, et que compte tenu du statut des coopératives (un adhérent = une voix), ceci puisse poser problème lors du vote de certaines résolutions en assemblée générale.

2 – Les moyens de la Coopérative MOKAI

La coopérative ne possède pas de moyens de production en propre. Chaque adhérent est propriétaire de son embarcation.

Elle est dépositaire d'une machine de production de glace en paillette, propriété du Territoire.
Cette machine d'une capacité de 0,8-1 tonne/jour , a été entièrement révisée à Papeete en juin 2000, puis réexpédiée à Taiohae en août.
Depuis son retour , réinstallée sur son silo, elle est en attente de raccordement à son alimentation en eau douce, et à son compteur électrique.
L'ancien président en assurait bénévolement le bon fonctionnement technique et son exploitation commerciale. Depuis son départ il ne semble pas y avoir une volonté clairement exprimée de la remettre en activité.
Les pêcheurs s'approvisionnent actuellement en glace de médiocre qualité, et au prix fort, auprès d'un magasin du village.

La coopérative n'assure pas non plus l'avitaillement en équipements de pêche (hameçon, nylon) auprès de ses adhérents. Ceux-ci en sont réduit à s'approvisionner au magasin , à des prix qui sont 4 à 5 fois supérieurs à ceux pratiqués à la vente en gros à Papeete.

La coopérative n'est pas impliquée dans la commercialisation des produits de la pêche. Son rôle semblant être de fixer un seuil de prix de vente (cf paragraphe 6).

Il ne fait aucun doute que dans la situation présente, la coopérative MOKAI, manque de moyens financiers, et que ce manque de solvabilité conduit

probablement certains fournisseurs à arrêter toute prestation , comme la fourniture d'énergie électrique pour la machine à glace.

Dans ce contexte, la coopérative fonctionne plus comme une « association amicale », ce qui est au demeurant fort sympathique, que comme une coopérative de production.

3 – L'outil de production

Les embarcations basées à Taiohae sont dans l'ensemble de dimensions modestes.

Nous dénombrons armés par :

- Pêcheurs professionnels :
  - . 2 bonitiers
  - . 7 Kau (speed boat)
  - . 4 Poti Marara
- Pêcheurs amateurs :
  - . 1 vedette
  - . 1 pirogue
  - . 5 Kau (speed boat)
- Membres adhérents :
  - . 2 Kau (speed boat)
  - . 1 Poti Marara

Dans l'ensemble ces unités sont opérationnelles.

4 – Les méthodes de pêche

Nous identifions trois méthodes de pêche :

- la chasse sous-marine, le long des falaises et dans les grottes (langoustes, perroquets, ihi)

- La pêche à la palangrotte de fond (150-250 mètres) concerne essentiellement la capture des espèces suivantes :
  - . Otu (loche)
  - . Haka
  - . Merou
  - . Paru (Matu vii)
  - . MoaKeka
  - . Matueka

- La ligne de fond pour la pêche aux thons (20-50 mètres)
  Les appâts utilisés sont des petits pélagiques, suivant disponibilité saisonnière (Orare, Operu, Sardine, Ature). Ces appâts sont pêchés dans les fonds des baies.

5 – Organisation de la pêcherie

Le plus souvent, plusieurs méthodes de pêche sont mises en œuvre au cours d'une « sortie de pêche ».

Pour les plus grosses unités ont peut identifier la séquence suivante :
Départ le matin, pêche à la palangrotte aux poissons de fond au cours de la journée, puis à partir de 18h jusqu'à 20h, pêche à la ligne de fond sur les bancs de petits thonidés (essentiellement Yellowfin), après 20h pêche aux lhi, langoustes jusqu'à environ 3h du matin ou la pêche aux thonidés peut alors reprendre jusqu'au levé du soleil. Ensuite retour à Taiohae pour la vente des produits vers 6h.

Les plus petites unités partent le soir pour pratiquer uniquement une pêche de nuit.

La zone de pêche traditionnelle des unités basées à Taiohae, couvre toute la partie Sud et Nord-Ouest de l'île , depuis la baie du contrôleur au Sud-Est , jusqu'à l'aéroport au Nord –Ouest.
Deux à trois par an , certains bateaux vont pêcher à Motu iti et Eiao pour la capture de poissons de fond, bec de cannes (Oeo) et carangues sur les haut-fonds à l'Est de Eiao.
Motu iti et Eiao sont revendiqués comme territoires de pêche des pêcheurs de Taiohae.

Les pêcheurs professionnels sortent en général deux fois par semaine , le mardi et le vendredi pour des ventes respectivement le mercredi et le samedi matin.
Le plus souvent, la production est limitée à la capacité d'absorption instantané du marché. A certaines périodes de l'année les pêcheurs reconnaissent qu'ils pourraient pêcher beaucoup plus de thons, mais que faute d'un marché suffisant, 'ils ont tendance à restreindre les captures aux quantités commandées.

Les rendements annoncés sont d'environ 100 kg de poissons de fond, et 200 à 300 kg de thonidés par sortie .
En deux jours de pêche à Eiao, un poti marara , peut capturer 600 à 700 kg de poissons de fond.

Concernant les poissons de fond, Il convient de relativiser ces rendements, car cette pêcherie s'exerce sur un stock vierge, et de façon très ponctuelle.

6 - La commercialisation

La coopérative n'intervient pas dans le processus de commercialisation, excepté dans la fixation d'un tarif pour la première vente, lequel est appliqué par les pêcheurs lors de la vente de leur produits à leurs clients.

Les prix pratiqués sont :

- 500 CFP/kg pour les poissons de pêche sous-marine,
- 400 CFP/kg toutes espèces (et produits) confondus pour les poissons pêchés à la ligne,
- 1500 CFP/kg pour les langoustes (quelque soit la taille)

La première vente à lieu sur le quai du débarcadère de Taiohae, sans aucun respect des mesures d'hygiène les plus élémentaires (la découpe entre autre du poisson à même le quai).

Les poissons de fond sont vendus entier vidé ou non, mis en glacière avec un peu de glace de mauvaise qualité.

Les thonidés :

. essentiellement des petits Yellowfin de 12-14kg, qui sont vendus entier vidé (bonitier) ou non vidé (autres bateaux).

Ils sont parfois découpés sur le quai en demi poisson dans le sens longitudinal. Dans ce dernier cas une moitié est vendue avec les arêtes et la tête, le prix de vente au kg restant inchangé !.

. Bonites vendues entières vidées.

Si la première vente ne permet pas l'écoulement de la totalité de la production du jour, le surplus est vendu au porte à porte, probablement à des prix inférieurs à ceux du tarif officiel.

De l'avis de la plupart des consommateurs (cantines scolaires, restaurateurs, particuliers) il existe un paradoxe de surproduction hebdomadaire ponctuelle (apports limités à deux jours par semaine, mercredi et samedi), et de pénurie chronique de produits compte tenu de l'absence de moyens terrestre (chambre froide, glace) de traitement et conservation des produits .

A noter qu'en plus du marché local d'autoconsommation, il existe des courants de commercialisation à « l'export » vers certaines autres îles de l'archipel et vers Tahiti.

L'importance de ces courants commerciaux est très difficile à quantifier, certains pêcheurs s'exprimant en plusieurs tonnes par semaine, d'autres en centaines de kg.

Il est certain que du poisson frais est expédié à chaque passage de goélette, en particulier vers UA POU, UA UKA et HIVA OA.

Ceci concerne aussi bien du thon que des poissons de fond , expédiés sur glace en glacière.

Ce flux commercial se situe dans une fourchette de 3 à 13 tonnes par mois, très dépendant du cycle d'activité scolaire (restauration collèges, écoles)

Un courant de commercialisation sur Tahiti , vers la diaspora Marquisienne.

Le tonnage expédié par goélette serait de 1 à 1,5 tonnes, toutes espèces confondues, y compris les langoustes. La plupart de ces produits sont expédiés congelés (filets de thon mis en congélateurs ménagés).

Enfin il convient de mentionner des essais de commercialisation de poissons de fond avec un mareyeur Tahitien (Fenua Fish).

Ces poissons dans un premier temps étaient expédiés en glacière de grande capacité (1m3) par goélette, puis dans un deuxième temps par avion pour les espèces plus nobles (ihi, paru).

Dans les deux cas des problèmes essentiellement d'ordre logistique (manque de coordination des pêcheurs, absence de glace en quantité suffisante, manque de capacité de fret sur AIR TAHITI) n'ont pas permis de pérenniser cette activité commerciale.

7 - Conclusions

En première analyse il ressort :

- Une forte motivation de la catégorie des pêcheurs professionnels à vouloir :
  - . développer leur activité par une meilleure valorisation de leur outil de production,
  - . créer des emplois pour leurs enfants,

- Que la flottille existante, est dans son ensemble opérationnelle, mais en sous activité constante.

- Hormis le fait d'avoir suscité cette étude, la Coopérative est actuellement au point mort, et n'assure même pas l'une de ses fonctions essentielles qui est la production de glace pour ses adhérents.

- La filière « survie » dans un système archaïque de production commercialisation caractéristique d'une pêcherie vivrière.
  De ce fait elle apparaît comme peu attractive aux jeunes générations, tant sur les aspects techniques par rapport à la pêche hauturière à la palangre, qu'économiques (revenus trop faibles).

- Faute d'outil de conservation, traitement à terre, la production est Directement soumise à la demande journalière plus ou moins bien Exprimée par les consommateurs de proximité.
  Logique décisionnelle de production d'une pure économie vivrière.

- Le système de commercialisation avec tarif imposé, correspond à cette Logique de production vivrière basée sur l'adéquation constante entre L'offre et la demande et où le marché n'existe plus.
  Le tarif imposé par la Coopérative ne vise qu'à protéger le pêcheur des effets d'une éventuelle surproduction. Mais il conduit dans le même temps à un nivellement par le bas de la qualité, et à un manque certain d'innovations sur les produits.
  Le gommage de ces deux facteurs essentiels au développement d'un marché quelqu' il soit, aboutit à une sclérose générale de la filière.

La situation actuelle sans être critique, peut être considérée comme inquiétante.

Elle ne peut perdurer très longtemps sans que l'on observe un déclin de l'activité pêche, comme cela s'est déjà produit sur d'autres îles de l'archipel des Marquises.

Des solutions sont possibles pour re dynamiser cette activité économique, assurer son développement et sa pérennité.

Ces solutions dans leurs mise en œuvres toucheront des aspects techniques, financiers, commerciaux, mais essentiellement humains.

Les acteurs économiques de la filière et au premier chef, les pêcheurs devront se remettre profondément en cause pour passer d'une économie de production vivrière,
À celle d'une économie libérale de marché.

Chapitre 2

Proposition de Projet

Chapitre 2 – Proposition de Projet

Compte tenu de l'analyse qui a pu être faite de la situation actuelle et des conclusions que nous avons pu exprimer, nous pensons qu'un projet de développement de l'activité pêche peut se concrétiser à Taiohae, mais que celui-ci devra se bâtir en différentes étapes. Les résultats acquis à chaque étape devront valider le passage à l'étape suivante.

1 – Les objectifs du projet de développement

Les objectifs devront prendre en compte :

a) les aspirations pour un développement de la filière pêche, exprimées par les pêcheurs de Taiohae.
Développement pour eux-mêmes à très court terme et pour leurs enfants à moyen et long termes,

b) la politique de développement du Territoire, pour l'exploitation de la ressource halieutique de la Zone Economique Exclusive (planification, aides financières, formation)

c) une intégration de la production marquisienne dans les filières commerciales existantes, ou à créer, des produits de la pêche polynésienne, en particulier pour les filières à l'exportation,

d) la capacité de financement des investisseurs Marquisiens qui seront désireux de s'impliquer dans cette filière économique.

Le projet tel que nous le percevons aujourd'hui pourrait se développer en deux étapes :

première étape à court terme :

Augmentation de la productivité de la flottille actuelle dans son environnement de pêcheries pélagique et démersale cotière, par la commercialisation des captures dans le cadre d'une économie de marché.

deuxième étape à moyen terme :

Investissement dans une flottille de pêche hauturière, avec mise en activité d'une pêcherie palangrière dont la production sera essentiellement destinée à l'exportation sur les marchés internationaux.

2 – Le projet pour la première étape du développement

2.1 - Les objectifs :

a) Faire évoluer la filière pêche d'une économie vivrière à une économie de marché, en alimentant à satiété le marché local de proximité (Taiohae, Taipivai) par une offre améliorée tant sur l'aspect quantitatif que sur l'aspect qualitatif (diversification des produits).
b) Accentuer la commercialisation sur les autres îles de l'archipel Marquisien, par une augmentation du volume de production, et également par une diversification de l'offre par des produits stabilisés (filets congelés), tout en respectant l'écoulement en frais des petites productions des pêcheurs locaux.
c) Réamorcer l' "*exportation*" vers Tahiti des espèces récifales (Paru, Ihi, Carangues, Haapu etc ...).

Ces objectifs sont des objectifs à court terme, qui permettront à l'actuelle génération des pêcheurs professionnels de :
- Développer et gérer leur activité dans le cadre d'une économie de marché,
D'augmenter leur revenu par une meilleure productivité de leur outil de travail,
d) D'apprendre à valoriser les captures par la mise en œuvre des règles sanitaires et d'hygiènes requises pour la conservation et la transformation des produits.
e) De préparer l'avenir, pour une possible évolution vers une pêcherie palangrière hauturière.

2.2 – Identification des marchés :

Afin d'avoir une appréciation cohérente des marchés, nous exprimerons les produits dans leur unité de mesure de commercialisation, que nous transformerons en Equivalent Poisson Entier (E.P.E.), prenant en compte les coefficients de transformation usuels.

2.2.1. – Le Marché de Nuku Hiva :

Nous entendons par marché de Nuku Hiva, pour l'essentiel celui de Taiohae , point de débarquement, étendu au village de Taipivai.

a) situation actuelle :

Restauration collective

. Cantines scolaires (collège + école primaire = 620 élèves)
2 repas/semaine x 125g filet thon x 36 semaines = 5.580 kg filet/an

. Hopital : 30 personnes x 3 repas/semaines x 110g x 52 semaines = 515 kg filet/an

Restauration

. Hotels : toutes espèces confondues 60 à 100 kg / semaine poissons entiers vidés, soit pour deux unités hotelières :
2 x 52 semaines x 80kg = 8.320 kg/an (poisson entier vidé)

. Restaurant : toutes espèces confondues 40 kg/semaine
1x52 semaines x 40 kg = 2.080 kg/an (poisson entier vidé)

Particuliers Taiohae

. Autoconsommation 500 kg/ semaine, poisson entier vidé, toutes espèces confondues.
. Congélation familiale pour expédition sur Papeete : 1.000 kg filet thon et 200 à 500 kg poissons de fond par mois.

b) Perspectives à terme de trois ans :

- Notre analyse de la croissance de ce marché repose sur :

. les observations constatés du marché Tahitien, face à une offre constante, à une diversification des produits, et intègre leur distribution à Taipivai.
. sur une croissance de 30% de l'activité touristique
. sur la distribution de nouveaux produits type plats à emporter (poisson crue, poisson au carry, brochettes, filet frais portion, etc ....) conditionnés en barquette filmée.

Restauration collective

. Cantines scolaires (750 élèves)
2,5 repas par semaine x 125g filet thon x 36 semaines = 8.438 kg filet de thon /an
. Hopital : inchangé 515 kg filet de thon an

Restauration

. Hotels : 130 kg par semaine, dont 2/3 filet de thon, 1/3 poissons de fond entier vidé
52 semaines x 130 kg x 2/3 = 4530 kg filet de thon par an
52 semaines x 130 kg x 1/3 = 2253 kg poisson fond entier vidé

. Restaurants et roulottes (4 unités) : 25 kg filet par semaine
52 semaines x 25 kg = 1.300 kg/an
(dont 2/3 filets de thon, 1/3 poissons de fond entier vidé)
. Plats à emporter 10 kg/jour filet de thon
312 jours x 10kg = 3.120 kg filets de thon/an

Particuliers Taiohae et Taipivai

. autoconsommation familiale : 500 kg/semaine filets thon, et 100 kg/semaine poissons entier vidé autres espèces.
. expédition familiale vers Papeete : 1.200 kg filets de thon congelés par mois, 600 kg poissons de fond par mois.

2.2.2. – Le marché Marquisien

Nous considérons comme marché Marquisien , celui des autres îles de l'archipel.

Trois îles sont essentiellement concernées : Ua Pou, Hiva Oa, Ua Huka.

Ces trois îles font actuellement l'objet de ventes plus ou moins régulières de produits de la pêche des producteurs de Taiohae. Ces ventes sont faites soit par débarquement direct des pêcheurs (Ua Huka, Ua Pou) ou le plus souvent par expéditions sur les goélettes lors de leur circuit inter-îles (ARANUI, TAPORO VI).

À noter qu'une partie des besoins de la restauration hôtelière de ces îles est actuellement assurée par des filets de poissons congelés bord en provenance de Tahiti.

Il existe donc un marché potentiel de substitution pour peu de pouvoir offrir des produits de qualité équivalente.

a) Situation actuelle :

Marché de Ua Pou : 4 à 5 tonnes par mois de thons (80%) et de poissons de fond (entier, vidé) pour les écoles, le SMA,et les particuliers.

Marché de Ua Uka : 250 kg par semaine de thons pour les écoles soit
250kg x 36 semaines = 9.000 kg / an

Marché de Hiva Oa : 2 à 4 tonnes par mois de thons (90%) et de poissons de fond (entier, vidé) pour les écoles, le SMA, les pensions de familles, et les particuliers.
Soit environ : 3t x 12 mois = 36t/an

b) Perspectives à terme de trois ans :

Nous avons pris en compte une croissance de 15% du marché sur trois ans.

Marché de Ua Pou : 26,33 tonnes par an de filets de thon
10,8 tonnes par an de poisson de fond (entier, vidé)

Marché de Ua Uka : 5,48 tonnes par an de filet de thon

Marché de Hiva Oa : 19,75 tonnes par an de filets de thon,
3,6 tonnes par an de poisson de fond (entier, vidé)

2.2.3. – Le marché Tahitien

La production actuelle de thonidés concerne essentiellement la pêche de petits « Yellowfin » de 12 à 20 kg de poids vif. Cette catégorie intéresse peu le marché tahitien du frais.

La mise en service de palangriers de pêche fraîche pourrait modifier cette situation en autorisant la capture au large de « Yellowfin » et de « Big Eye » de taille plus conséquente, dont on pourrait alors envisager le transport en frais par avion sur Papeete.

En première approche, seuls les poissons de fond semblent avoir un intérêt économique pour une commercialisation en frais (vidé entier) sur Papeete, ou fileté congelé pour les plus grosses pièces.

Le transport des produits frais par avion, est actuellement trop aléatoire (priorité aux passagers) pour être envisagé de façon régulière.

Il faudrait atteindre une masse critique de produits (agricole, pêche) et une régularité de production suffisante pour qu'AIR TAHITI puisse envisager un vol de nuit tout cargo par ATR 72-211 dont la cellule de type « quick change » en permet une exploitation polyvalente.

La capacité d'emport maximum d'un tel appareil sur la ligne Nuku Hiva – Papeete est de 6 tonnes.

Le transport des produits frais sur glace en glacière est possible par voie maritime.

Des essais réalisés par des mareyeurs ont été satisfaisants. Ces expéditions n'ont pu se pérenniser faute de régularité dans la production.

Une troisième voie pourrait être la congélation sur place de ces espèces. Le transport maritime par goélettes ne présentant aucune difficulté .

a) Situation actuelle :

Hormis quelques expéditions épisodiques de langoustes congelées, et de filets de thon pour l'autoconsommation des familles marquisiennes résidantes à Tahiti (cf. marché de Taiohae 2.2.1.), il n'y a plus d'expédition à caractère commercial de produits de la pêche marquisiens vers Tahiti.

b) Perspectives à terme de trois ans :

Le marché Tahitien , est soumis à un déficit chronique d'approvisionnement en poissons d'origines récifale et lagonaire.

Ce déficit est dû d'une part à une surexploitation de certains atolls, et d'autre part à une très nette baisse d'activité des parcs, au profit des fermes perlières.

Il est possible que compte tenu de la crise que subit actuellement le secteur perlier, crise qui se traduit par de nombreux licenciements dans les fermes, une partie de la population des Tuamotu réactive l'exploitation des parcs laissés à l'abandon.

Cependant même si un sursaut conjoncturel de la production des Tuamotu puisse être observé à court terme, sur le moyen et long terme cette production restera orienter à la baisse.

Pour peu qu'elle soit convenablement gérée, la pêcherie marquisienne dont le stock est quasiment vierge, pourrait se substituer partiellement à celle des Tuamotu, et répondre à la croissance régulière du marché pour des produits de qualité, en particulier pour le marché de la restauration hôtelière.

Notre analyse est qu'il semble possible de commercialiser en produits de qualité , 1tonne à 1,2 tonnes par semaine, de produits frais et congelés, filetés ou non suivant la taille et/ou les espèces.

2.2.4 – Conclusions sur les marchés

Nos conclusions sont de différents ordres :

- Le marché local (Taiohae, Taipivai) et le marché marquisien ne sont pas saturés, et sont porteurs dans la mesure ou l'offre pourra se diversifier sur des produits plus élaborés et plus diversifiés en termes d'espèces.

- Le marché Tahitien devra être abordé avec beaucoup plus de prudence, en particulier pour la commercialisation de thons frais.

En effet la prochaine mise en exploitation à Tahiti de nombreux palangriers de pêche fraîche devrait conduire pour certains produits, dont les thons de faible taille, à une certaine saturation du marché local.

Le marché Tahitien du frais à l'export devrait alors se développer de façon conséquente.

Il convient cependant de souligner que ce marché est plus exigeant en terme de qualité que le marché local. Pour exemple les « Yellowfin » d'origine marquisienne de moins de 30 kg ont peu de chance de pouvoir se positionner de façon rentable sur ce segment de marché.

Estimation du marché actuel

Espèces-produits	Marché local		Marché Marquisien	Marché Tahitien	Coeff transformation	E.P.E. (tonne/an)
	Restauration	Familial				
Thons (entier vidé)	18,4	17,3	84,6		0,95	126,66
Thons (filet)		12,0			0,53	22,64
Espèces de fond (e.v.)	3,4	14,7	14,4		0,97	33,51
Langoustes	3,0	2,0		4,0	1	9,00
					Total E.P.E. =	191,81

Perspectives du marché à fin 2004

Espèces-produits	Marché local		Marché Marquisien	Marché Tahitien	Coeff transformation	E.P.E. (tonne/an)
	Restauration	Familial				
Thons (entier vidé)					0,95	0,00
Thons (filet)	16,4	40,4	51,5		0,53	204,40
Espèces de fond (e.v.)	3,7	12,4	16,6	18	0,97	52,23
Espèces de fond (filet)				13	0,45	28,89
Langoustes	4			6	1	10,00
					Total E.P.E. =	295,51

Les poids sont exprimés en tonne
E.P.E. : Equivalent Poisson Entier

Le marché Tahitien des espèces démersales et récifales, offre de belles perspectives à une production d'origine marquisienne.

Ceci, pour peu que ces produits soient de qualité (frais et congelés) de façon à se démarquer des produits en provenance des Tuamotu, et qu'ils puissent approvisionner le marché de façon régulière.

Globalement les marchés apportent une réponse positive à la question posée sur la faisabilité de passer d'une économie de filière vivrière, à celle d'une économie de marché.

Les points qui restent à examiner sont :

. l'adéquation ou non de la flottille existante (aspects quantitatif et qualitatif)
. la définition d'un outil de mareyage,
. les moyens nécessaires à la mise en œuvre d'une stratégie de développement (formation, suivi de la ressource démersale et récifale, assistance à la gestion etc...)

2.3 – La Flottille

2.3.1 – Sa capacité de production

La flottille a été identifiée par l'inventaire communiqué par la Coopérative Mokai.

Nous prendrons en compte les deux groupes de bateaux appartenants aux pêcheurs professionnels, et aux pêcheurs amateurs dont l'activité essentiellement de week-end, participe à alimenter le marché local de Taiohae.

Pour la flottille professionnelle, les hypothèses d'utilisation suivantes ont été prises en compte :

- Arrêt technique et mauvais temps : 7 semaines par an
- Déplacement sur pêcherie de Eiaho et banc Clark : 10 déplacements d'une semaine par an pour les bonitiers , et 8 déplacements par an (suivant état de la mer) pour les Kau et les Poti Marara.
- Nombre de sorties le long des falaises de Nuku Hiva : en moyenne 105 par an (trois fois par semaine).

En ce qui concerne la flottille des pêcheurs amateurs, a été prise en compte une moyenne de deux sorties par mois.

Pour chaque catégorie, la capacité annuelle de production, a été résumée dans les tableaux suivants :

Capacité de production de la flottille existante

Pêcheurs professionnels	Nombre	Thons		Poissons de fond falaise Nuku Hiva		Poissons de fond Eiaho		Langoustes	
Type bateau	bateau	N. sortie	quantité	N. sortie	quantité	N.sortie	quantité	N.sortie	quantité
Bonitiers	2	105	450	105	80	10	800	10	100
Kau (speed boat)	7	105	200	105	80	8	500	10	100
Poti Marara	4	105	200	105	50	8	400	10	100
E.P.E. (tonne/an)			326		97		57		13

Pêcheurs amateurs	Nombre	Thons		Poissons de fond falaise Nuku Hiva		Poissons de fond Eiaho		Langoustes	
Type bateau	bateau	N. sortie	quantité	N. sortie	quantité	N.sortie	quantité	N.sortie	quantité
vedette	1	24	50	24	20	0	0	5	30
pirogue	1	24	30	24	20	0	0	5	30
Kau (speed boat)	5	24	50	24	20	0	0	5	30
E.P.E. (tonne/an)			8		3		0		1

Si l'on prend en compte un facteur de 80% d' "opérationalité" par rapport à la capacité théorique, cette flottille aurait une capacité de production annuelle de :

Thons : (326 + 8) x80% = 267 tonnes
Poissons de fond : (97+57+3) x 80% = 126 tonnes
Langoustes : (13+1) x 80% = 11,2 tonnes.

Il est clair que cette flottille est largement surdimensionnée pour alimenter le marché actuel, et que sa capacité de production sera en meilleure adéquation avec les hypothèses de marché prises en compte dans le schéma de développement envisagé.

L'approvisionnement de ces marchés tel que nous le percevons à l'horizon 2004, permettra globalement d'améliorer d'environ 54% le taux d'utilisation de cette flottille, sans saturer sa capacité de capture sur la pêcherie des thonidés.

Le taux opérationnel d'utilisation de cette flottille serait alors de 73% (pour 47,5% actuellement).

Concernant la capacité de production, nous pouvons conclure à son adéquation avec le développement envisagé du marché.

2.3.2 – Aspect qualitatif

On observe une grande hétérogénéité tant dans la taille que dans la forme des embarcations.

D'une façon générale, elles sont bien entretenues. Mais cependant le traitement et la conservation à bord du poisson, ne semble pas être une préoccupation majeure des pêcheurs.

Il conviendra :

- *d'équiper de glacières de volumes appropriés à chaque bateau pour conserver le poisson sur glace jusqu'au moment de son débarquement,*

- *de réactiver la production de glace en écaille,*

- *de former les équipages aux règles élémentaires de conservation du poisson (éviscération, glaçage).*

2.4 – L'unité de mareyage

Le développement des ventes sur le marché local, le marché marquisien, et dans une moindre mesure le marché tahitien, passe obligatoirement par une augmentation de l'offre et par un élargissement de la gamme des produits (filets, plats à emporter etc...).

L'amélioration de l'offre peut être obtenu par une plus grande régularité des apports, mais aussi par la constitution de stocks de produits stabilisés (congélation par exemple).

L'élargissement de la gamme de produits, par la transformation localement d'une partie de la production (filetage, plats cuisinés à emporter).

L'opération de transformation apportant une plus value localement.

Ces objectifs ne pourront être tenus, que par la création d'une véritable unité de mareyage qui regroupera les fonctions suivantes :

- réception du poisson (pesage après déglaçage, examen visuel qualitatif, tri par espèce, glaçage et entreposage tampon en chambre froide avant transformation éventuelle et commercialisation,
- un atelier de filetage,
- un tunnel de congélation à air pulsé,
- une chambre froide négative pour le stockage des produits congelés,
- un espace de vente au détail,
- un bureau,
- un bloc sanitaire pour le personnel,
- une unité de production de glace en écaille.

2.4.1 – Positionnement de l'unité de mareyage

Pour des raisons nautiques, l'ensemble de la flottille de pêche débarque ses prises au vieux quai de Taiohae. Le nouveau quai, de par sa conception et son implantation est trop soumis à l'action de la houle, et n'est absolument pas adapté à l'amarrage ce type de petits bateaux.

Compte tenu de l'exiguïté de l'espace disponible au vieux quai de Taiohae, une solution consisterait à réaménager le hangar désaffecté, situé en partie haute de la plate-forme portuaire.
Ce hangar est propriété du Service de l'Equipement, qui est d'accord pour en assurer sa réhabilitation et une nouvelle affectation à l'unité de mareyage.

2.4.2 – Dimensionnement

L'unité de mareyage doit être dimensionné pour traiter un volume annuel d'environ 300 tonnes de poissons.

La livraison de ces 300 tonnes s'effectuant sur 200 jours par an.

Soit une capacité moyenne journalière de réception de 1,5 tonnes.

Compte tenu du problème de cumul de certains apports par rapport au nombre de bateaux en activité(13 unités pêcheurs professionnels) , nous considérerons un coefficient de foisonnement des apports égal à 10%, soit une capacité journalière de réception de 1,5 t x 1,10 = 1,65 tonnes.

a) Volume de stockage de la chambre froide tampon :

Densité de stockage poisson en bac sur glace : 300 kg/m 3
Volume requis de stockage 1650 kg/300 = 5,5 m3
Volume brut chambre froide : 5,5m3 x 2,5 = 13,75 m3

b) Surface salle de filetage :

Quantité à fileter en 7 h de travail :
1tonne de thon + 150 kg poisson de fond
➔ trois personnes en travail simultané
Surface minimum requise : 12 m2
Une déchèterie sera mitoyenne de la salle de filetage

c) Capacité du tunnel de congélation :

75 t/an de filets de thon + 20 t/an de filets poisson de fond = 95 t/an
temps de congélation à –40°c : 6 h (pour une température d'introduction inférieure à +4°c)
poids moyen journalier : 95t /200 j = 475 kg/cycle
capacité par cycle de congélation : 475 kg x 1,1 = 522 kg/cycle

La capacité de congélation, élément majeur de la stabilisation des produits, ne doit pas être un facteur limitant, aussi nous convenons de la surdimensionnée à une capacité de 600 kg/cycle.
En cas de débarquements journaliers très importants, l'unité de filetage et de congélation pourra travailler en deux successifs de 6 heures.

d) Chambre froide de stockage des produits congelés :

Son volume doit permettre de stocker la production destinée à l'"export" entre la rotation d'une goélette, avec un complément de stockage permanent pour le marché local (environ 300 kg).
Fréquence rotation ARANUI : 3 semaines
Production moyenne de produits congelés en trois semaines :
Poids production filets congelés : 475kg x4jx3semaines = 5700 kg
Densité de stockage : 430 kg/m3
Volume requis de stockage : (5700 + 300)/ 430 = 13,95 m3
Volume brut de stockage : 13,95 m3 x 2,5 = 35 m3

e) espace vente – poissonnerie :

installation d'un comptoir avec vitrine réfrigérée, et d'une petite chambre froide à +1°c pour le stockage des produits frais transformés en attente de distribution : surface requise 20 m2

f) Bureau :

Bureau pour la gestion de l'ensemble de l'unité mareyage.
Surface minimum : 10 m2

g) Production de glace en écaille :

L'actuelle machine Généglace a une capacité de 800 kg/jour , avec un silo de capacité utile de 2 m3.
Besoins en glace : basés sur un ratio de 1kg de glace pour 1 kg de poisson traité dans l'ensemble de la chaîne de froid (bord et unité de mareyage) soit 296 t/ an.
Tonnage qui pourra être produit en 6 jours par semaine, soit une capacité journalière requise de 950 kg/jour.
L'unité actuelle est insuffisante, et nous recommandons d'installer une deuxième unité de même capacité, ce qui aura l'avantage une capacité de secours proche du besoin journalier en cas d'arrêt pour entretien ou défaillance technique de l'une des machines.
Surface requise du local pour l'installation des deux unités de production de glace : 20 m2.

h) Bloc sanitaires – vestiaires :

Installation d'un bloc sanitaires – vestiaires, conformément aux règlements d'hygiène du travail dans la filière du mareyage.
Surface requise : 14 m2

2.4.3 - Aménagement du bâtiment existant :

Se reporter au plan en pièce jointe au présent rapport.

Le dimensionnement et l'organisation des espaces et volumes prennent en compte que les opérations de traitement et de conditionnement, seront réalisées dans le cadre d'un plan HACCP conforme aux règles d'hygiènes applicables sur le Territoire.

2.5 - Investissements :

L'estimation des investissements est résumée dans le tableau ci-après.

Nous avons distingué :

- ceux propres à la réhabilitation du bâtiment, qui pourraient pris en charge sur le budget du Service de l'Equipement,
- ceux concernant les équipements et leur installations qui seraient pris en charge par le Service de la Pêche.

Ces estimations prennent en compte une réalisation en 2002, et en particulier des nouveaux taux de TVA applicables au 1er janvier 2002.

Le montant total hors T.V.A. est estimé à 56.696.000 CFP

Se répartissant :

Budget Service de l'Equipement : 6.814.000 CFP
Budget Service de la Pêche : 49.882.000 CFP

Tableau des INVESTISSEMENTS

Investissements	Montant H.T. KCFP	Total KCFP	T.V.A. KCFP
1- Frais de 1er établissement			
Etude de faisabilité (P.A.S.)	886		58
Formation des pêcheurs (conservation poisson)	200		20
Formation du personnel de l'unité de mareyage	250		25
		1 336	
2 - Terrassements - Travaux de nettoyage			
Nettoyage terrain en arrière du bâtiment	150		15
Terrassement pour système assainisselment	240		24
Evacuation matériaux de couverture et gravats	150		15
		540	
3 - Travaux de réfection du bâtiment			
Démontage couverture	320		32
Réparation charpente	1800		180
Traitement anti-termite de la charpente	800		80
F+P cheneaux galva + descentes E.P.	600		60
Couverture, bardeaux bitumineux	2754		275
		6 274	
4 - Travaux d'aménagement du bâtiment			
Dalle béton armé	2240		224
Revêtement de sol carelage	1100		110
Maçonnerie, enduits	1800		180
Plomberie, sanitaires	850		85
Système assainissement	1200		120
Huisserie aluminium,PVC, volets roulants	970		97
Plafonds CP	650		65
Peintures	1200		120
Electricité (éclairage, PC, force froid)	2500		250
		12 510	
5 - Equipements unité mareyage			
Equipements frigorifiques (panneaux, portes,producti	19500		1950
Machine à glace, capacité 800/1000 kg/j, silo	2800		448
Tables de découpe, rayonnages	700		112
Vitrine réfrigérée	850		136
Coutellerie	80		13
Ameublement bureau	180		29
Vêtements de travail	250		40
Bacs palettes de manutention pour poissons et glace	750		120
Bascule mécanique pesée réception	1650		264
Bascule électronique poissonerie	270		43
Chariot inox pour congélation	1080		173
Boubelles	180		29
Protection incendie (extincteurs)	120		19
Transpalette manuel (2u)	320		51
		28 730	
6 - Equipements pour bateaux pêche			
Glacières	2000		
		2 000	

Tableau des INVESTISSEMENTS (suite)

Investissements	Montant H.T. KCFP	Total KCFP	T.V.A. KCFP
7 - Téléphone			
Branchement téléphonique	30		3
		30	
8 - Ingénierie			
PEO,DCE,DEO,AMT,définition équipements, plans	1800		180
Assistance technique réalisation travaux (3 missions)	840		83
		2 640	
Total partiel 1 à 8		**54 060**	
9 - Imprévus et divers (5% postes 2-8)		2 636	422
Total Général		**56 696**	6150

2.6 – Compte d'Exploitation Prévisionnel de l'unité de Mareyage

Le compte d'exploitation Prévisionnel est établi pour les trois premières années d'exploitation.

Ceci, pour être représentatif d'une montée progressive de l'activité de pêche et de commercialisation sur trois ans, à raison de 80% la première année, 90% la deuxième année et 100 % de l'objectif en année 3.

2.6.1 - Les Comptes de Charges :

2.6.1.1 – Le personnel

Nous prenons en compte que :

- le personnel sera salarié de l'unité de mareyage.
- Le poisson sera pris en charge aux pêcheurs au local réception poisson, la manutention depuis le quai étant réalisée par les pêcheurs.
- La glace est livrée au local production. La manutention jusqu'au quai est assurée par les pêcheurs.

Rémunération mensuelle brute :

. ouvrier fileteur : 120.000 CFP/mois
. Gérant : fixe 200.000 CFP/mois + prime de 1,5% sur le chiffre d'affaires

Revalorisation annuelle des salaires de 2% (ancienneté, inflation)

Nombre d'employés :

. 1ère année : 1 gérant + 2 employés
. 2ème année : 1 gérant + 3 employés
. 3ième année : 1 gérant + 3 employés

2.6.1.2 – L'Energie

Energie électrique , abonnement ELECTRA, suivant tarif n°4, 220/380V.
La puissance installée est estimée à 19 kw,
Coefficient de foisonnement : 85%
Puissance souscrite = 19 kw x 85% = 16 kw

Consommation annuelle : calculée suivant différents scenarii d'utilisation de l'unité de mareyage :

Année 1 : 57 570 kwh
Année 2 : 71 990 kwh
Année 3 : 90 000 kwh

Prix hors TVA du kwh = 38,3 CFP
Prime mensuelle d'abonnement : 232 CFP

2.6.1.3 – Emballages

Les filets seront filmés individuellement après parage et avant congélation.
Film alimentaire, d'épaisseur 16μ, en rouleau de 1.500 m
Consommation : 1 rouleau pour 1,5 tonnes de filets.
Prix du rouleau de film : 8 500 CFP

Après congélation les filets seront empaquetés dans des cartons d'environ 29kg (poids net), pour stockage en chambre froide tampon et expédition ultérieure.
Prix du carton : 275 CFP/carton

Les plats à base de poissons (essentiellement poisson cru, seront conditionnés en barquette plastique de 350g + légumes ou riz d'accompagnement.
Prix de la barquette : 25 CFP

2.6.1.4 – Télécommunications

Le démarchage et la prospection commerciale se feront essentiellement par téléphone.
Budget évolutif, fonction de l'activité.

2.6.1.5 – Achats poissons et langoustes

Les prix d'achat aux pêcheurs , pris en compte dans la présente étude, pourront paraître fixés de façon arbitraire, en réalité ils sont calculés à partir des prix de marché escomptés localement et dans les autres îles de l'archipel , ainsi que des prix parfaitement connus et établis sur le marché tahitien.

Ces prix sont rapportés au kg de poissons entier :

Thons : 290 CFP/kg (305 CFP/kg poisson vidé, G&G)
Poissons de fond de petite taille (ihi, haapu etc) : 460 CFP/kg
Poissons de fond, grosse taille pour filetage : 370 CFP/kg
Langoustes : 1 500 CFP/kg

Les pêcheurs seront payés le jour de la livraison, après pesée et identification des produits et de leur qualité.

2.6.1.6 – Fret maritime

L'ensemble des expéditions sur les marchés marquisiens et Tahitiens, se feront par voie maritime, en utilisant soit des glacières pour le poisson frais, soit les containers frigorifiques des goélettes pour les produits congelés.

Nous considérons qu'une négociation devra avoir lieu avec les armateurs pour obtenir une remise de 50% sur le tarif de fret retour sur Tahiti , et inter insulaire.
L'obtention de cette remise est indispensable au bon développement économique de la filière, et devrait pouvoir obtenir le soutien de l'administration pour sa négociation.

Tarif de fret : Taiohae – Papeete : 55 CFP/kg
Tarif de fret inter insulaire Marquises : 20 CFP/kg

2.6.1.7 – Produits d'entretien et de désinfection

Savons antibactérien, produits détergent et bactéricide pour nettoyage des sols et murs, papier de toilettes, papier essuie main jetable etc ....
Budget progressif fonction de l'activité.

2.6.1.8 – Petit outillage, papeterie

Le petit outillage, concerne essentiellement la coutellerie.
Papeterie : documents commerciaux

2.6.1.9 – Voyages

Afin de permettre le développement des marchés « export » et assurer les relations clientèles, il est prévu un budget annuel de déplacement du gérant pour deux voyages à Tahiti, ainsi que dans les autres îles de l'archipel.

2.6.1.10 – Entretien des équipements frigorifiques

Du bon fonctionnement des équipements frigorifiques dépendra la réussite du projet.
La maintenance devra être du type préventif, avec intervention dans le cadre d'un contrat de maintenance auprès d'un prestataire de service spécialisé .

Budget : 700 000 CFP les deux premières années d'exploitation
1 000 000 CFP à compter de la troisième année

2.6.1.11 – Sel pour la production de glace

Consommation : 0,42 kg par tonne de glace produite
Prix : 17 000 CFP par sac de 25 kg

2.6.1. 12 – Honoraires Comptable

Le gérant aura recours à l'assistance d'un comptable pour la tenue mensuelle de la comptabilité, et pour l'établissement du bilan annuel.

Année 1 : 30 000 CFP/mois + 100 000 CFP préparation bilan
Année 2 : 40 000 CFP/mois + 100 000 CFP préparation bilan
Année 3 : 45 000 CFP/mois + 100 000 CFP préparation bilan

2.6.1. 13 – Loyer unité mareyage

Le loyer devrait pouvoir au minimum couvrir les charges d'amortissements des équipements (poste 5 du tableau des amortissements), soit 4 494 000 CFP/an (374 500 CFP/mois).

A l'évidence un loyer établi sur cette base, n'est pas compatible avec l'économie du projet.

L'aspect politique doit donc en la matière primer sur l'aspect strictement financier, de façon à rendre économiquement viable ce type de projet dans le cadre d'un archipel éloigné tel que celui des Marquises.

Nous suggérons donc de prendre en compte un loyer d'un montant symbolique de 50 000 CFP/mois.

Tableau des AMORTISSEMENTS -

(les montants sont exprimés en KCFP)

Investissements			Amortissements		
Désignation	Montant	Code	Durée	Taux %	Amort.
1- Frais de 1er établissement	1336	NR	10	10,00%	134
2 - Terrassements - Travaux de nettoyage	540	NR	10	10,00%	54
3 - Travaux de réfection du bâtiment	6274	R	15	6,67%	418
4 - Travaux d'aménagement du bâtiment	12510	R	15	6,67%	834
5 - Equipements unité mareyage					
. Equipements frigorifiques	19500	R	10	10,00%	1 950
. Machine à glace	2800	R	7	14,29%	400
. Transpalettes	320	R	3	33,33%	107
. Bascules	1920	RD	3	33,33%	640
. Autres équipements	4190	R	3	33,33%	1 397
6 - Equipements pour bateaux de pêche					
. Glacières	2000	R	5	20,00%	400
8 - Téléphone	30	NR	2	50,00%	15
9 - Ingénierie	2640	NR	8	12,50%	330
10 - Imprévus et divers	2636	NR	8	12,50%	330

Totaux	**56 696**		**7 009**
Taux moyen d'amortissement		**12,36%**	
Durée moyenne d'amortissement		**8,09 ans**	

Code : NR = non renouvelé
R = renouvelé au terme de l'amortissement
RD = renouvellement différé

2.6.1. 14 – Frais financiers

Pour faire face à ses besoins en fonds de roulement, l'unité de mareyage devra négocier une ligne de crédit bancaire sous forme d'A.C.C. d'environ quatre millions CFP.

Ce besoin est estimé en considérant :

- un règlement immédiat aux pêcheurs,
- D'un temps d'encaissement moyen d'un mois auprès des clients.

2.6.2 – Les comptes de produits :

Les objectifs de ventes des poissons et langoustes, sont ceux de la troisième année.

Les objectifs de ventes des années 1 et 2 sont respectivement de 80% et 90% de ceux de l'année 3.

Les prix de vente indiqués pour les marchés marquisien et tahitien , sont C&F ports de destination.

2.6.2.1 – Ventes de glace en écaille

La vente de glace en écaille concerne prioritairement l'approvisionnement des pêcheurs au prix de 10 CFP/kg.
Ventes proportionnelles à la production dans un rapport de 1/1 .

Accessoirement pourra être développé la vente de glace aux particuliers, car d'une bonne rentabilité, sur la base de 25 CFP/Kg, glace conditionnée en sac de 20 kg.

Hypothèses de vente : année 1 = 200 kg / semaine
Année 2 = 300 kg / semaine
Année 3 = 360 kg / semaine

2.6.2.2 – Ventes de poissons et langoustes sur le marché local

Objectifs de vente :

- Filets de thon frais : 53,6 tonnes à 600 CFP/kg
- Filets de thon, plats à emporter : 3,2 tonnes à 1100 CFP/kg
- Espèces de fond /récif (entier, vidé) : 16,1 tonnes à 600 CFP/kg
- Langoustes : 4 tonnes à 1600 CFP/kg

2.6.2.3 – ventes de poissons sur le marché Marquisien

Objectifs de vente :

- Filets de thon congelés : 51,5 tonnes à 550 CFP/kg
- Espèces de fond/récif (entier, vidé) : 16,6 tonnes à 600 CFP/kg

2.6.2.4 – Ventes de poissons et langoustes sur le marché tahitien

Objectifs de vente :

- Espèces de fond/récif (entier, vidé) : 18 tonnes à 950 CFP/kg
- Espèces de fond/récif (filets) : 13 tonnes à 1100 CFP/kg
- Langoustes : 6 tonnes à 1700 CFP/kg

Etude : Service de la Pêche - Taiohae
Unité de mareyage

COMPTE D'EXPLOITATION PREVISIONNEL

(K CFP)

Années	1	2	3
Production en % de l'objectif	80%	90%	100%
CHARGES			
Salaires	5960	8215	8944
Charges sociales CPS	1458	1959	2079
Energie	2208	2760	3450
Emballages	2064	2322	2580
Télécommunications	100	120	130
Achats Poissons, Langoustes	87193	98092	108991
Fret maritime et aérien	1360	1530	1700
Produits entretien/désinfection	180	200	220
outillage, papeterie	60	80	100
Voyages, déplacements	130	130	130
Entretien équipements frigo.	700	700	1000
Sel pour production glace	44	50	55
Honoraires Comptable	460	580	640
Loyer unité mareyage	600	600	600
Frais financiers A.C.C.	400	200	100
Total des charges	**102 917**	**117 538**	**130 719**
PRODUITS			
Glace en écaille	1260	2388	3323
Poisson marché local	41392	46566	51740
Poisson marché marquisien	30628	34457	38285
Poisson marché tahitien	33280	37440	41600
Total des produits	**106 560**	**120 851**	**134 948**
R.B.E.	**3 643**	**3 313**	**4 229**
RBE en % du CA	**3,42%**	**2,74%**	**3,13%**

2.7 – Gestion de l'unité de mareyage

Malgré la bonne volonté de ses dirigeants, la Coopérative MOKAI n'a ni les moyens financiers, ni les hommes pour prendre en gestion et développer de façon durable cette unité de mareyage.

À l'expérience, il semble plus efficace de séparer les fonctions de production et de mareyage. En effet, les intérêts ne sont pas toujours convergents. En particulier l'arbitrage des prix à la production est difficile à établir en toute sérénité dans une structure unique dont les membres sont tous producteurs.
Situation qui a souvent exposé nombre de coopératives de pêcheurs à de graves difficultés financières, conduisant parfois au dépôt de bilan.

Replacé dans le contexte humain et commercial de Taiohae, il est primordial de rechercher une solution qui associerait :

- Le dynamisme commercial d'un entrepreneur privé. Facteur essentiel dans cette phase cruciale de recherche et de développement de nouveaux produits et nouveaux marchés à « l'export ».
- La garantie d'approvisionnement en produits avec le savoir faire des pêcheurs.

Différentes solutions sont envisageables :

- L'unité de mareyage est une société commerciale privée, ayant un contrat d'amodiation avec le Territoire pour l'usage du bâtiment et des équipements. Lequel contrat pouvant comporter une clause relative à l'exploitation d'un outillage public pour la production de glace en écaille, avec obligation de production en faveur des pêcheurs à un prix de vente conventionné.
  Un contrat commercial avec la Coopérative MOKAI, peut venir compléter ce dispositif. Contrat qui garantirait l'approvisionnement de quotas minimum par espèce à des prix d'achat garantis.
  Cette solution a souvent le mérite d'une excellente efficacité.
  Le capital de cette société pourrait être ouvert partiellement de façon minoritaire à la Coopérative de production.

- Une Société d'économie mixte locale : structure qui permettrait d'associer le Territoire (financement de l'investissement, et apport d'aides publiques en cas de nécessité pour l'exploitation), la coopérative de production, et des privés pour le mareyage.
  Ce type de société est peu adapté à une gestion d'activité essentiellement de négoce.

2.8 – Incidence du projet sur la rentabilité de la flottille

Le manque de données, précises sur le financement et l'exploitation des bateaux en activité, conduirait à un exercice difficile de vouloir comparer la différence de rentabilité par catégorie d'embarcations entre le système d'exploitation actuel et celui proposé dans le projet.

Aussi nous nous bornerons à une comparaison des chiffres d'affaires en première vente, générés par chacun des systèmes d'exploitation pour la globalité de la flottille.

Estimation du chiffre d'affaires actuel :

Thons (entier, vidé) : 141,81 tonnes à 400 CFP/kg = 56 724 000 CFP
Espèces fond (ligne) : 32,5 t x 90% à 400 CFP/kg = 11 700 000 CFP
Espèces fond (fusil) : 32,5 t x 10% à 500 CFP/kg = 1 625 000 CFP
Langoustes : 9 tonnes à 1500 CFP/kg = 13 500 000 CFP

Total C.A. = 83 549 000 CFP

Chiffre d'affaires prévisionnel du projet :

Pour 80% de l'objectif = 87 193 000 CFP
Pour 90% de l'objectif = 98 092 000 CFP
Pour 100% de l'objectif = 108 991 000 CFP

A 100% de l'objectif de commercialisation, l'augmentation du chiffre d'affaires en première vente serait d'environ vingt cinq millions CFP (soit +30,5%).

Cette augmentation du chiffre d'affaires compenserait très largement le surplus de consommation de carburant nécessaire à l'augmentation de la production et sera suffisamment attractive pour les pêcheurs pour en justifier sa mise en œuvre.

D'autant, que la plus forte augmentation en tonnage se ferait sur la pêcherie de thons, dont le potentiel est de loin le plus important.

Ceci est beaucoup moins vrai pour une réalisation à 80% de l'objectif.

En effet serait demandé un effort sur la production, sans augmentation significative en retour du revenu des pêcheurs.

2.9. – Conclusions

Faire évoluer l'exploitation de la flottille basée à Taiohae d'une économie vivrière à celle d'une économie de marché semble être un projet réaliste.

D'une part, Il y une volonté clairement exprimée de nombreux pêcheurs professionnels à vouloir rompre avec la situation existante pour évoluer vers une économie de marché, qui leur permettrait de mieux utiliser leur outil de production.

D'autre part l'analyse des marchés accessibles, montrent qu'ils ont encore un bon potentiel de développement, pour peu de proposer des produits innovants et conditionnés.

Cette évolution ne sera possible que par une intervention forte et claire du Territoire à vouloir réaliser ce projet en cohérence avec une politique de développement de la pêche dans les archipels et en particulier aux Marquises.

Cette intervention devra s'intégrer dans un projet qui assumera :

- Le financement d'une unité de mareyage, dont le rôle pivot sera autant financier que technique.
  . financier, en assurant le fond de roulement de la filière
  . technique, en conditionnant, stockant et commercialisant les produits de la pêche,

- Le financement d'un complément d'équipements (glacières) à bord des bateaux,
  de façon à améliorer la qualité des produits pêchés.

- La prise en charge d'actions de formation des pêcheurs concernant les règles d'hygiène, et de conditionnement du poisson à bord,

La faible rentabilité (RBE/CA de 3%) de l'unité de mareyage, fait que ***l'investissement devra être obligatoirement réalisé sur fonds publics,***

Les hypothèses de commercialisation (tonnages, prix) prises en compte dans l'étude, pourront paraître modestes. Cependant nous pensons qu'elles sont le reflet de notre connaissance actuelle des marchés, et de leur évolution à très court terme avec en particulier la prise en compte de la forte augmentation programmée de la flottille de pêche fraîche basée à Papeete.

Il est envisageable une augmentation significative du marché tahitien pour les poissons de fond et de récif. Sur ce créneau commercial, le facteur limitant ne sera pas tant celui du marché, que celui de la ressource.

Ce stock est actuellement sous-exploité.

Préalablement à toute exploitation plus intensive il conviendrait d'en étudier sa potentialité.

À cet effet, ***le Service de la Pêche, devrait affecter sur place un agent, chargé des statistiques de débarquement.***

Cet agent, pourrait également assister le gérant de l'unité de mareyage lors de sa période de démarrage.

En termes de développement, le projet est à l'échelle de la pêcherie côtière marquisienne.

À moins qu'elle ne soit rattachée à un programme de développement plus ambitieux qui s'intégrerait dans de nouveaux circuits de commercialisation à l'export, l'introduction de la palangre monofilament, constituerait un risque majeur pour la pérennité de l'activité de l'actuelle flottille.

La productivité des palangriers, en particulier sur la pêcherie thonière, conduirait à une saturation très rapide du marché local et du marché marquisien au détriment des pêcheurs déjà en activité.

3- Le projet pour une deuxième étape du développement

Une deuxième étape du développement de la filière pêche, consisterait en la mise en exploitation de la ressource hauturière.

L'exploitation de cette ressource hauturière n'est pas contradictoire de celle de la ressource côtière, dans la mesure d'un objectif d'exportation de la quasi-totalité de la production sur les marchés internationaux.

Un préalable doit être levé : celui d'une meilleure connaissance du déterminisme de cette pêcherie.

En effet si de nombreuses voix s'accordent à vanter les richesses halieutiques de l'archipel des Marquises et de la Zone Economique Exclusive attachée, il s'avère qu'à l'expérience des pêcheurs asiatiques (Japonais, Coréens) et des palangriers Tahitiens qui ont fréquenté cette zone, la ressource y est fugace et occasionnelle.

Deux stratégies d'exploitation de cette pêcherie sont possibles :

- Navires de pêche fraîche, avec débarquement des captures dans un port et centre de conditionnement qui serait construit à Taiohae (cf. étude COFREPECHE).

- Navires congélateurs, voir surgélateurs, avec débarquement des captures à Papeete.

La première solution pourrait être mis en œuvre avec des navires glaciers de 15 à 18 m, mais dont l'exploitation ne pourra reposer à 100% sur la ressource pélagique thonière.
Afin d'assurer son emploi pendant les périodes creuses, cette flottille devra alors travailler à la palangre de fond sur les espèces démersales.

La rentabilité de cette stratégie, repose sur l'exportation par avion de poissons frais à forte valeur marchande (Big Eye) via la plateforme aéroportuaire de Papeete.

En première approche, cette solution serait mieux adaptée à la capacité financière des investisseurs Marquisiens.

Elle présente cependant les inconvénients :

- De dépendre d'investissements publics très importants (2 à 2,5 milliards F. CFP, hors financement routier), pour la réalisation d'un port de pêche, et la viabilisation pour un usage tous temps de la piste entre Taiohae et l'aéroport de Terre Déserte,
- De dimensionner dès sa phase de démarrage le projet à une taille critique importante, pour justifier d'une certaine rentabilité économique (problème de poids minimum à enlever par rotation de l'avion cargo).

La solution des navires congélateurs, offre les avantages suivants :

- D'être plus en accord avec le déterminisme de la pêcherie, tel que nous l'appréhendons actuellement, grâce à une grande autonomie de déplacement, et donc une plus grande souplesse d'exploitation en travaillant sur d'autres zones de pêche, dont la pêcherie de germon du nord-est des Tuamotu.
- Ne nécessite pas de nouvelles infrastructures portuaires aux Marquises pour se développer.
- L'inconvénient majeur est que même si les navires seraient contrôlés par des capitaux Marquisiens, leurs équipages marquisiens seront dans les faits basés à Papeete et leurs familles sédentariser à Tahiti.

Cette solution si elle peut contribuer à l'enrichissement de l'archipel conduit au paradoxe, d'en accélérer son dépeuplement.

En conclusions :

L'exploitation de la pêcherie hauturière Marquisienne par des navires palangriers, devra être appréhendé avec beaucoup de soins.

Son développement devra prendre en compte celui de la pêcherie côtière afin de ne pas interférer sur la commercialisation des produits.

Une analyse détaillée prenant en compte les grandes variabilités spatiales et temporelles des rendements observés sur cette pêcherie, les aspects politiques du développement économique des archipels, les investissements structurants déjà programmés (réseau routier, aéroports etc...) ou à programmer par le Territoire, devrait permettre de décider en toute connaissance de cause d'un choix stratégique de filière (frais, congelé) .

POLYNESIE FRANÇAISE

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

SERVICE DU PERSONNEL
ET DE LA FONCTION PUBLIQUE

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

UNE NOTE DE SYNTHESE

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

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

Le sujet comporte 100 pages.

CONCOURS EXTERNE D'INGENIEURS EN CHEF DE CATEGORIE A

REDACTION D'UNE NOTE DE SYNTHESE

Sujet :

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

La sécurité des systèmes d'information

Un enjeu majeur pour la France

Pierre LASBORDES
Député

Le 26 novembre 2005

REMERCIEMENTS

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

M. Roger BALERAS, *ancien Directeur des applications militaires du CEA* ;
M. Jean-Paul GILLYBOEUF, IGA, *Chargé de mission pour la mise en place d'une direction générale des systèmes d'information et de communication au ministère de la Défense* ;
M. Michel LACARRIERE, *Directeur de l'administration centrale honoraire* ;
M. Jean RANNOU, *Général* ;
M. Dominique ROUX, *Professeur à l'Université de Paris Dauphine* ;
M. Jacques STERN, *Professeur à Ecole normale supérieure ULM, Directeur du département informatique*
M. Jean-Pierre VUILLERME, *Directeur des services environnement et prévention du groupe Michelin.*

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

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

Avertissement

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

Sommaire détaillé

ANNEXES

INTRODUCTION

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

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

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

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

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

De leur côté, les entreprises doivent protéger de la concurrence et de la malveillance leur système d'information qui irrigue l'ensemble de leur patrimoine (propriété intellectuelle et savoir faire) et porte leur stratégie de développement.

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

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

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

Tous les utilisateurs identifient au quotidien la menace constante des virus et des vers qui submergent Internet. Leur nombre a explosé au cours de ces dernières années et ceux-ci deviennent de plus en plus sophistiqués. Les outils nécessaires aux pirates sont aisément accessibles en ligne et il existe un échange constant d'information et de savoir-

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

faire au sein de la communauté des pirates pour rendre ces attaques de plus en plus efficaces. Cependant, leur désir de performance cède de plus en plus le pas au développement d'entreprises criminelles dont les activités en ligne se sont accrues parallèlement à la dimension économique d'Internet. Le nombre de fraudes se traduit chaque année par des coûts s'élevant à des milliards d'euros, en particulier pour les banques et les entreprises.

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

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

L'espionnage d'Etat ou industriel visant à intercepter des informations d'adversaires ou de concurrents constitue une autre pratique. Au-delà de la dimension offensive propre aux agences de sécurité gouvernementales, les atteintes au secret industriel sont de plus en plus systématisées. Le vol des secrets commerciaux est lui aussi en constante augmentation. Il représentait, en 2001, aux Etats-Unis, un préjudice de 59 milliards de dollars aux mille premières entreprises américaines. L'exemple le plus spectaculaire porte sur la révélation[2], en juin 2005, des agissements d'une entreprise israélienne qui « louait » un cheval de Troie[3] à ses clients ; une affaire qui a conduit à l'arrestation de plusieurs dirigeants d'entreprises à travers le monde. En s'adressant à cette société, un client demandait tout simplement à ce que le produit soit installé dans le système d'information de la cible, pour en extraire en toute impunité toutes les informations qu'il désirait.

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

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

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

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

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

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

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

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

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

SYNTHESE

SECURITE DES SYSTEMES D'INFORMATION

Un enjeu majeur pour la France

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

I- Une menace qui doit être prise au sérieux

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

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

L'organisation (recours à l'externalisation, absence de classification des informations,...), la faiblesse des acteurs humains (inconscience, insouciance, naïveté), les réseaux de communication (risques de saturation, d'interception,..), les logiciels dont la complexité croissante est source d'erreurs difficiles à détecter, ou les composants matériels, sont autant de sources de vulnérabilités.

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

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

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

II- Les réponses organisationnelles et techniques

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

Au sein du SGDN[4], la DCSSI[5] est chargée d'organiser les travaux interministériels et de préparer les mesures que le Secrétaire général de la Défense nationale propose au Premier ministre ; elle prépare les dossiers en vue des autorisations, agréments, cautions ou homologations, et en suit l'exécution ; elle met en œuvre les procédures d'évaluation et de certification; elle participe aux négociations internationales ; elle assiste les services publics dans le domaine de la SSI (conseil, audit, veille et alerte sur les vulnérabilités et les attaques, réponse aux incidents) ; elle assure la formation des personnels qualifiés dans son centre de formation (CFSSI).

La DCSSI mène également des inspections dans les systèmes d'information des ministères. Aux dessus du CERTA[6], elle a mis en place un centre opérationnel de la sécurité des systèmes d'information (COSSI), activé en permanence, chargé d'assurer la coordination interministérielle des actions de prévention et de protection face aux attaques sur les systèmes d'information. Elle a également mis en place un nouveau label ainsi qu'une cellule chargée d'entretenir des relations avec le tissu des entreprises de SSI.

L'effectif de la DCSSI est d'une centaine de personnes, en majorité de formation scientifique et technique. Les auditions menées ont montré en particulier que :

- la faiblesse de l'effectif conduit à limiter la capacité d'inspection de la DCSSI à seulement une vingtaine de déplacements par an sur site, ce qui est insuffisant ;
- son rôle de conseil aux entreprises est insuffisamment développé et se révèle peu en phase avec les attentes du monde économique ;
- les formations du CFSSI[7], considérées comme de très grande qualité, sont malheureusement réservées aux personnels de l'administration exerçant directement dans le domaine de l'informatique ou de la SSI et souffrent d'un manque de notoriété.

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

Le Ministère de l'économie, des finances et de l'industrie a pour mission l'animation du développement industriel d'équipements de sécurité non gouvernementaux. Le service des technologies et de la société de l'information (STSI) de la direction générale des entreprises (DGE) du ministère a un bureau du multimédia et de la sécurité qui suit le domaine SSI et finance des projets SSI au travers des appels à projets Oppidum. Enfin, comme pour les

[4] Secrétariat général de la défense nationale

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

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

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

autres domaines technologiques, le MinEFI contribue au financement de l'innovation dans les PME par divers mécanismes d'aide, en particulier le crédit impôt recherche, et au travers d'OSEO-ANVAR dont il assure la tutelle.

L'ADAE[8], assure la maîtrise d'ouvrage des services opérationnels d'interconnexion et de partage des ressources pour l'administration électronique, dont le volet sécurité regroupe toutes les activités nécessaires à la mise en place de l'infrastructure de confiance (outils, référentiels, guides méthodologiques et expertise). Alors que la SSI est une composante importante de ce type de projets, la DCSSI n'est pas citée dans le décret instituant l'ADAE.

Le Ministère de l'Intérieur est chargé de la lutte contre la cybercriminalité. Dans le cadre de ses missions, la Direction de la surveillance du territoire (DST) assure des prestations techniques et informatiques, autour de trois volets : la prévention, la répression et la sécurité informatique. L'OCLCTIC[9] , est une structure à vocation interministérielle placée au sein de Direction de la police judiciaire (DCPJ). Elle lutte contre les auteurs d'infractions liées aux TIC, enquête à la demande de l'autorité judicaire, centralise et diffuse l'information sur les infractions à l'ensemble des services répressifs. La Police parisienne dispose d'un service similaire, le BEFTI.

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

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

De plus, les disparités dans la mise en œuvre d'une organisation type, au sein de l'administration, des difficultés à mobiliser les ressources nécessaires et l'absence d'autorité des acteurs de la SSI, peuvent rendre cette organisation inopérante. Face aux difficultés de recrutement de personnels, des ministères sont conduits à recourir à l'externalisation. Il est fréquent de constater que les services informatiques ne suivent pas les recommandations des HFD[10] lors de choix de solutions pour des applications sensibles, sous couvert d'une stricte application du Code des marchés publics. Toutefois certains ministères ont mieux intégré la problématique SSI et s'appuient sur des équipes compétentes et motivées.

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

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

Le rapport analyse la situation de plusieurs pays (Etats-Unis, Royaume-Uni, Allemagne, Suède, Corée du Sud et Israël) et aborde les initiatives multilatérales (Union européenne,

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

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

[10] Haut fonctionnaire de Défense

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

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

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

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

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

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

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

III - Base industrielle et technologique

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

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

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

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

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

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

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

Les PME de la SSI ne disposent pas des ressources suffisantes pour affronter la concurrence des offres étrangères. Elles ont des difficultés à financer leurs investissements, que ce soit en fonds propres (le secteur n'attire pas les investisseurs nationaux) ou par des crédits bancaires. Il faudrait développer des fonds d'investissement spécifiques, adaptés à des entreprises de croissance modérée, à même d'assurer un financement stable sur une durée supérieure à 10 ans.

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

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

Labellisation des produits de sécurité

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

- Une évaluation est conduite par un laboratoire privé, CESTI, agréé par la DCSSI

- Le processus de certification est jugé trop long et trop coûteux par beaucoup d'industriels, a fortiori pour les PME.

- La qualification par la DCSSI est donnée à un produit qui a été évalué et certifié à partir d'une "cible de sécurité" qu'elle a approuvé au préalable.10 produits ont déjà été qualifiés et 7 sont en cours de qualifications. La moitié de ces produits sont développés par des PME.

- L'agrément est l'attestation délivrée par la DCSSI qu'un produit de chiffrement est apte à protéger des informations classifiées de défense, après évaluation par le Celar et par la DCSSI. C'est un label national.

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

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

IV – SIX RECOMMANDATIONS

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

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

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

Axe 2 : Responsabiliser les acteurs

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

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

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

Axe 4 : Rendre accessible la SSI à toutes les entreprises

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

Axe 5 : Accroître la mobilisation des moyens judiciaires

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

Axe 6 : Assurer la sécurité de l'Etat et des infrastructures vitales

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

***

Il est à noter que certaines recommandations du rapport rejoignent les mesures proposées dans le Plan de Renforcement de la Sécurité des Systèmes d'Information de l'Etat en 2004.

UN IMPERATIF

Refondre l'organisation de la SSI de l'Etat

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

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

Il est proposé :

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

- de **séparer les fonctions opérationnelles des fonctions d'autorité :**

    - **les fonctions d'autorité resteraient** au **sein du SGDN qui, pour le compte et sous l'autorité du Premier ministre,** seraient notamment en charge de l'élaboration de la politique nationale de la SSI, de la validation des politiques SSI des ministères et des organismes sous tutelle, d'évaluer les résultats de la mise en œuvre opérationnelle, d'assurer une veille stratégique sur l'évolution des risques, d'initier le renforcement de la dimension judiciaire et les actions interministérielles en matière de politique d'achat.

    - à partir des fonctions opérationnelles de la DCSSI renforcées, **une structure opérationnelle rattachée au Premier ministre, dédiée et centralisée,** ayant une culture de résultats **pourrait être mise en place.**

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

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

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

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

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

Ainsi, une segmentation des systèmes d'information en trois sous-systèmes principaux permet de mieux appréhender le champs couvert et leur complexité (voir schéma en annexe 4) et en corollaire les enjeux de sécurité sous-jacents :

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

- Les réseaux de communication :
  - Les réseaux de satellites de communication ;.
  - Les réseaux sans fil (WiMax, WiFi, Bluetooth,...) ;
  - les réseaux de localisation GPS ou Galiléo ;
  - Les réseaux téléphoniques filaires ;
  - Les réseaux d'opérateurs de téléphonie mobile (GSM, GPRS, UMTS).

- Les réseaux de diffusion de télévision (TNT, câble) et de radio.

La disponibilité de nouveaux supports physiques de transmission ou l'optimisation de la bande passante sur ceux qui existent (modulations radio-électriques, câbles sous-marins, câbles optiques, satellites, multiplexage sur la paire de cuivres, etc.) offrent de grandes possibilités techniques (amélioration des interconnexions, des débits, etc.).

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

Ainsi :

- La dématérialisation des relations entre une administration et ses administrés en donne un bon exemple. L'utilisation et l'envoi électronique d'imprimés administratifs sur Internet permettent de réduire significativement les coûts de traitement des procédures manuelles (allègement de la masse salariale des agents publics). Dans le

même temps, le traitement central et automatisé d'une procédure permet d'escompter un gain d'efficacité (statistiques et prévisions quasi-immédiate pour l'administration) ;

- Un programme d'armement visant à assurer un flux continu d'information entre un état-major de forces et des militaires œuvrant sur un théâtre d'opérations est à même de donner au commandement une visibilité totale et instantanée des actions et des mouvements entrepris par le fantassin sur le champ de bataille.

- Quant à l'ordinateur individuel connecté à Internet, il offre de nouveaux loisirs et un confort de vie : parcourir un supermarché virtuel, payer et se faire livrer à domicile la commande.

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

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

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

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

- Il y a asymétrie entre les moyens de l'attaquant (sans limite) et ceux du défenseur (très contraint). Le défenseur doit tout imaginer sans pouvoir riposter (principe de la vision de Clausewitz) car il n'y a pas de légitime défense en SSI[11] tandis que l'attaquant s'autorise tout ce qui est possible.

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

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

La gestion du risque et la SSI participent d'une même démarche globale, fondée sur l'identification des attaques potentielles, mais également sur l'idée qu'aucun système d'information n'est invulnérable car :

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

- il n'est pas possible d'envisager de se protéger à 100% des codes malveillants (comme par exemple les virus ou les chevaux de Troie ;
- les pares-feu protègent uniquement des attaques résiduelles (i.e. qui ne correspondent pas aux services offerts)[12] ;
- les algorithmes cryptographiques secrets ne sont pas tous fiables ;
- les solutions de détection d'intrusion peuvent être trompées ;
- la SSI repose sur des outils mais également sur un facteur humain ;
- il n'est pas possible de tester les systèmes et les applications dans des délais raisonnables au regard de leur déploiement auprès des utilisateurs.

La sécurité des systèmes d'information vise généralement cinq objectifs :

- la confidentialité : il s'agit de garantir que l'accès aux données n'est possible que pour les personnes dûment autorisées à les connaître ;

- l'intégrité : il s'agit de garantir que les fonctions et données sensibles ne sont pas altérées, et conservent toute leur pertinence ;

- la disponibilité : il s'agit de garantir qu'une ressource sera accessible au moment précis où quelqu'un souhaitera s'en servir ;

- l'authentification a pour but de vérifier qu'une entité est bien celle qu'elle prétend être ;

- la non répudiation vise à interdire à une entité de pouvoir nier avoir pris part à une action (cela est fortement lié à la notion juridique d'imputabilité).

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

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

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

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

1.2 La sensibilité de l'information à prendre en compte

Les informations qui doivent demeurer confidentielles, celles qui doivent absolument être disponibles ou celles qui peuvent représenter un attrait pour une tierce partie, sont appelées sensibles (cf. Annexe 5).

[12] Lire à ce propos la note du CERTA : « Tunnel et pare feu : une cohabitation difficile » (http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003/) ;

• **L'AFNOR[13] distingue trois types d'informations :**

- « L'information aisément et licitement accessible » que certains appellent « l'information blanche » est ouverte à tous. Elle se trouve dans la presse, Internet,....

- « L'information licitement accessible mais caractérisée par des difficultés dans la connaissance de son existence et de son accès ». Cette « information grise » pour la trouver, il faut d'abord savoir la chercher. Elle se rapproche davantage du renseignement.

- « L'information à diffusion restreinte et dont l'accès et l'usage sont expressément protégés ». Il s'agit ici de « l'information noire » qui est protégée par un contrat ou une loi. Seules quelques personnes sont autorisées à y accéder.

• **Les deux mentions préconisées par la Directive 901 : CONFIDENTIEL et DIFFUSION LIMITEE**

Aux termes de l'art.4, portant sur les informations sensibles, non classifiées « Défense », il est recommandé que ces informations reçoivent une mention rappelant leur sensibilité en considération de la gravité des conséquences qu'aurait leur divulgation, leur altération, leur indisponibilité ou leur destruction.

À cette fin, une distinction est opérée par deux mentions désignant le niveau de protection qu'il faut assurer à l'information: CONFIDENTIEL et DIFFUSION LIMITEE.

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

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

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

Les principales menaces effectives pesant sur les systèmes d'information sont de nature distincte mais tout aussi préjudiciable à la protection de l'information :

- **l'utilisateur** : Il n'est pas généralement une menace : il peut se retrouver face à une gestion de la complexité à laquelle il n'a pas été préparé (le particulier n'est pas un administrateur informatique). L'exemple typique est la mauvaise utilisation de SSL ou encore le phishing ;
- **les programmes malveillants** : un logiciel destiné à nuire ou à abuser des ressources du système est installé sur le système (par mégarde ou par malveillance), ouvrant la porte à des intrusions ou modifiant les données ;
- **l'intrusion** : une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès ;

[13] Association française de normalisation.

- **un sinistre** (vol, incendie, dégât des eaux...) génère une perte de matériel et/ou de données ;

La sécurité des systèmes d'information est partie intégrante de la sécurité globale visant à se protéger des attaques :

- **physiques** : ces attaques (vols ou destructions par exemple) visent les infrastructures physiques des systèmes d'information, tels les câbles ou les ordinateurs eux-mêmes ;
- **électroniques** : il s'agit par exemple de l'interception ou du brouillage des communications ;
- **logicielles** : ces attaques regroupent l'intrusion, l'exploration, l'altération, la destruction et la saturation des systèmes informatiques par des moyens logiques ;
- **humaines** : l'homme est un acteur clef d'un système d'information. Il constitue à ce titre une cible privilégiée, et peut faire l'objet de manipulation aux fins de lui soutirer de l'information via l'« ingénierie sociale »[14] par exemple ;
- **organisationnelles** : un attaquant cherchera à abuser des défauts de l'organisation et de sa sécurité pour accéder à ses ressources sensibles.

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

1.3.1 Des attaquants aux profils et aux motivations hétérogènes

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

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

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

Les principaux objectifs d'un attaquant sont de cinq ordres :

- désinformer ;
- empêcher l'accès à une ressource sur le système d'information ;
- prendre le contrôle du système par exemple pour l'utiliser ultérieurement ;
- récupérer de l'information présente sur le système ;
- utiliser le système compromis pour rebondir vers un système voisin.

Il est toujours difficile de connaître les motivations d'un acte, même si ces dernières telles que le besoin de reconnaissance, l'admiration, la curiosité, le pouvoir, l'argent et la vengeance sont le plus souvent moteur dans des actes délictueux. Il est cependant utile de

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

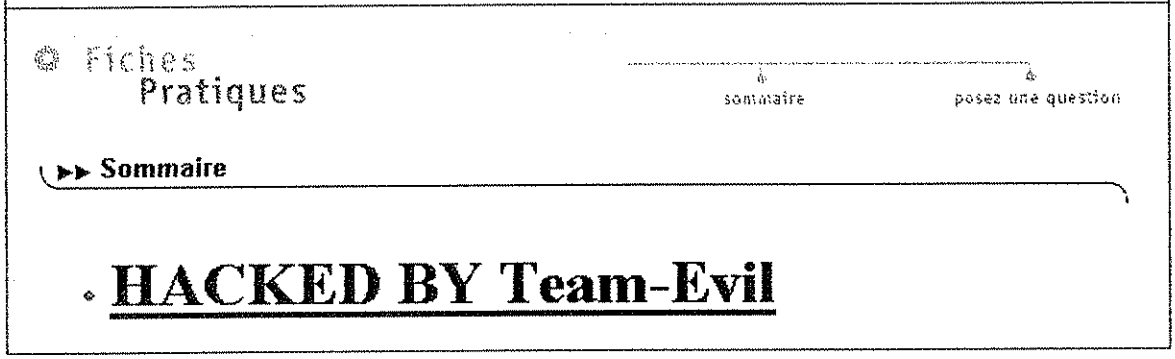
chercher à les comprendre pour mettre en place des stratégies et des tactiques de réponses adaptées.

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

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

Défiguration ludique

Le 16 juillet 2005, le site www.expatries.diplomatie.gouv.fr était défiguré[15] : une de ses pages était remplacée a priori par une référence au groupe de pirates.



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

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

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

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

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

Profils des attaquants

Sans détailler tous les profils (cf. Annexe 6), on retiendra le plus connu ; les « hackers »[16] qui interviennent individuellement ou via des organisations. Différentes catégories de hackers existent en fonction de leur champ d'implication (légal ou illégal) ou de leur impact sur les réseaux informatiques : les chapeaux blancs, certains consultants en sécurité, administrateurs réseaux ou cyber-policiers, ont un sens de l'éthique et de la déontologie ; les chapeaux gris pénètrent les systèmes sans y être autorisés, pour faire la preuve de leur habileté mais ne connaissant pas la conséquence de leurs actes; les chapeaux noirs, diffuseurs volontaires de virus, cyber-espions, cyber-terroristes et cyber-escrocs, correspondent à la définition du pirate. Ces catégories peuvent être subdivisées en fonction des spécialités. Ainsi, le « craker », s'occupe de casser la protection des logiciels, le « carder », les systèmes de protection des cartes à puces, le « phreaker », les protections des systèmes téléphoniques.

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

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

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

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

La Commission européenne, dans une communication en date d'octobre 2004 (« Protection des infrastructures critiques[17] dans le cadre de la lutte contre le terrorisme »[18]), propose la définition suivante :

« Les infrastructures critiques sont des installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des États membres. Les infrastructures critiques se trouvent dans de nombreux secteurs de l'économie, y compris le secteur bancaire et des finances, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires et les communications, ainsi que certains services administratifs de base. »

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

[16] Un « hacker » est un expert technique/scientifique, sans connotation morale particulière, contrairement au langage usuel. C'est pourquoi, dans ce rapport, les termes de pirates ou d'intrus pour désigner une personne employant des moyens illégaux pour rentrer et/ou se maintenir dans un systèmes d'information seront préférés.

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

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

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

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

Les réseaux nationaux britanniques victimes d'attaques ?

Le 16 juin 2005, le *National infrastructure security coordination-center (*NISCC) du Royaume-Uni émettait, à travers la presse nationale, une alerte concernant des virus qui s'attaqueraient aux réseaux informatiques d'entités publiques et privées dans plusieurs secteurs clés : énergie, communications, transport, santé, finances et organismes gouvernementaux.
Il s'agissait selon le NISCC d'un type d'attaque de haut niveau, combinant une large variété de techniques, connues mais difficiles à détecter et qui visait certaines infrastructures critiques.

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

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

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

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

[19] Source auditions

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

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

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

Ainsi, en juin 2005, des révélations[21] sur une entreprise israélienne qui « louait » un cheval de Troie à ses clients ont conduit à l'arrestation de plusieurs dirigeants d'entreprises à travers le monde. En s'adressant à cette société, un client demandait tout simplement à ce que le produit soit installé dans le système d'information de la cible, et pouvait ensuite en extraire en toute impunité toutes les informations qu'il désirait.

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

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

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

- **Les citoyens, des cibles vulnérables**

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

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

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

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

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

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

Liaisons transatlantiques
Le réseau TAT-1422, assure une partie du transit Internet entre l'Europe et les Etats-Unis. Toute rupture des fibres optiques entraîne des perturbations importantes des communications transatlantiques. Ce fut accidentellement le cas en novembre 2003, à cause d'un chalutier.

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

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

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

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

1.3.4.1 Les attaques physiques sont à traiter en priorité

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

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

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

La miniaturisation des moyens de stockage, comme les clés USB[23], et leur facilité d'emploi plaident également en faveur du renforcement de ce contrôle. Il est possible, à partir d'une clé USB modifiée, de prendre le contrôle d'un poste et d'y insérer un programme indésirable ou d'en extraire des données. **Aucun ordinateur ayant accès à des données sensibles, et a fortiori relevant du secret de défense, ne devrait être laissé sans surveillance, en particulier lorsque des tiers** (agents d'entretien, visiteurs, concurrents potentiels,...) **ont accès aux locaux**.

1.3.4.2 Les menaces électroniques demeurent encore sous estimées

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

La menace TEMPEST[24] :

La menace "TEMPEST"est la menace que représente l'interception des signaux parasites compromettants, émis par tout équipement traitant des informations sous forme électronique, en vue de reconstituer les informations traitées.

Il est possible de tirer parti des signaux émis par un système électronique, perceptible jusqu'à plus d'une centaine de mètres. Les tensions électriques peuvent aussi révéler des informations intéressantes, par conduction, soit sur les conducteurs d'alimentation de l'appareil cible, soit sur des conducteurs passant à proximité, L'analyse des signaux parasites compromettants classiques s'est enrichie, en 2004, d'une nouvelle technique de cryptanalyse acoustique des cœurs d'unités centrales *(Core Process Units).* La menace TEMPEST, connue des services de renseignement et de protection, l'est moins du grand public. La parer est difficile et coûteux : il convient de placer tous les équipements sensibles dans des cages de Faraday ou d'acquérir des matériels conçus pour émettre un minimum de signaux.

L'utilisation croissante des moyens de communications sans-fil : réseaux WIFI, communications bluetooth® ou puces RFID sont autant de technologies qui multiplient les vecteurs d'attaque possibles. Une transmission WiFi ou bluetooth® non sécurisée, utilisée dans un sous-système identification biométrique, donc supposé donner une bonne garantie sur l'identité d'un utilisateur, non seulement détruit de facto toute sorte de garantie, mais peut, si elle est exploitée, mettre à mal l'ensemble du système d'information.

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

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

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

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

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

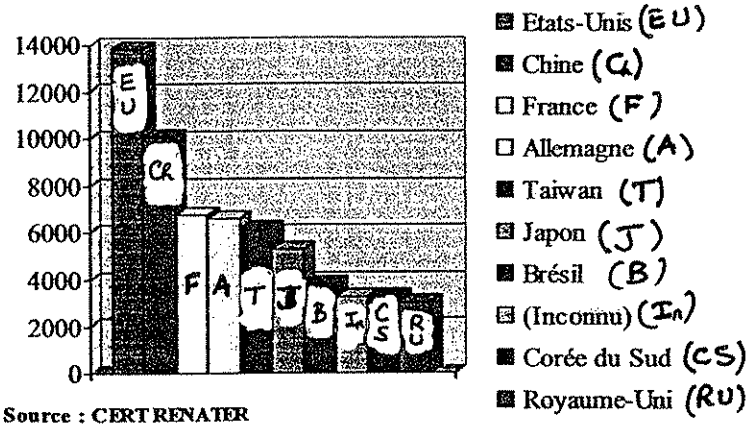
Considérant, par exemple, l'intérêt que pourrait trouver un concurrent à lire à distance l'ensemble du flux logistique de distribution d'un industriel, et dans la mesure où ce type de technologie est envisagé pour transmettre des données personnelles (sur des passeports par exemple) l'emploi de la technologie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

1.3.4.3 Les menaces logicielles sont en évolutions constantes

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

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

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



Source : CERT RENATER

Provenance des « scans »

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

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

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

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

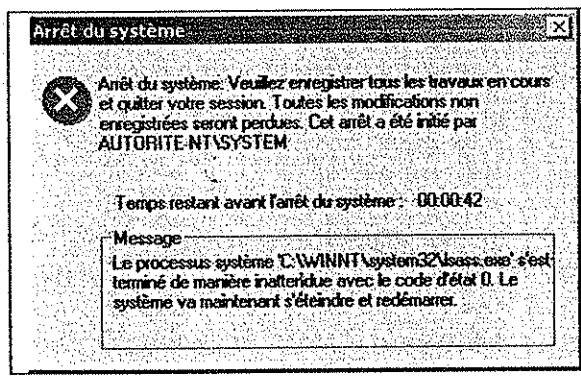
- **L'altération et la destruction :** il peut s'agir d'altérer ou de détruire des données stockées sur le système, ou bien le système lui-même, avec des finalités diverses. Au-delà des implications financières et industrielles évidentes, le but poursuivi peut être la dégradation des mécanismes de protection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

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

Quelques exemples parmi les plus connus :

- **Un ver** est un logiciel malveillant indépendant qui se transmet d'ordinateur à ordinateur par l'Internet ou tout autre réseau en utilisant les failles existantes et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. Contrairement au virus, le ver ne s'implante pas au sein d'un autre programme.

  Les tous premiers vers sont apparus en 1982. On retiendra la déferlante médiatique d'**I LOVE YOU** en mai 2000 et en 2002/2003, **Slammer** fait son apparition. Des dizaines de milliers de serveurs ont été touchés en quelques dizaines de minutes. Slammer a eu comme conséquences un ralentissement mondial de l'Internet, des arrêts de certains services pouvant aboutir, par exemple dans les aéroports américains, à reporter ou annuler des vols, compte tenu de répercussions négatives sur les systèmes de réservations automatisées en ligne. Les pertes économiques directes et indirectes ont été estimées à 1 milliard $. S'agissant de **Blaster**, une **grande entreprise française a chiffré à 1,5 M€ les conséquences de ce ver sur ses propres systèmes d'information**[26].



Un ver bien ordinaire

Si vous avez déjà vu cette fenêtre, sans doute faites-vous partie des quelques **millions** d'internautes à travers le monde à avoir été infectés par le ver **Sasser**[27].

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

[26] Source auditions

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

- **Un virus** est un logiciel malveillant, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un événement donné.

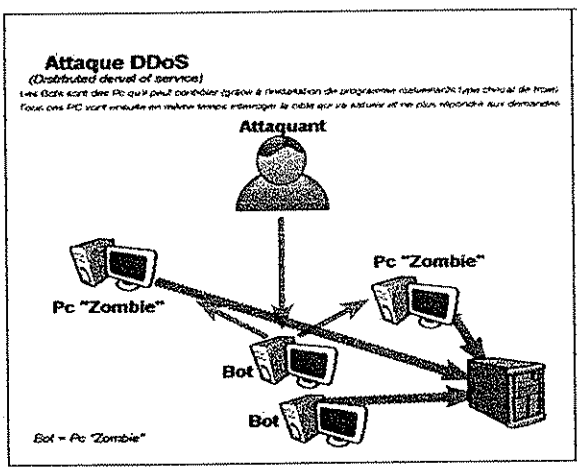
  A titre d'exemple, dans un grand groupe[28] , 5% des courriels échangés en 2004 ont été interceptés et éradiqués. Mais il faut aussi et surtout tenir compte de tout ce qui ne se détecte pas à cause de mise à jour non effectuée ou de vulnérabilité encore inconnue. Les anti virus agissent par définition a posteriori. C'est précisément pour cela que la protection contre les virus ne peut et ne doit pas se limiter à un anti virus mais que l'utilisateur doit être formé et rester vigilant.

  2004 a vu l'explosion du nombre de variantes virales, avec plus de **10 000 nouveaux virus** identifiés[29] comme MyDoom, ciblant les systèmes d'exploitation Windows, avec pour objectif de lancer des attaques comme par exemple des dénis de service.

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

- **Les réseaux de robots** visent à donner la possibilité à un pirate de contrôler des machines, en vue d'une exploitation malveillante. Ils peuvent provoquer des redémarrages intempestifs ou empêcher le téléchargement de correctifs tout en bloquant l'accès à certains sites Internet.

  Les attaquants dont la motivation est souvent financière, pour ne pas être détectés et préserver leur anonymat, ont de plus en plus tendance à mettre en place un réseau de machines devant rester invisible leur permettant, le moment venu, de relayer de manière massive à partir des machines infectées l'attaque désirée : des Spam, des virus, ou des attaques en déni de service. Les réseaux de robots (**botnets**) peuvent mettre en œuvre entre 3 000 et 10 000 ordinateurs **"zombies"**. Au premier semestre 2005, en moyenne 10 352 ordinateurs de réseaux de bots ont été actifs, par jour, soit **une augmentation de 140%** par rapport au semestre précédent[30].



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

En 2002, pendant une heure, les treize serveurs de noms racine (dont 10 aux Etats-Unis), qui permettent directement ou indirectement, à tous les navigateurs de trouver les pages web demandées, à tous les emails d'arriver à destination, ont été la cible d'une attaque de déni de service coordonnée. Le problème n'est pas tant la géographie physique mais qui concrètement contrôle ces serveurs (contenu, mise à jour, etc.).
Ces serveurs sont le centre nerveux d'Internet et en même temps son talon d'Achille.

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

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

- **Un Spam** est un courrier électronique d'exemplaires identiques, envoyé en nombre, de façon automatique et non sollicité[31].
  En 2004, il y a eu une inondation graduelle du Net par les Spams. De ce fait, nombre de responsables sécurité ont dû mobiliser leurs équipes sur le sujet des Spam pour répondre à la pression de leur direction et des utilisateurs face à la saturation de leurs messageries. A titre d'exemple un grand groupe français[32] dans lequel 500 000 mails sont échangés chaque jour, en rejette 60 000, dont 31 000 Spam et 29 000 virus. Au premier semestre 2005 le Spam a représenté **61% de la totalité du trafic de courriers électroniques** (51% de tous les Spams diffusés à travers le monde provenaient des Etats-Unis)[33]. Cependant, le Spam occasionne plus de désagréments que de dégâts, et s'il est parfois qualifié d'ennemi logique numéro un, ce n'est pas du fait de sa dangerosité.

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

1.3.4.4 Des attaques humaines

Dans la typologie des menaces, le facteur humain est essentiel et revêt deux formes :

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

1.3.4.5 Les attaques organisationnelles

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

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

La conjonction de phénomènes tels que l'ouverture vers l'extérieur, l'interconnexion des réseaux, la possibilité offerte à un utilisateur de se connecter, par voie filaire ou hertzienne, à

[31] Le CERTA a émis en 2005 une recommandation complète à ce sujet (limiter l'impact du SPAM : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004.pdf).

[32] Source auditions

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

distance, la mobilité des liaisons, la miniaturisation des ordinateurs et des supports d'information crée un environnement plus propice encore aux attaques. Toutes ces vulnérabilités doivent être vues sous l'angle de la gestion des risques et de l'homologation de sécurité.

1.4.1 Des vulnérabilités techniques multiples en évolution permanente

Lorsqu'elles sont identifiées, les vulnérabilités peuvent être communiquées directement à l'éditeur, mais peuvent également faire l'objet d'une publicité, avant la publication d'un correctif (un « patch »). Le temps qui sépare la publication d'une vulnérabilité de l'apparition du code d'exploitation correspondant diminue, exposant d'autant les systèmes jusqu'à la publication du correctif (patch) ; le danger étant le « 0-day » : des vulnérabilités inconnues avec des codes d'exploitation disponibles.
Au cours du premier semestre 2005, **on estime à environ 2000 le nombre de nouvelles vulnérabilités.** 97% de ces vulnérabilités étaient considérées comme modérées à très graves. Cependant, cette appréciation de criticité doit être réévaluée en fonction des environnements des différents systèmes concernés.

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

Certaines vulnérabilités, gardées secrètes, sont l'apanage d'organismes aux moyens plus importants (industriels, étatiques ou mafieux) et sont utilisées dans des optiques plus graves : espionnage, lutte informatique offensive, déstabilisation (cf. Annexe 7).

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

- **Les risques liés à l'utilisation d'infrastructures spontanées** [34]

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

C'est la raison pour laquelle les responsables de sécurité de plusieurs organisations, conscients des risques sous-jacents, limitent ou interdisent l'emploi de ces systèmes,[35] le plus souvent sans succès. D'autres imposent pour l'emploi de tels outils d'utiliser des courriels sécurisés, le contenu confidentiel est dans un fichier attaché crypté[36].

- **La menace des périphériques externes**

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

Il y a deux grandes catégories de risques, l'introduction de codes malveillants sur le réseau et la perte ou de vol de données de l'entreprise alors que des mesures simples concernant

[34] Une infrastructure spontanée est une nouvelle couche réseau mise en place à l'insu de l'administrateur réseau ou qu'il ne peut réellement contrôler. On peut citer par exemple les offres de services de convergence, susceptibles d'intéresser des particuliers ou des PME qui sont depuis 2004 en pleine croissance. C'est par exemple le cas des offres Blackberry ou Skype (téléphonie sur IP).

[35] Source auditions

[36] Source auditions

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

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

1.4.2 Les organisations sources de vulnérabilités

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

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

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

- **L'externalisation favorise les vulnérabilités**

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

Les principaux risques identifiés sont de nature :

- **informationnelle :** des données peuvent être dérobées ou manipulées et les systèmes d'information peuvent être neutralisés ;

- **juridique :** les sociétés utilisant des entreprises d'infogérance étrangère doivent prendre garde à la législation en vigueur dans le pays qui héberge leur informatique ainsi qu'à sa stabilité ;

- **économique :** un coût de transfert sous évalué et une baisse de la qualité de services. Une perte de savoir-faire en matière d'administration de systèmes définitive ;

- **organisationnelle :** la réversibilité éventuelle du transfert doit être clairement prévue contractuellement et organisée.

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

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

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

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

1.4.2 Les organisations sources de vulnérabilités

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

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

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

- **L'externalisation favorise les vulnérabilités**

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

Les principaux risques identifiés sont de nature :

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

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

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

1.4.3 Les vulnérabilités humaines peuvent être liées à :

- une mise en réseau déraisonnable et systématique ;
- **une méconnaissance de la menace** (formation inadaptée, sensibilisation insuffisante) qui peut engendrer de nouveaux risques, dans le cas notamment :
  - de l'utilisation d'architectures spontanées ;
  - face à des attaques d'ingénierie sociale ;
  - de la manipulation d'individus.
- **un mauvais climat social** susceptible de générer des mécontentements ou des vindictes ;
- **une insouciance des salariés, voire même de la direction, utilisateurs** de moyens informatiques ;
- **une utilisation mal contrôlée** : le risque résultant d'une connexion permanente « haut débit » à Internet (ADSL ou par câble) est supérieur à celui qui existait lorsque la consultation et les échanges se faisaient à travers un modem (modulateur-démodulateur) ;
- **une ergonomie inadaptée** : elle peut avoir des conséquences dramatiques (perte de données, diffusion d'informations secrètes, découragement des utilisateurs).

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

1.4.4 Les vulnérabilités extérieures

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

1.5 Des enjeux futurs en matière de SSI

1.5.1 Les aspects techniques

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

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

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

Parmi les tendances actuelles identifiées, le CERT-IST et le CERTA notent que les attaques visent préférentiellement les utilisateurs finaux, plutôt que les serveurs d'entreprise, mieux protégés.

La porte d'entrée du système d'information pour les hackers se déplace progressivement vers des équipements périmétriques, comme les lignes Internet protégées par des pare-feux, vers les postes de travail. « Il existe un lien très fort entre la sécurité individuelle des postes de travail et la sécurité informatique de l'entreprise. En protégeant son propre poste, on protège aussi les autres »[38].

[38] Source auditions

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

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

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

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

Un grand groupe auditionné a insisté sur **la séparation nécessaire entre l'équipe qui réalise et celle qui préconise.** Autrement dit, **le maître d'œuvre de la SSI ne peut pas être le donneur d'ordre.**[39]

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

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

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

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

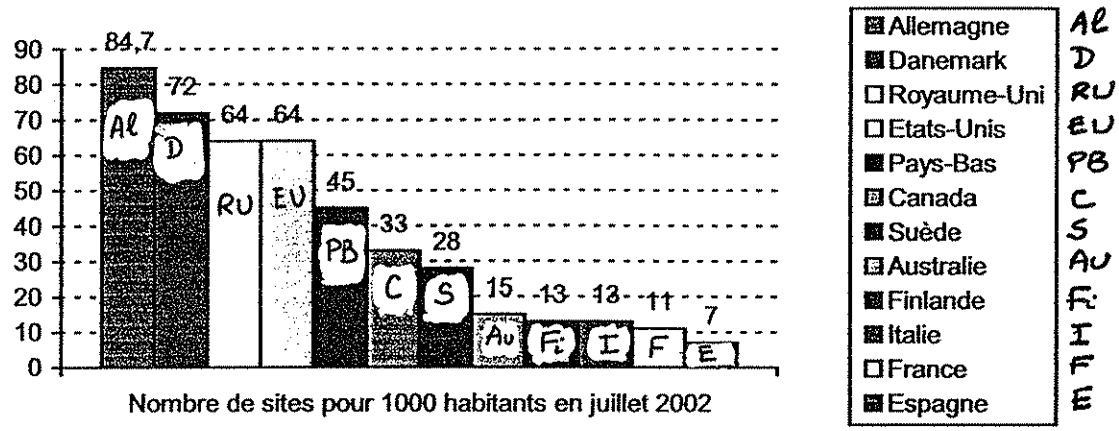
Les champs d'actions de la SSI et de l'Intelligence économique, se recoupent pour partie, car ils font la synthèse de l'économie de la connaissance, et donc de l'information. Pour être efficace, une politique volontariste d'Intelligence économique doit notamment s'appuyer sur des systèmes d'information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

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

[39] Source auditions

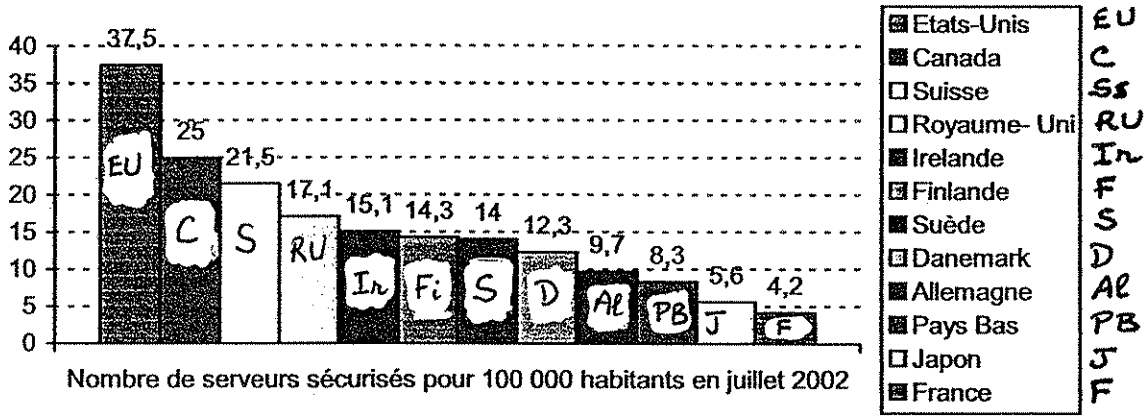
Un enjeu économique : un environnement sécurisé est nécessaire afin d'accompagner le rattrapage français dans l'usage des TIC par les citoyens et les entreprises françaises indispensable pour la croissance française.
Selon le tableau de bord du commerce électronique de décembre 2004[40] malgré un taux d'équipements comparable pour les entreprises, des retards persistants demeurent par rapport aux concurrents en matière d'usage. Retenons quelques données de cette étude de 2002 qui reste cependant d'actualité.

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



Nombre de sites pour 1000 habitants en juillet 2002

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



Nombre de serveurs sécurisés pour 100 000 habitants en juillet 2002

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

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

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

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

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

2 Les réponses organisationnelles et techniques

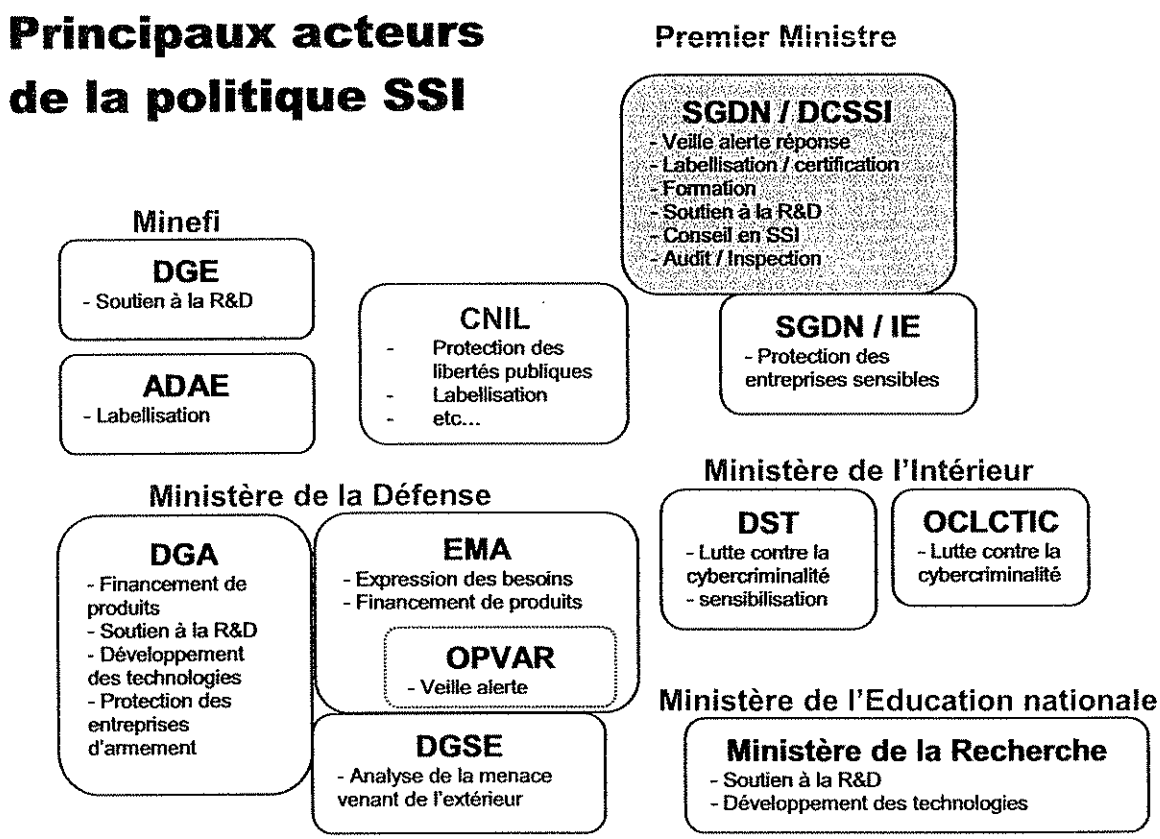
2.1 Comment l'Etat est-il organisé pour assurer la SSI ?

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

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

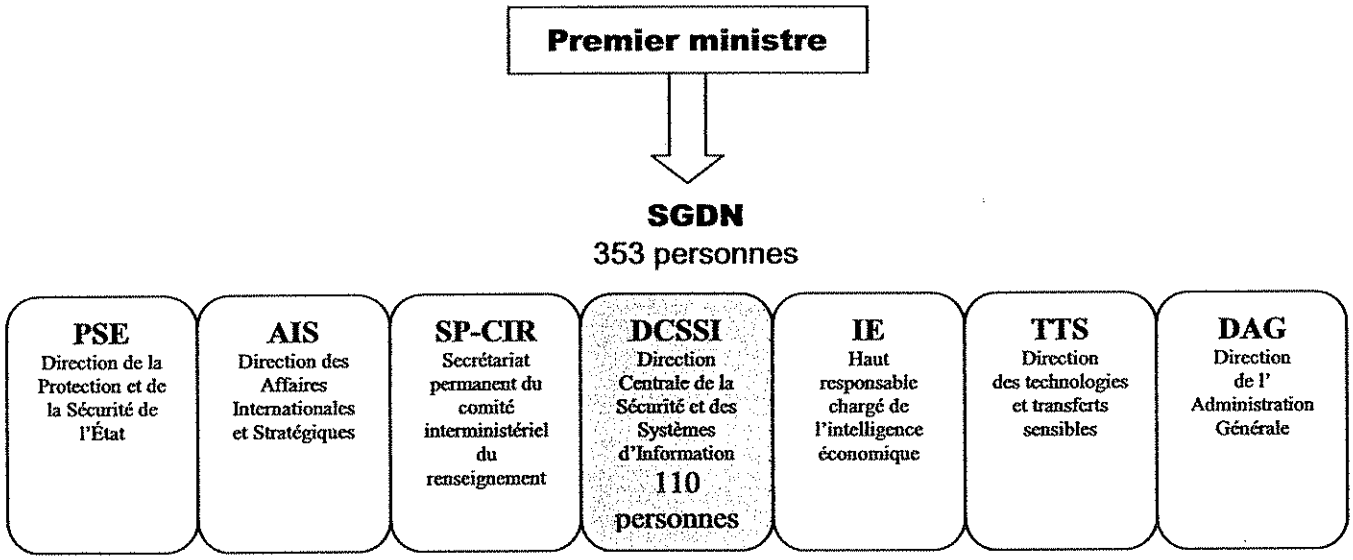
La réglementation en sécurité des systèmes d'information (SSI) n'existe pas sous la forme d'un code législatif ou réglementaire. La SSI n'est d'ailleurs pas même définie d'un point de vue juridique. En fait, le domaine de la SSI fait référence à une multitude de textes de niveaux juridiques très divers relatifs à l'organisation institutionnelle, à la protection des systèmes d'information, au développement de l'administration électronique, à la cryptologie, à la signature électronique ou à la cybercriminalité. (cf. Annexe 9)

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



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

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



Le décret n°96-67[41] *prévoit que* ***le Secrétaire général de la Défense nationale veille à la cohérence des actions entreprises en matière de sécurité des systèmes d'information*** *(article 1). Il suit l'exécution des directives et instructions du Premier ministre et propose les mesures que l'intérêt national rend souhaitables. Il coordonne l'activité de tous les organismes concernés et assure que les relations entre ceux-ci répondent aux objectifs définis par le Premier ministre. Il veille au respect des procédures applicables à des utilisateurs privés en matière de sécurité des systèmes d'information. Il participe à l'orientation des études confiées aux industriels et suit leur financement (article 2). Il est tenu informé des besoins et des programmes d'équipement des départements ministériels et veille à ce que ceux-ci soient harmonisés.*

Plus précisément, **la DCSSI**[42] (Direction centrale de la sécurité des systèmes d'information) assiste le Secrétaire général de la défense nationale **dans ses missions de sécurité des systèmes d'information** qui répondent à deux objectifs principaux :

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

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

[41] Décret n°96-67 du 29 janvier 1996 relatif aux compétences du secrétaire général de la défense nationale dans le domaine de la sécurité des systèmes d'information (NOR : PRMX 9600002D).

[42] Le décret 2001-69342 précise les missions de la DCSSI

La DCSSI :

- Contribue à la définition et à l'expression de la politique gouvernementale dans le domaine de la SSI. au sein de la Commission interministérielle pour la sécurité des systèmes d'information **(CISSI)**[43], présidée par le SGDN.

- Assure la fonction d'autorité nationale de régulation dans le domaine de la SSI.

  Dans ce cadre, la DCSSI :

  - organise les travaux interministériels et prépare les mesures que le Secrétaire général de la Défense nationale propose au Premier ministre ;

  - prépare les dossiers en vue des autorisations, agréments, cautions ou homologations délivrés par le Premier ministre, notamment pour l'application de la réglementation de la cryptologie, et en suit l'exécution ;

  - met en œuvre les procédures d'évaluation et de certification du décret 2002-535 (certifications ITSEC et Critères communs) ;

  - participe aux négociations internationales ;

  - entretient des relations avec le tissu des entreprises de SSI.

- Assiste les services publics dans le domaine de la SSI : audit, veille et alerte d'incidents, conseil.

  - Audit et inspection : chaque ministère et chaque grande entreprise a sa politique d'audit et d'inspection, effectuée par des ressources internes ou sous-traitée aux nombreuses sociétés privées commercialisant une telle offre. La DCSSI dispose d'une équipe chargée d'inspecter systématiquement la sécurité des systèmes d'information des ministères sur un cycle de trois ans. 8 personnes sont affectées à ces missions. **La faiblesse de l'effectif** conduit à limiter le nombre de ces inspections à seulement une vingtaine de déplacements par an sur les sites locaux et les organismes sous tutelles. **Ces relevés ponctuels et les inspections de l'administration centrale aboutissent à des recommandations adressées au Directeur de cabinet du Ministre concerné et du Premier ministre qui ont la responsabilité d'y donner suites.**

  - Veille, alerte, réponse : la DCSSI dispose d'un centre opérationnel de la sécurité des systèmes d'information, le **COSSI**, activé 24h/24 7j/7, et créé dans le cadre de l'élaboration des plans de vigilance (VIGIPIRATE) volet SSI et (PIRANET). Le COSSI est chargé d'assurer la coordination interministérielle des actions de prévention et de protection face aux attaques sur les systèmes d'information. Il est composé d'une unité de Conduite & Synthèse (CEVECS) et d'une unité technique, le CERTA[44] (centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques). Chacune de ces unités regroupe une dizaine de personnes. Les ministères et les opérateurs d'infrastructures vitales sont invités à signaler au COSSI les attaques dont ils sont victimes.

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

[44] Il existe d'autres Computer Emergency Response Teams (CERTs) français (CERT IST financé par des grands groupes industriels, CERT Renater pour les réseaux de recherche).

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

- Développe une expertise scientifique et technique.

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

- Organise la formation dans le domaine de la SSI

  Sensibilisation et formation : la formation des personnels de l'Administration incombe principalement au Centre de formation à la sécurité des systèmes d'information (CFSSI)[45], même si des initiatives de contractualisation dans le domaine de la formation ont été entreprises en partenariat avec des grandes écoles sur le modèle de celle, très complète, de sensibilisation, délivrée à l'attention des cadres du secteur privé par les écoles du GET regroupant l'ENST, l'ENST Bretagne et l'INT.

  L'objectif du CFSSI est double : dispenser une formation adaptée aux différents acteurs publics de la SSI et créer un réseau informel d'échanges avec les établissements d'enseignement supérieur et les centres de formations continues. A titre d'exemples le CFSSI propose plusieurs degrés de stages[46] de haut niveau de spécialisation ou de simple sensibilisation, d'une durée d'une journée, ou après deux années de formation tel que le Brevet d'études supérieures de la sécurité des systèmes d'information (BESSSI). En 2004, pas moins de 898 stagiaires avaient suivi l'une ou l'autre des formations[47].
  De très grande qualité, d'après un grand groupe d'infrastructures vitales, celles-ci sont **malheureusement restreintes aux personnels exerçant directement dans le domaine de l'informatique ou de la SSI.** De plus, **un déficit de notoriété de l'offre du CFSSI** limite le recours à cette opportunité.

2.1.2.2 Une multiplicité d'acteurs insuffisamment coordonnés

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

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

2.1.2.2.1 Le ministère de la Défense, un acteur majeur à distinguer

Le ministère de la Défense assure deux missions SSI distinctes :

- une mission de sécurité interne, comme dans tous les ministères ;
- une mission technique chargée de la prise en compte de la sécurité dans les programmes d'armement et de la réalisation de produits de sécurité à vocation ministérielle ou interministérielle.

Contrairement aux autres ministères, le ministère de la Défense n'a pas de Haut fonctionnaire de Défense (HFD)[48] et la responsabilité de la prise en compte de la SSI au ministère est dévolue aux autorités qualifiées (CEMA, DGA, SGA, CEMAT, CEMM, CEMAA, DGGN, DGSE, DPSD)[49], aux bureaux centraux de SSI, aux officiers de sécurité des systèmes d'information (OSSI) d'organismes centraux ou locaux et aux responsables de la sécurité des systèmes d'information (RSSI) de programmes ou de projets.

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

La politique SSI du ministère de la Défense est intégrée dans la politique générale des systèmes d'information définie par le Secrétariat du Directoire des systèmes d'information[50].

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

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

Des missions particulières sont confiées au ministère de la Défense en SSI, dépassant son propre périmètre, c'est à dire l'emploi ou la préparation des forces. Accompagnée de l'instruction [77], la recommandation [4201] précise que le ministre de la Défense :

- est « maître d'œuvre des équipements ou moyens destinés à protéger les systèmes d'information gouvernementaux lorsque ces équipements ou moyens sont susceptibles de satisfaire un besoin commun à plusieurs départements ministériels ou, lorsque le besoin est particulier, sur demande du département intéressé » ;

- a «la capacité d'apporter son concours aux contrôles et mesures que peuvent nécessiter les systèmes d'information en service dans les départements civils » ;

- est chargé de « doter l'État des équipes et laboratoires de mesures propres à satisfaire l'ensemble des besoins gouvernementaux. »

Au sein de la DGA, ces responsabilités particulières sont confiées au SPOTI, service de programmes de la DGA dédié à la conduite des programmes spatiaux, aux systèmes d'information et de commandement. Pour les travaux de réalisation des mécanismes

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

cryptographiques, de réalisation des circuits, d'expertise technique sur la réalisation de produits et systèmes et d'évaluation, la DGA dispose d'une division du CELAR.

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

La DGSE : la Direction générale de la sécurité extérieure

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

2.1.2.2.2 Exemples d'autres acteurs publics intervenant en matière de SSI

- **Le ministère de l'Intérieur de la sécurité intérieure et de l'aménagement du territoire**

La DST : la Direction de la surveillance du territoire

Dans le cadre de ses missions de lutte contre l'espionnage, de la lutte anti-terroriste et de la protection du patrimoine économique et scientifique, la Direction de la surveillance du territoire (DST) assure des prestations techniques et informatiques, autour de trois volets : la prévention, la répression et la sécurité informatique.

L'activité de prévention de la DST s'exerce dans quatre domaines distincts qui représentent les pôles de compétence du service : **la téléphonie, la criminalité informatique, les satellites et les matériels soumis à une réglementation** (art R226 du Code pénal). Pour ce faire, la DST entretient des relations avec les opérateurs de télécommunication (téléphonie, satellites, fournisseurs d'accès à Internet) et les sociétés de SSI, commercialisant des matériels pouvant porter atteinte à la vie privée, et les sociétés de cryptologie.

La DST assure également **une veille permanente dans le domaine des TIC.**

En matière de répression la DST dispose de pouvoirs de police judiciaire spécialisés concernant la **sécurité des réseaux gouvernementaux et des établissements à régime restrictif** (ERR).

La DST peut également se voir confier une mission d'expertise judiciaire consistant en **l'analyse de supports informatiques** lors des enquêtes judiciaires autres que dans le domaine du piratage informatique.

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

L'OCLCTIC : l'Office Central de Lutte contre la Criminalité liée aux technologies de l'information et de la communication.

En matière de lutte contre la cybercriminalité, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), structure nationale à vocation interministérielle et opérationnelle, a été créée en 2000 au sein de la Direction de la police judiciaire (DCPJ).

L'OCLCTIC est principalement chargé :

- d'animer et coordonner la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions liés aux TIC ;
- de procéder, à la demande de l'autorité judicaire, à tous actes d'enquêtes et travaux techniques d'investigation ;
- de centraliser et diffuser l'information sur les infractions technologiques à l'ensemble des services répressifs (DCPJ, Douanes, Gendarmerie).

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

- **Le ministère de l'économie, des finances et de l'industrie**

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

La DGE (Direction générale des entreprises)

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

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

L'ADAE :

L'ADAE (Agence pour le Développement de l'Administration Electronique), créée par le décret du 21 février 2003, publié au JO du 22 février, un service interministériel rattaché au ministre chargé du Budget et de la réforme de l'Etat.
L'agence pour le développement de l'administration électronique favorise le développement de systèmes d'information et de communication permettant de moderniser le fonctionnement de l'administration et de mieux répondre aux besoins du public.

Dans ce domaine :

- Elle contribue à la promotion et à la coordination des initiatives, assure leur suivi et procède à leur évaluation et apporte son appui aux administrations pour l'identification des besoins, la connaissance de l'offre et la conception des projets.
- Elle propose au Premier ministre les mesures tendant à la dématérialisation des procédures administratives, à l'interopérabilité des systèmes d'information, ainsi qu'au développement de standards et de référentiels communs.
- Elle assure, pour le compte du Premier ministre, la maîtrise d'ouvrage des services opérationnels d'interconnexion et de partage des ressources, notamment en matière de transport, de gestion des noms de domaine, de messagerie, d'annuaire, d'accès à des applications informatiques et de registres des ressources numériques.

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

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

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

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

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

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

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

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

La CNIL et la DCSSI ont commencé à travailler ensemble de manière quasi informelle. Mais si la CNIL a, aux termes de la loi, un pouvoir d'imposer que la DCSSI n'a pas, la DCSSI en

revanche, dispose du fait de ses origines, de compétences techniques incontestables. Dans le cadre des expérimentations menées suite au rapport Babusiaux (transmission d'information de santé vers les assureurs complémentaires) le système de transmission sécurisée envisagé par la FNMF (fédération nationale de la mutualité française) a été audité par la DCSSI à la demande de la CNIL. Il devrait en être de même pour le dispositif transitoire envisagé par AXA (avant les déploiements de Sésame Vitale 1.40 chez les pharmaciens). Cette non formulation peut-être très préjudiciable au bon fonctionnement de l'Etat.

2.1.2.2.3 Les conséquences de la multiplication des acteurs publics

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

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

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

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

« La sécurité des systèmes d'information relève de la responsabilité de chaque ministre, pour le département dont il a la charge.

A ce titre, chaque ministre prend, dans les conditions fixées par le Premier ministre et sous son contrôle, des dispositions en vue de :

- *développer à tous les échelons le souci de la sécurité ;*
- *apprécier en permanence le niveau de sécurité des installations ;*
- *recenser les besoins en matière de protection des systèmes d'information et veiller à ce qu'ils soient satisfaits.*

Dans les départements autres que celui de la Défense, ces attributions sont exercées par les Hauts fonctionnaires de défense. »

- **Organigramme type proposé** :

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

Le haut fonctionnaire de défense **(HFD)**

Dans chaque département ministériel, à l'exception de celui de la défense, le ministre est assisté pour l'exercice de ses responsabilités de défense par un ou, exceptionnellement, plusieurs hauts fonctionnaires de défense.

Le haut fonctionnaire de défense est responsable de l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information. Il contrôle en particulier les programmes d'équipement de son département. Il fait appel aux compétences du service central de la sécurité des systèmes d'information pour la spécification et l'homologation des produits et des installations.

Le fonctionnaire de sécurité des systèmes d'information **(FSSI)**

Dans les départements ministériels qui utilisent des systèmes d'information justifiant une protection ou qui assurent la tutelle d'organismes ou d'entreprises utilisant de tels systèmes, le ministre désigne un fonctionnaire de sécurité des systèmes d'information (FSSI), placé sous l'autorité du haut fonctionnaire de défense. Lorsque la charge de travail n'est pas suffisante, le ministre peut charger le haut fonctionnaire de défense d'assurer lui-même les fonctions de FSSI.
Une équipe de sécurité des systèmes d'information, à la disposition du haut fonctionnaire de défense et du fonctionnaire de sécurité des systèmes d'information, peut être constituée si les besoins du département ministériel l'exigent.

L'autorité qualifiée **(AQSSI)**

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

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

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

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

2.1.3 Des ressources humaines insuffisantes

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

En effet, la pénurie de personnel formé, associé au manque de perspectives de carrière au sein de l'Administration et au niveau de rémunération proposé, n'encouragent pas les candidatures. Face aux difficultés de recrutement de personnels, les ministères sont contraints soit à privilégier la spécialisation interne[51], soit à recourir à l'externalisation[52].

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

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

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

- Pour ce qui est de l'architecture de sécurité, si on peut regretter que la DCSSI n'ait pas un rôle plus directif dans ses missions de conseil, on constate cependant que des progrès ont été accomplis pour faire face à la menace externe. En revanche, la menace interne est insuffisamment prise en considération, en particulier lorsque des ministères disposent d'organes ou de services sous tutelle, le niveau de sécurité n'est pas toujours maintenu et garanti[53].

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

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

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

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

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

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

- corollairement à cette indifférenciation, il n'existe aucun chiffre précis du budget consacré à la SSI par ministère ;

- des schémas directeurs existent, la plupart sont en cours d'implémentation ;

- la classification des données sensibles (hors confidentiel défense et secret défense) ne semble pas obéir à une règle uniforme entre tous les ministères ;

- il n'existe pas, par ministère, une liste des logiciels associés aux applications traitant de ces données sensibles, démontrant une carence de l'attention portée aux solutions de confiance pour ce type d'application ;

- les chartes utilisateurs existent parfois, en cours d'élaboration pour certaines ou de mise en place pour d'autres ; en tout état de cause, il n'y a pas de règle précise concernant le descriptif précis de ces chartes, la manière de les appliquer, qui doit les signer, et à quel type de document les apposer.

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

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

L'Etat a la responsabilité, en relation avec les représentants des secteurs stratégiques économiques, de la protection des infrastructures vitales.
Les secteurs d'activités d'importance vitale sont les activités ayant trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, à l'exercice de l'autorité de l'Etat, au fonctionnement de l'économie, au maintien du potentiel de défense et à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables, ou peuvent causer un danger grave pour la population.

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

De plus en plus, ces activités nationales s'élargissent à des actions coordonnées au plan international (Table top exercice impliquant les pays du G8 en mai 2005) et européen avec notamment la préparation d'un Programme européen de protection des infrastructures critiques (EPCIP).

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

2.4 Comment sont organisés nos principaux partenaires étrangers ?

Les ressources humaines des agences homologues de la DCSSI, peuvent être considérées comme un bon indicateur de la priorité politique accordée à ces questions : environ 3000

personnes à la *Division Information Assurance de la NSA* aux Etats-Unis, 450 *au Bundesamt für Sicherheit in der Infromationstechnik* (BSI) en Allemagne et 450 au *Communications Electronics Security Group* (CESG) au Royaume-Uni, contre à peine 110 à la DCSSI. Disposant de plus de moyens que la DCSSI, ces agences développent un véritable partenariat privé-public centré sur les produits de sécurité.

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

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

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

L'E*xecutive order* 12333 du 4 décembre 1981 décrit les principales responsabilités de la NSA (*National security agency* créée le 4 novembre 1952). : ***« The ability to understand the secret communications of our foreign adversaries while protecting our own communications, a capability in which the United States leads the world, gives our nation a unique advantage ».*** Tout est dit en quelques mots sur le pouvoir que revêtent la maîtrise et la protection de son information pour un Etat.

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

L'Information Assurance a pour missions de :

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

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

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

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

L'USA PATRIOT ACT, promulgué en octobre 2001, invite à la mise en œuvre d'actions nécessaires à la protection des infrastructures critiques, actions développées sous la responsabilité de partenariats public privé. L'Office of Homeland Security (OHS) est établi par l'executive order 13228 et est chargé de coordonner les efforts de protection des infrastructures critiques.

Prise en compte de la menace : veille, alerte, réponse : la création du Department of Homeland Security par regroupement d'agences auparavant dispersées est un premier pas. Les responsabilités du DHS en matière de sécurité du cyberespace concernent la direction *Information Analysis and Infrastructure Protection and Directorate* (IAIP) chargée de :

- développer un plan national de sécurisation des infrastructures critiques ;
- mettre en place un dispositif de réponses aux attaques sur la sécurité les systèmes d'informations critiques ;
- assurer une assistance technique au secteur privé et aux administrations dans le cadre d'incidents sur les systèmes d'information critiques et coordonner la diffusion d'informations d'alerte et de protection ;
- encourager la recherche dans ces domaines techniques.

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

2.4.1.2 Royaume-Uni : un partenariat public-privé très développé

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

Le *Communications and Electronic Security Group* (CESG) placé sous l'autorité du *Communication Government Head Quarter,* chargé de la protection des systèmes d'information de l'Etat, est l'homologue de la DCSSI. Au Royaume Uni, le NISCC[54], rattaché au Home Office, s'appuie sur l'UNIRAS (CSIRT gouvernemental) pour fournir aux opérateurs des infrastructures critiques des avis techniques, des informations sur les menaces, les vulnérabilités et les niveaux d'alerte. Il s'appuie aussi sur des WARP[55], chargé de recueillir des alertes et de signaler des incidents (mais sans capacité d'intervention) et des ISAC[56], qui diffusent des informations d'alerte et d'incident au sein d'une communauté donnée d'utilisateurs, généralement sur une base commerciale.

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

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

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

dont l'objectif principal est de garantir la confidentialité absolue des informations transmises par le NISCC.

Le ministère de l'économie et de l'industrie poursuit sa procédure de tests fonctionnels des produits de sécurité, nommée GIPSI[57] et a émis deux premiers certificats (le niveau d'exigence est moins élevé que pour *les certificats critères communs*). Au CESG, les travaux se poursuivent sur le passeport électronique (délivrance des clés et évaluation du dispositif) pour une délivrance des premiers passeports à l'automne 2006. Par ailleurs, un nouveau programme de recherche (IADP[58]) a été mis en place afin d'optimiser les efforts dans le domaine SSI, en partenariat avec l'industrie.

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

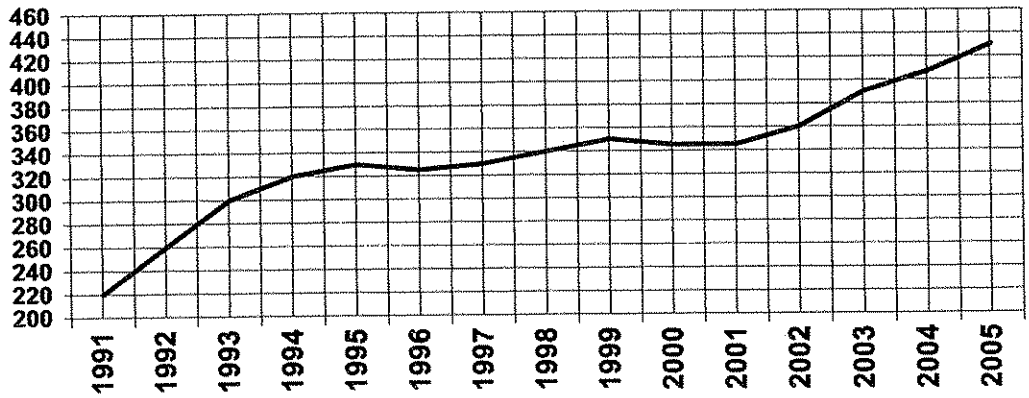
L'Allemagne a adopté en juillet dernier, un plan national pour la protection des infrastructures d'information (NPSI)[59] qui comporte trois objectifs principaux :

- la prévention afin de protéger convenablement les infrastructures ;
- la préparation afin de répondre efficacement en cas d'incidents de sécurité informatique ;
- le maintien et le renforcement des compétences allemandes dans le domaine SSI.

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

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

Evolution du nombre de salariés du BSI



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

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

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

- **Informer le pays**
  - o en sensibilisant le public aux enjeux de la SSI par exemple par une information trimestrielle sur leur site web et la production de CD-ROM conçus pour les citoyens. L'industrie supporte cette initiative du BSI et fournit gratuitement des démonstrateurs ;
  - o en participant à des campagnes de sensibilisation des PME en 2004 (Sécurité de l'Internet pour les PME) ;
  - o le BSI réalise également des analyses de tendance et des futurs risques qui pèsent sur les systèmes d'information.

- **Fournir des conseils et des supports techniques dans le cadre d'un partenariat avec le privé très fort :**
  - o ainsi le BSI a créé un **standard** professionnel en 1993, une «IT Baseline Protection » (les bases de la protection d'un système d'information) remise à jour constamment qui est devenu un standard pour l'industrie. C'est un ensemble de bonnes pratiques qui permettent de sécuriser un système (CD-ROM ou 3 classeurs papier). Au départ, des grandes entreprises allemandes (SIEMENS, DAIMLER, VW, des banques ...) se sont associées à cette initiative. La « baseline protection » est utilisée par le gouvernement et par les entreprises ;
  - o il assure du conseil et un support technique en sécurité des SI vers les agences gouvernementales par exemple l'initiative 2005 BundOnline ou la justice et la police ;
  - o il réalise des tests d'intrusion et apporte l'expertise sur la protection contre les bogues et les émissions radios. Ainsi, le BSI a une équipe spécialisée qui réalise des tests d'intrusion pour les ministères et les entreprises des secteurs sensibles ;
  - o la protection des infrastructures critiques est confiée au BSI qui a entrepris un travail d'identification de ces infrastructures, grâce à des exercices impliquant l'administration (ministères de l'intérieur, de la défense, des transports, des télécommunications) et des industriels. Dans ce cadre, il entretient des relations avec d'autres pays comme les Etats-Unis, la Suisse, la Suède et la Finlande ;
  - o le BSI conseille également les Länder sur le plan technique.

- **Analyser les risques, évaluer et tester :**
  - o le BSI assure la certification des produits et services de SSI (38 en 2004) ainsi que l'attribution de licences pour des applications classifiées ;
  - o il a une action particulière sur les procédures biométriques et des applications mobiles ;
  - o il conduit une analyse permanente de la sécurité Internet et de ses évolutions. Par exemple le BSI a une équipe spécialisée sur le projet de l'alliance TCG (Trusted Computing Group – Cf. infra § 3.1) qui a des relations avec TCG mais qui recherche aussi des alternatives.

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

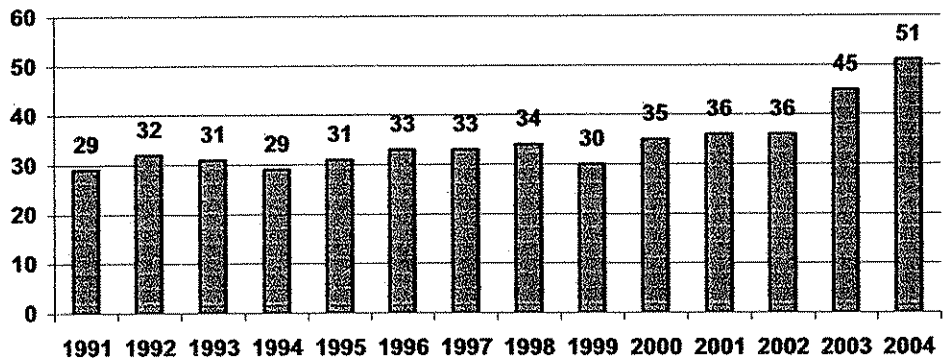
- **Assurer des fonctions opérationnelles :**
  - o assurer la fonction de CERT allemand (Computer Emergency Response Team) ;
  - o coordination technique du réseau d'information Berlin-Bonn ;

- administration de la PKI du gouvernement ;
- production de clés pour les équipements cryptographiques.

- **Jouer un rôle actif dans la normalisation et la standardisation**
  Le BSI joue un rôle actif dans les comités nationaux et internationaux de normalisation et de standardisation relatifs à la SSI.

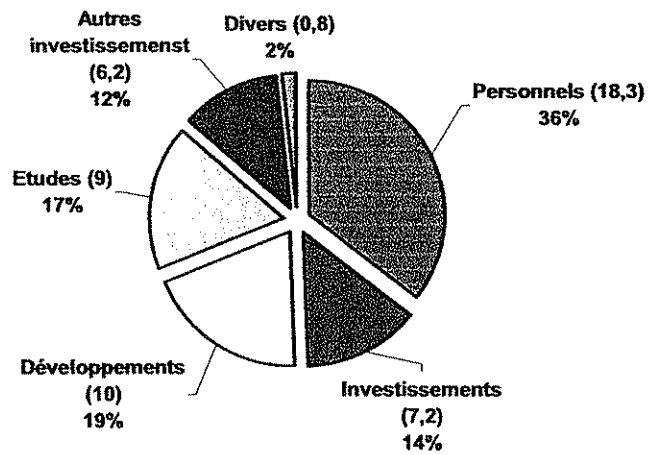
Pour assurer l'ensemble de ces missions, le BSI dispose d'un budget significatif de **51 millions d'euros** en augmentation régulière depuis 2002.

BUDGET en millions d'euros du BSI



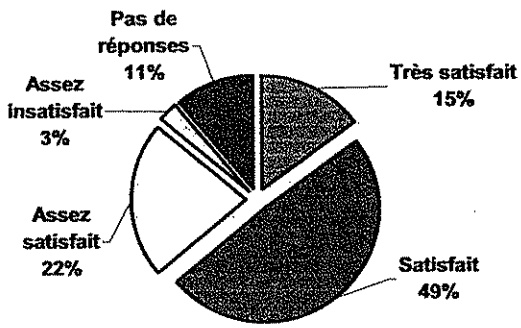
La répartition de ce budget, montre une action forte sur les développements, 10 M€, soit 19% du budget et les études pour 9 M€ soit 17% du budget que l'on ne retrouve pas en France.

Répartition des dépenses du BSI en 2004



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

Taux de satisfaction de l'action du BSI



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

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

La commission parlementaire sur la sécurité de l'information a publié son rapport final en septembre dernier et prône la mise en place d'une nouvelle politique de sécurité de l'information en Suède ainsi qu'une réorganisation des services compétents en matière de SSI. Il est ainsi proposé de s'appuyer sur les compétences existantes en matière de renseignement électronique pour renforcer les capacités dans le domaine SSI et partager ainsi les responsabilités entre deux agences : la SEMA[60] pour les aspects organisationnels et l'IST[61] (appelé à remplacer le FRA[62]) pour les aspects techniques. Un projet de loi pourrait être présenté prochainement pour mettre en place l'ensemble de ces propositions.

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

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

A la suite de la journée noire du 25 janvier 2003 au cours de laquelle les réseaux d'information et l'économie coréenne ont été paralysés pendant plusieurs heures à cause d'un virus, le ministère de l'Information et de la Communication sud-coréen a créé une nouvelle organisation rassemblant les procureurs, la police et les services de renseignement en vue de prévenir l'attaque des infrastructures et des systèmes d'information et les perturbations qui en résultent. Le 20 juin 2003, le président sud-coréen Roh Moo-Hyeon a ordonné au National Intelligence Service (NIS) que des mesures soient prises pour faire face

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

à ce type de situation. **Le National Security Council (NSC)**, structure de la présidence sud-coréenne, est chargé de définir la politique de lutte contre la criminalité informatique, de la mettre en pratique et d'assurer la coordination entre les différentes agences.

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

2.4.1.6 Israël : le rôle prépondérant du ministère de la défense

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

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

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

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

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

- **Activités européennes**

La Commission européenne a publié en juin dernier une communication sur un nouveau programme dans le domaine de la société de l'information, faisant suite au programme

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

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

L'importance croissante accordée dans l'Union européenne aux questions de sécurité et la nécessité d'améliorer le partage de l'information et la coopération entre les initiatives nationales en la matière ont amené le Conseil et le Parlement de l'Union européenne à approuver, au début de 2004, la création d'une agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[63]. Son principal objectif est de promouvoir le développement d'une culture de la sécurité des réseaux et de l'information au sein de l'Union européenne.

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

Le directeur de l'agence est un Italien, M. Pirotti, qui vient du secteur privé.

• ONU

Les Nations Unies ont perçu très tôt les nouveaux enjeux, liés à la sécurité des systèmes d'information, dans leurs différentes composantes : juridiques, économiques et de sécurité nationale. Ainsi, depuis 1998, l'Assemblée générale a adopté plusieurs résolutions relevant de la 1ère commission sur les conséquences de l'utilisation des technologies de l'information et des communications (TIC)[64], de la deuxième commission sur le développement d'une

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

[64] Résolutions n° 53/70 of 4 décembre 1998, 54/49 du 1er décembre 1999, 55/28 du 20 novembre 2000, 56/19 du 29 novembre 2001, 57/53 du 22 novembre 2002, 58/32 du 8 décembre 2003 et 59/61 du 3 décembre 2004.

culture globale de la cybersécurité[65] et de la troisième commission sur la lutte contre l'utilisation criminelle des technologies de l'information[66]. Ces résolutions ont permis entre autres d'élever au niveau international des travaux menés par des organisations plus régionales telles que l'OCDE, le G8 ou le Conseil de l'Europe. Elles ont également mis en place un groupe d'experts gouvernementaux chargé d'examiner les menaces potentielles et existantes dans le domaine de la sécurité de l'information et les mesures possibles de coopération à mettre en place afin de mieux les contrer. En raison de fortes oppositions entre les Etats-Unis et la Russie sur la prise en compte de l'utilisation des TIC à des fins militaires, ces travaux n'ont pas abouti à ce jour mais pourraient donner lieu à moyen ou long terme à une nouvelle convention régissant l'utilisation des TIC aux dépens de la sécurité nationale et internationale et complétant le droit international dans ce domaine.

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

L'UIT[67] et l'assemblée générale des Nations Unies ont décidé d'organiser un sommet mondial sur la société de l'information. La première phase du sommet, tenue à Genève du 10 au 12 décembre 2003, a permis l'adoption d'une déclaration de principes et d'un plan d'action, dont une section est dédiée à la sécurité de l'information et des réseaux. La deuxième phase du sommet, a eu lieu du 16 au 18 novembre 2005, et a consacré ses travaux au problème épineux de la gouvernance de l'Internet ; elle a notamment examiné la possibilité d'une internationalisation de la gestion des ressources de l'Internet.

• OCDE

Le groupe de travail sur la sécurité de l'information et la protection de la vie privée (WPISP[68]), qui dépend du comité PIIC (Comité de la politique de l'information, de l'informatique et des communications), se réunit deux fois par an à Paris au siège de l'OCDE. Il réunit des experts des 30 Etats membres de l'OCDE ainsi que des représentants du secteur privé et de la société civile. Il favorise le rapprochement des politiques publiques dans ce domaine par l'échange d'information et la promotion de bonnes pratiques. L'OCDE a émis en juillet 2002 des lignes directrices sur la sécurité des systèmes d'information et des réseaux[69] qui ont donné naissance à un nouveau concept : la promotion de la culture de la sécurité. Depuis cette date, le WPISP s'efforce de mieux comprendre les stratégies nationales mises en place pour répondre à ces lignes directrices et de cerner les nouveaux enjeux dans ce domaine liés à l'évolution des technologies.

• G8

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

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

en œuvre des « bonnes pratiques » dans le domaine de l'alerte et de la veille informatique (CERT) ; la conduite d'exercices communs pour tester les capacités de réactions en cas d'incidents ; la sensibilisation des autres pays à ces questions.

En mai dernier, le G8 a organisé un « Table Top Exercice », premier exercice sur les infrastructures critiques d'information impliquant les Administrations et l'industrie. Cet exercice a permis d'identifier des points de contacts au sein des CERTs, des services de police. La DCSSI, l'OCLCTIC ainsi que des représentants d'EDF et de RTE y ont participé.

Coopération internationale entre les CERTs

La mise en place de dispositifs d'alerte tels que les CERTs (Computer Emergency Response Teams) afin de pouvoir faire face à des attaques de virus ou à toutes sortes de nouvelles vulnérabilités nécessite de nombreux échanges entre les équipes aux niveaux national, régional et international. Pour la France, ces échanges ont lieu à l'échelle internationale au sein du FIRST[70] et à l'échelle européenne au sein de la TF-CSIRT[71] qui contribue également à la formation des nouvelles équipes. Enfin, la coopération étroite entre les CERTs gouvernementaux de six pays européens est très fructueuse.

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

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

2.5.1 Le déplacement des enjeux et des risques vers l'économique

- **Gérer le paradoxe de l'ouverture et de la protection**

Le système d'information de l'entreprise est désormais déployé dans un contexte d'entreprise étendue permettant un travail en réseau avec ses clients ou usagers, ses fournisseurs, ses donneurs d'ordre, ses partenaires ou les représentants de l'administration. Ces échanges génèrent des vulnérabilités pour les systèmes d'information de l'entreprise vis-à-vis d'attaques potentielles contre lesquelles elle doit se protéger.

En outre, la généralisation des outils nomades (téléphones mobiles, PDA, ordinateurs portables...) et le passage au tout numérique gomment la frontière entre espace professionnel et espace privé, accentuent très significativement les risques.

- **De nombreux sinistres identifiés dans les entreprises**

Dans l'étude Clusif 2003[72] qui met en évidence les principaux sinistres chez les grandes et moyennes entreprises on notera que:

[70] Forum of Incident Response and Security Teams.

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

[72] Enquête intersectorielle auprès de 608 entreprises et 111 collectivités publiques (de 10 à 199 salariés : 54%, 200 à 499 : 27% ; 500 à 999 : 12% ; + de 1000 :7%)

- **41%** des sondés déclarent avoir subi un sinistre dont 76% n'ont procédé à aucune évaluation de l'impact financier ;
- les facteurs déclenchant se répartissent comme suit : infection par virus (35%), panne interne (18%), vol (15%), perte de services essentiels (10%), erreurs d'utilisation (8%), évènement naturel (3%).

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

- **Des incidences économiques considérables**

Les incidents dus à une défaillance de la SSI peuvent affecter l'ensemble des activités et du patrimoine de l'entreprise et peuvent conduire à :

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

De manière moins visible mais plus lourde de conséquences, les actions d'espionnage industriel relayées parfois par des moyens étatiques vont se traduire pour les entreprises françaises par une perte de substance ou de compétitivité et au final par des incidences négatives sur l'emploi. Un parallèle s'impose avec les dommages causés par la contrefaçon qui représente un coût en France évalué à 6 milliards d'euros et le nombre d'emplois perdus à 30 000 par an[73].

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

D'après une étude de l'institut américain en sécurité informatique CSI[74], menée en 2004 en partenariat avec le FBI ("Federal Bureau of Investigation"), une société perdrait **en moyenne** 204 000 dollars par an consécutivement aux incidents de sécurité informatique. Le « US CERT » américain quant à lui évalue à 506 670 dollars par an les conséquences financières des incidents de sécurité en entreprise.

La fiabilité de ces chiffres est très relative. D'une part, de nombreux responsables sécurité des systèmes d'information (28% des participants) ne connaissaient pas le nombre d'attaques réussies survenues dans leur entreprise. D'autre part, même concrétisées, les conséquences de ces incidents et leurs coûts demeurent difficiles à évaluer.
Ainsi lors de l'étude sécurité 2005 du CERT, 62% des personnes interrogées n'ont pu chiffrer précisément la perte annuelle engendrée par les incidents de sécurité informatique.

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

[73] Source Minefi

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

- **Des protections insuffisantes, en particulier dans les PME** (Etude Clusif 2003)

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

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

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

2.5.2 Un référentiel SSI partagé, des enjeux et des réponses spécifiques

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

La sécurité est certes liée à la fiabilité du système d'information, mais au-delà des équipements et des équipes en charge de leur sécurisation, elle implique pour les dirigeants de ces entreprises la mise en oeuvre d'une réflexion globale sur la maîtrise de ces risques impliquant l'ensemble de ses personnels ainsi que ses partenaires sur le périmètre de ses activités.

Le déploiement de solutions de sécurité (produits ou services) et des procédures associées doit s'inscrire dans une démarche préventive, les investissements nécessaires pour couvrir raisonnablement et efficacement les menaces potentielles étant en général sans commune mesure avec les conséquences d'une attaque majeure qui pourrait se traduire par des pertes économiques ou d'image considérables voire à une perte d'indépendance ou à une cessation d'activité.

- **Vers un référentiel commun de bonnes pratiques**

Les pouvoirs publics, des cabinets de conseil spécialisés en SSI, des SSII, des éditeurs de logiciels, des fournisseurs de matériels de sécurité, des organisations patronales, notamment le Medef[75], et des organismes privés et publics divers ont formalisé des recommandations convergentes pour une démarche de sécurisation des grandes entreprises et des PME/PMI :

  - bâtir une politique de sécurité ;
  - connaître les législations en vigueur, les jurisprudences et les usages en vigueur dans chaque pays où les activités s'exercent ;
  - alerter et activer les services compétents ;
  - mettre en œuvre des moyens appropriés à la confidentialité des données ;
  - sensibiliser et mobiliser les personnels par une charte d'utilisation, des campagnes régulières de formation et de sensibilisation ;

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

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

- **A chaque entreprise, sa propre démarche d'implémentation**

Si les entreprises et les organisations sont toutes menacées, elles ne sont pas exposées au même niveau de risque. Il y a en effet des jeux de facteurs aggravants tels que :

- la taille et la complexité des activités ;
- le déploiement mondial des implantations et des systèmes d'information ;
- la nature des activités (nucléaire, défense, agro-alimentaire, réseaux d'infrastructures...) qui peuvent créer une attractivité en tant que cibles privilégiées pour des pirates, des terroristes, des concurrents ou des Etats ;
- la culture ou l'expérience en matière de sécurité et de protection acquises par l'entreprise et l'organisation.

Elles doivent donc adopter leur démarche à leur situation particulière.

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

Selon une étude récente de Ernst&Young[76], les obstacles principaux à la mise en œuvre d'une sécurité efficace des SSI sont les suivants :

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

Source : Etude Ernst & Young - 2005

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

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

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

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

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

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

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

- **Des freins organisationnels**

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

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

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

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

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

Le RSSI d'un grand groupe manufacturier[77] est ainsi rattaché directement au PDG. Il anime et contrôle une structure transversale « sécurité » qui croise et s'impose à la responsabilité SSI de chaque grande unité opérationnelle (cette structure matricielle est doublée d'une structure d'audit indépendante qui couvre également le domaine SSI). Il a tout pouvoir d'arrêter un dispositif opérationnel s'il juge que la politique de sécurité n'est pas respectée, même si cette décision est susceptible de générer des pertes financières significatives.

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

[77] Source auditions

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

Certaines entreprises, par leurs activités notamment liées à la Défense nationale, ont une pratique des données classifiées ou des données sensibles[78]. D'autres entreprises se sont appuyées sur ces méthodologies afin d'identifier, de classifier et de protéger de manière spécifique certaines informations sensibles.

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

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

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

D'après une étude du Clusif réalisée en 2004, 21,4 % des responsables en sécurité des P.M.E. de 200 à 499 salariés estiment que cette justification est effectivement nécessaire, mais dans les entreprises de plus de 2 000 salariés, ils ne sont plus que 7,5 %. Plus les dirigeants sont informés de leur responsabilité civile ou pénale, moins ils exigent de justifier une dépense en sécurité informatique par un rendement particulier. Ainsi, pour plus de 26 % des responsables sécurité, **la première justification des investissements en sécurité est désormais de se conformer aux réglementations**. Ce taux atteint 37,5 % dans les grandes entreprises.

L'étude CSI/FBI 2005, précise en outre que seules 25% des entreprises prennent une assurance extérieure contre les risques de menaces informatiques. La menace reste sous estimée.

- **Le budget SSI souvent insuffisant**

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

Selon l'étude CSI/FBI 2005 : 27% des sondés dépensent plus de 6% de leur budget informatique en SSI, près d'un quart de 3 à 5%, autant de 1 à 3% et 25% moins de 1% ou ne savent pas. **Les grandes entreprises françaises sensibilisées dépensent quant à elles en moyenne 6% de leur budget informatique en SSI**[79]. La motivation à investir dans la SSI varie de manière considérable selon la taille de l'entreprise.

[78] Source auditions

[79] Source auditions

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

2.5.4.1 Quelques exemples d'organisations[80]

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

Quelques points clés se dégagent :

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

- **Politiques de sécurité** : en complément d'une politique de sécurité générale, qui intègre des règles, des instructions et des recommandations, mise en œuvre de politiques complémentaires SSI dédiées :
  - en cas de crises ;
  - pour les filiales ;
  - pour les réseaux sans fil ;
  - pour les fournisseurs ;
  - pour les personnels (internes, administrateurs systèmes, missionnaires, expatriés,...).

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

- **Organisation** :
  - la présence de RSSI rattaché à une direction en charge de la sécurité des systèmes d'information au niveau groupe et des RSSI par branches ou filiales ;
  - un suivi régulier des plans d'actions validés par la Direction Générale ;
  - des cellules de veille et de crise activées en H24 7/7 ;
  - une externalisation croissante d'un certain nombre de fonctions mais pas d'externalisation globale ;
  - la réalisation en interne ou sous traitée de tests d'intrusion ;
  - la réalisation d'audits sur les différentes entités des groupes.

- **Personnels** :
  - des formations / sensibilisations pour **tous** les personnels ;
  - la **signature de chartes** (Cf. annexe 11 pour des exemples) d'utilisation des systèmes d'information par tous les salariés. Celles-ci peuvent être annexées au contrat de travail ou faire partie du règlement intérieur des entreprises.

- **Aspects techniques** :
  - existence de solutions redondantes pour les systèmes critiques et des évolutions en cours pour disposer de solutions de secours général ;
  - sécurisation des postes individuels et des nomades ;
  - sécurisation de l'accès aux réseaux privés des entreprises et à Internet ;
  - la sécurisation des données sensibles devient une priorité conduisant à l'utilisation croissante du chiffrement de tous les flux échangés pour l'accès

[80] Source auditions

aux données techniques, financières,... stockées dans des banques de données ;
- renforcement croissant des contrôles d'accès (sécurisation de l'authentification, gestion et contrôle des habilitations, authentification forte,...) ;
- logique de hiérarchisation : l'accès aux systèmes d'information est possible de l'intérieur ou de l'extérieur selon des droits affectés à la personne, à sa fonction et au niveau de sécurité de son poste au moment de la connexion ;
- sécurisation en cours des données et des accès des partenaires ;
- approches spécifiques pour les dirigeants.

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

2.5.4.2 Une montée en puissance de l'infogérance de sécurité

La définition d'une politique SSI, sa mise en œuvre et sa **maintenance** peuvent être assurées par des ressources internes, par une sous-traitance à un prestataire de services informatiques ou par l'utilisation des services mutualisés à distance par des MSSP[81] (tests de vulnérabilité, cartographie des flux applicatifs, gestion des moyens de protection, gestion des identifications/authentifications...).

Même si les RSSI, à une large majorité, ne confieraient pas l'ensemble de l'administration de la SSI à un prestataire unique comme le montre l'enquête CSO d'avril 2005[82] dans laquelle la sécurité est gérée en interne à 82,4%, la montée en puissance de l'infogérance en France se confirme. En effet, selon l'enquête IDC Sécurité 2005[83], en moyenne 60% des sondés font appel à des prestataires externes pour intégrer les solutions de sécurité et 43% pour définir la politique de sécurité. Enfin, 39% des sondés confient certaines activités de leur politique de sécurité à une société d'infogérance, parmi lesquels 26% externalisent l'ensemble de l'administration de la sécurité de leur système d'information.
Selon un sondage LOGICACM[84] les motifs d'externalisation sont liés principalement à la réduction des coûts (89%) et l'accès à de nouvelles technologies (60%) et d'après le Syntec[85], la croissance de l'activité d'infogérance informatique, qui intègre également de la SSI, sur 2005 a été de plus de 10% et devrait se poursuivre sur 2006.

On peut cependant noter que certaines entreprises expérimentent des modèles hybrides, par exemple BNP Paribas qui a créé une joint venture avec IBM pour gérer une partie de son activité informatique mais qui a gardé en interne la maîtrise de la sécurité, la relation avec les métiers et la gestion des applications[86].

L'inventaire et l'élaboration de la politique de sécurité imposent généralement l'intervention de consultants externes qui doivent s'inscrire dans une relation de partenaires de confiance car ils seront amenés à identifier les cibles potentielles ou les failles des systèmes

[81] Managed Security Service Provider
[82] CSO Entreprise & Sécurité de l'Information – Enquête auprès de 144 entreprises de plus de 200 salariés
[83] Enquête IDC Sécurité 2005 – 103 entretiens auprès d'un panel de grandes entreprises et administrations en France composées à 45% de plus de 2000 salariés et 55% de 1000 à 1999 salariés – novembre 2005
[84] Source L'Agefi
[85] Source Syntec et 01 Informatique
[86] Source L'Agefi

d'information. Ainsi, les **RSSI souhaitent à une large majorité que la certification des prestataires soit obligatoire.**

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

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

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

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

- **Une capacité insuffisante à répondre à un risque d'accident grave**

Il n'y a que **30%** des entreprises françaises du panel de l'enquête Ernst & Young qui estiment pouvoir faire face à un risque d'incident grave et pouvoir assurer leur continuité d'activité (**47%** pour le reste du panel mondial).

Si beaucoup d'entreprises ont mis en place une organisation SSI et des plans de continuité, il est cependant très inquiétant de constater que plus d'un tiers des entreprises, françaises ou mondiales, reconnaissent ne pas tester leur plan de continuité de l'activité (31%), leur plan de secours informatique (21%) et/ou leur plan d'intervention d'urgence suite à un incident (30%).

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

Les nombreuses dispositions législatives et réglementaires qui s'appliquent à la SSI procèdent de trois grandes préoccupations majeures dont certaines peuvent parfois être antinomiques :

- les atteintes aux droits de la personne ;
- les atteintes aux systèmes d'information ou l'usage délictueux de l'informatique ;
- les menaces spécifiques sur les activités liées à la Défense et à certaines activités sensibles.

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

Par exemple la loi Sarbannes-Oxley, votée par le Congrès en juillet 2002, suite aux affaires Enron et Worldcom, implique que les Présidents des entreprises cotées des Etats-Unis certifient leurs comptes auprès de la Security and Exchange Commission (SEC), l'organisme de régulation des marchés financiers US. Cette loi est guidée par 3 grands principes :

l'exactitude et l'accessibilité des informations, la responsabilité des gestionnaires et l'indépendance des vérificateurs / auditeurs.

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

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

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

Cependant, il existe une disproportion de jugement chez les magistrats, pour qui une intrusion physique au sein d'un établissement bancaire sera considérée comme plus grave qu'une intrusion par mode informatique, alors que les préjudices financiers conséquences de ce dernier peuvent être plus significatifs.[87]

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

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

- **Le besoin impératif d'outils et d'architectures certifiés**

En matière de produits, les entreprises expriment une forte demande de produits certifiés tels que :

- techniques et protocoles cryptographiques (chiffrement de messages, signature électronique, sécurité des transactions commerciales,...) ;
- fabrication de réseaux virtuels privés ;
- pare-feu matériel et/ou logiciel ;
- systèmes de détection d'intrusion et de surveillance réseaux, systèmes antivirus ;
- filtrage de contenus, antispams... ;
- tatouage électronique ;
- cartes à puces et infrastructures associées ;
- identification biométrique...

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

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

[87] Source auditions

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

Le **troisième niveau** est de pouvoir disposer à moyen terme :

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

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

La maintenance au fil de l'eau 24h/24h et 7j/7j et la garantie de déploiement des mises à jour sur l'ensemble du parc dans des délais généralement de l'ordre de l'heure ou de la demi-heure constituent un enjeu majeur pour la majorité des responsables de SSI des grandes entreprises.

Cela exige des solutions techniques fiables et certifiées, un processus régulier de déploiement des correctifs de sécurité et une équipe de supervision en alerte permanente prête à intervenir à l'arrivée de nouvelles failles de sécurité des systèmes d'exploitation et à réagir aux déploiements de nouvelles menaces.

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

- **L'identification du bon interlocuteur**

Les entreprises qui ne disposent pas d'expertises internes ou de connaissances précises de l'organisation de l'Etat ont des difficultés à **identifier rapidement le bon interlocuteur**[88] parmi les nombreux services de l'Etat.

Elles souhaiteraient pouvoir disposer d'un **guichet unique** permettant :

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

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

Cette organisation génère un chevauchement des compétences et une absence d'optimisation des ressources qui rend la coordination des actions défensives ou

[88] Source auditions

d'investigations extrêmement complexes et se traduit généralement par un manque d'efficacité et de réactivité alors que les attaques se font plus précises, rapides et violentes.

- **Les entreprises françaises sont confrontées à des contraintes particulières dans leurs activités internationales**

Les grands groupes français déployés à l'international conjuguent par nature toutes les contraintes :

- d'une organisation complexe ;
- d'une organisation s'exerçant dans des environnements variés, parfois hostiles ou pouvant coopérer avec des concurrents ;
- de cadres législatifs ou réglementaires à l'étranger insuffisamment connus et mal maîtrisés.

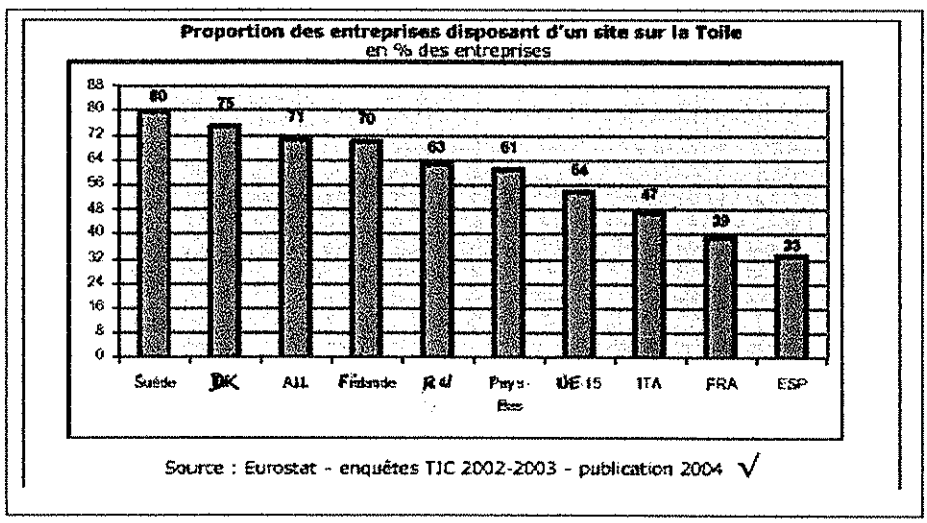
Les entreprises intervenant à l'international **souhaitent** disposer d'un support efficace des services de l'Etat pour les accompagner face aux risques spécifiques de l'international : veille, alertes, informations sur les menaces, conseils (juridiques, procédures, méthodologie, outils et solutions,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

En outre, **l'interdiction ou la limitation du chiffrement dans certains Etats** devient problématique pour la politique de sécurité de grands groupes[89].

2.5.8 Les problématiques spécifiques des PME face à la SSI

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

Ce retard des PME françaises et de la France en général, dans l'usage des TIC, qui a été présenté au § 1.5.3 est également attesté par les éléments chiffrés ci-après issus de l'étude de la Mission pour l'Economie Numérique 2004[90], relatifs à la proportion des entreprises disposant d'un site sur Internet fin 2002. La France, l'Italie et l'Espagne affichent des taux d'équipements nettement inférieurs aux autres pays.



[89] Source auditions

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

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

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

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

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

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

2.5.8.2 Une absence de moyens et de compétences suffisants expose les PME

De tailles plus réduites et disposant de moins de moyens que les PME de pays concurrents, les PME françaises sont confrontées à :

- une difficulté pour investir dans les TIC et la SSI, qui risque de les exclure des chaînes de fournisseurs ;
- une quasi impossibilité de s'appuyer sur des compétences fortes en SSI et plus généralement en TIC.

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

Le concept d'entreprise étendue, que l'on peut définir comme un ensemble d'entreprises indépendantes du point de vue capitalistique mais qui travaillent pour des clients communs, un marché spécifique ou pour un produit identifiant un marché (automobiles,...), prend une ampleur qu'il convient de ne pas négliger. L'entreprise étendue est désormais considérée comme un levier de performance dont **les technologies de l'information sont une composante essentielle** avec en particulier les technologies EDI, le trio Internet / intranet / extranet, datawarehouse[91], workflow[92],...

Compte tenu de l'importance des TIC dans cette nouvelle organisation, le traitement de la problématique SSI devient primordial. Selon une étude réalisée par l'éditeur Novell[93] auprès de 80 décideurs informatiques sur la zone EMEA (Europe, Moyen-Orient et Afrique), le premier critère des entreprises pour choisir un outil de collaboration en temps réel est **la sécurité (69%),** loin devant la conformité à la réglementation (13%) et l'interopérabilité (13%).

La tendance sera donc de voir **les grands groupes imposer progressivement des impératifs de sécurité à l'ensemble de leur chaîne de fournisseurs.** Un rapprochement doit être opéré avec le processus qui a conduit à la mise en œuvre d'une politique « qualité ». Rappelons que l'action de l'Etat en matière de politique « qualité », à travers les

[91] Stockage de données

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

[93] Source Le Monde Informatique

DRIRE (MINEFI), a consisté notamment à prendre en charge une partie significative des dépenses engagées par les entreprises pour la mise en conformité aux normes ISO 9000 et la formation du personnel. Cette politique avait réellement permis à de nombreuses PME de progresser en matière de qualité, mais également de soutenir l'activité des sociétés de conseil sur ces thématiques. Une politique similaire pourrait être envisagée en matière de certification de sécurité.
Ainsi, l'AFNOR[94] constate un intérêt croissant porté à la politique de sécurité induit par la norme ISO 17799 (issue de la norme BS 7799).

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

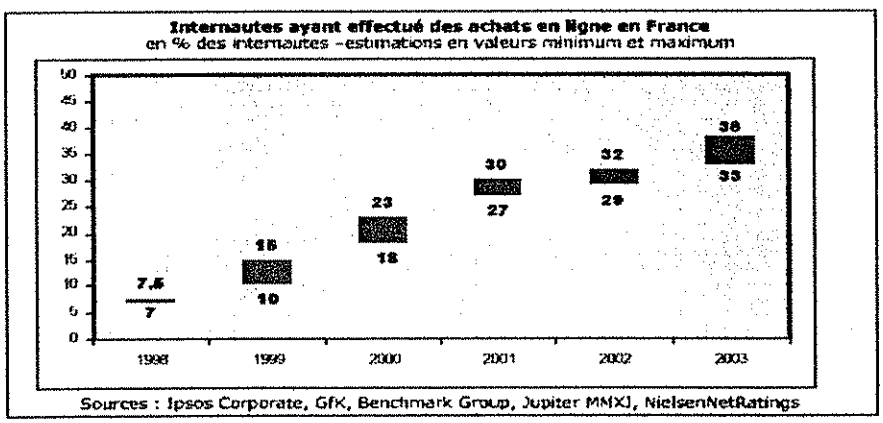
Les tendances du marché et surtout les positionnements pris par de nombreux acteurs informatiques le démontrent, **les PME apparaissent comme un futur marché en croissance en matière d'infogérance et de services de sécurité informatique** afin de compenser leurs déficiences internes qui les obligent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

Ainsi des opérateurs industriels, filiales de groupes étrangers asiatiques, sont en train de préparer des offres orientées sur les entreprises disposant de 50 à 500 postes principalement des PME, laissant les entreprises de plus de 1 000 postes aux SSII[95]. Les PME confiant à des tiers le cœur de leur société, sont dans une situation de faiblesse par rapport à l'offre de sociétés de services bien plus importantes.

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

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

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



[94] Source auditions
[95] Source 01 Informatique

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

La campagne lancée récemment pour prévenir les internautes de ne jamais divulguer de données personnelles, en particulier sur les « Chats », va dans le sens d'une meilleure prise de conscience des risques. Il est à noter également la première semaine nationale de la sécurité informatique du 3 au 10 juin 2005[96]. Ce type d'action est à amplifier.

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

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

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

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

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

[96] Source Délégation aux usages de l'Internet

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

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

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

Le secteur des TIC, dont fait partie la SSI, peut se caractériser de manière synthétique par :

- son caractère totalement mondialisé avec des fournisseurs performants et des utilisateurs répartis à travers le monde ;
- une vitesse très rapide des évolutions technologiques et des usages ;
- une complexité croissante conséquence d'une explosion des usages qui orientent les marchés, avec la prolifération des terminaux et produits de toutes sortes.

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

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

Le marché en matière de produits, logiciels et services en sécurité des systèmes d'information est intrinsèquement difficile à délimiter tant techniquement que financièrement. Quelques exemples illustrent cette difficulté :

- la réalisation d'un système d'information est susceptible d'inclure des prestations pour la sécurité de ce système qui ne sont pas identifiées ;
- les systèmes d'exploitation sont rarement inclus par les études de marché dans les logiciels de sécurité. Pourtant un système d'exploitation évolué inclut pourtant toujours de nombreux mécanismes de sécurité et ces mécanismes sont souvent le socle de la SSI ;
- les prochaines générations de microprocesseurs doivent intégrer de nombreuses fonctions de sécurité – chiffrement, vérification de l'intégrité et l'authenticité de codes exécutables, vérification de DRM[97]. Ils ne sont pas habituellement inclus dans le marché de la SSI ;

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

- certains logiciels permettant la virtualisation de matériels ne sont devenus des logiciels de sécurité que depuis que leur utilisation est envisagée pour réaliser des fonctionnements multi niveaux.

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

3.1.1 La segmentation du marché de la SSI

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

- **Des besoins multiples à satisfaire**

Selon une étude Ernst&Young[98] réalisée auprès de 1 230 entreprises, grandes et moyennes, dans 51 pays dont 50 en France, l'origine des besoins et donc **de la demande** apparaît multiple : exigence commerciale de continuité de service, obligations légales ou réglementaires, préoccupations d'image et protection du patrimoine de l'entreprise par rapport aux concurrents. Les besoins d'un Etat relèvent d'exigences de souveraineté et de sécurité des biens et des personnes.

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

- **Des clients aux exigences diversifiées**

La demande en sécurité des systèmes d'information vient du secteur institutionnel et gouvernemental, des entreprises et du grand public.

Le secteur institutionnel et gouvernemental se distingue par des exigences réglementaires voire légales, la nécessité pour certains ministères de prendre en compte la menace stratégique, des conditions de contractualisation complexes et lentes et des budgets contraints.

Les entreprises se distinguent par une sensibilité à la sécurité et des moyens extrêmement variables, des politiques d'achat sous contraintes de prix et de pérennité, de standardisation des produits achetés, et des exigences réglementaires de source nationale ou européenne (notamment les banques).

Le grand public se distingue par un système d'information souvent limité à une ou à quelques machines, un niveau technique très variable et une connaissance de la sécurité souvent limitée aux virus et aux Spams.

- **Les technologies de sécurité**

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

Les technologies essentielles de la sécurité des systèmes d'information sont par exemple:

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

- *les systèmes d'exploitation ;*
- *la conception d'architectures de sécurité, l'ingénierie logicielle sûre, la preuve logicielle, la preuve de protocoles et les méthodes d'évaluation associées ;*
- *la cryptographie, pour fournir des mécanismes de confidentialité, intégrité, preuve et authentification ;*
- *les dispositifs électroniques de protection de secrets (cartes à puces,...) ;*
- *les méthodes applicatives de filtrage (anti spam, anti-virus,...), de modélisation du comportement et de détection d'intention (intrusions,...) ;*
- *le matériel avec des composants et circuits intégrés sécurisés.*

Il existe une gamme de produits et technologies pour répondre aux différents besoins de sécurité. Ils ne constituent pas des alternatives, mais doivent être utilisés de façon combinée pour assurer la protection requise. Les technologies de base sont :

- *identification/authentification par mot de passe (à usage unique ou pas), biométrie, carte à puce ou clé USB, combinaison de ces technologies ;*
- *signature électronique ;*
- *chiffrement ;*
- *effacement sûr ;*

Ces solutions sont mises en œuvre dans différents types de produits de sécurité :

- *sécurité des réseaux : VPN (Virtual Private Networks, en français Réseaux Privés Virtuels), matériel/logiciel de chiffrement de liaison (standardisé ou non) ;*
- *sécurité du poste de travail : FireWall logiciels et/ou matériels, AntiSpam, Antivirus, Contrôle parental ;*
- *sécurité des contenus : logiciel de chiffrement de fichier (standardisé ou non), Digital Right Management (DRM) pour le multimédia ;*
- *contrôle d'accès : cartes à puce et terminal associé, capteur biométrique ;*
- *Trusted Platform Module (TPM).*

En complément des produits, il est nécessaire de prendre en compte les services de sécurité qui accompagnent la mise en œuvre de ces produits. Aux services traditionnels (gestion des clés et autres services de certification) se sont ajoutés des services plus commerciaux (conseil, audit, exploitation de la sécurité des réseaux). Comme dans le reste des TIC, ils constituent une activité en croissance plus forte que celle des équipements et plus difficilement délocalisable :

- *infrastructure de gestion de clés (IGC) ;*
- *services de certification électronique (horodatage...) ;*
- *processus d'évaluation et de certification ;*
- *single Sign On et Fédération d'identité ;*
- *conseil en SSI (audit, recommandation, formation) ;*
- *management et surveillance des réseaux.*

Parmi ces technologies et produits certains sont critiques pour la garantie d'un haut niveau de sécurité et devraient être de source française ou européenne, par exemple : des composants cryptologiques, des systèmes d'exploitation multi-niveaux, des processeurs de confiance, des dispositifs de gestion de clés, les PKI,....
En outre, il conviendrait d'initier des études complémentaires visant à élargir les possibilités offertes par les logiciels libres (par exemple les systèmes d'exploitation).

3.1.2 Le marché de la sécurité est en forte croissance

Selon l'enquête IDC Sécurité 2005[99], les dépenses informatiques globales sur le marché professionnel en **France** devraient atteindre en 2005, 41 009 M€, en croissance de 3,5%.

Les dépenses de **sécurité informatique,** des entreprises et des administrations atteindraient **1 113 M€, en hausse de 17,4%** (contre 15,4% de hausse entre 2004 et 2003). Parmi ces dépenses de sécurité informatiques en 2005 :

- les services représentent 612 M€ (55%) en hausse de 15,5% ;
- les logiciels représentent 405 M€ (36,4%) en hausse de 16,4% ;
- les appliances (boîtiers physiques intégrant de une à plusieurs fonctionnalités : pare-feu/VPN, anti-virus, anti-spam, prévention et détection d'intrusion,...(Cf. Annexe 12 pour les définitions) représentent 96 M€ (8,6%) en hausse de 37,1%.

Un taux de croissance moyen **de 17,2% est attendu pour le marché de la SSI** sur la période 2005 – 2009 pour atteindre 2 100 M€ (administrations et entreprises).

- **Pour les services**, le taux de croissance annuel devrait atteindre **19% en 2009 ;**
- **Pour les logiciels**, il est prévu une baisse du taux de croissance à partir de 2007 qui ne serait plus que de 12,3% en 2009.

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

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

Concernant les matériels, la croissance est réelle sur certains produits :

- **les cartes à puce**, dont le taux de croissance en volume[100] attendu sur 2005 est de 18% avec 1 727 millions d'unité après une croissance de 12% en 2004;
- les **systèmes biométriques**, qui devraient représenter environ 1 Md$ au niveau mondial en 2007.

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

[100] Source Les Echos / Eurosmart

3.1.3 Caractéristiques de quelques marchés logiciels et matériels de SSI

Selon IDC 2005[101]

Segment	Croissance du marché/an (2004-2009)	Marché national (M€) en 2004	Principaux acteurs	Présence française	Produit logiciel libre public	Criticité des produits
Logiciels : Anti–virus, Anti-spam et Spyware (segment SCM[102])	16%	157	Symantec, Network Associates (MC Afee), Trend, Sophos ...	Non	Oui, ClamAV	Non
Pares – feu / VPN (appliances)	2%	47	Check Point, Cisco,...	PME	Oui, netfilter, IP filter	Oui
Pares-feu (logiciels)	5%	44				Oui
Prévention et détection d'intrusion (appliances)	22%	11	Symantec et Internet Security Services (50% du marché à 2)	PME	Oui, Snort	Oui
Administration sûre (3A)[103]	13%	88	IBM, Computer Associates, Verisign,...	GE[104] et PME		Oui

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

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

En France, les fournisseurs de produits ou services en SSI sont :

- de grands groupes, certains liés au marché de l'armement : Thalès, Safran, EADS, Bull, France Télécom ;
- des SSII ;
- des industriels du marché de la carte à puce ;
- une centaine de petites et moyennes entreprises, souvent à forte valeur technologique.

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

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

[102] Secure Content Management – Cf. annexe 12

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

[104] GE: Grande Entreprise

Le classement IDC 2003[105], selon le **chiffre d'affaires** réalisé en Europe en 2003, uniquement dans le **domaine des logiciels liés à la SSI,** montre que les leaders sont américains avec Symantec (405 M$ de CA et 16% de parts de marché), Computer Associates (EU[106]), Check point (Israël-EU), Network Associates (EU), IBM (EU), Trend micro (EU), Sophos (RU[107]), Verisign (EU), Panda (EU), Microsoft (EU).

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

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

- **Les marchés de la carte à puce en 2005**[108]

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

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

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

3.1.5 Caractéristiques de quelques segments du marché des services de sécurité informatique

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

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

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

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

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

- **Infogérance de la sécurité**

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

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

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

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

Les ICP sont l'ensemble des moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer avec des systèmes cryptographiques asymétriques (Cf. Annexe 3 – glossaire pour les définitions) un environnement sécurisé aux échanges.

Certaines entreprises ou organisations choisissent de se doter de leur propre infrastructure ICP (en anglais PKI[109]) et de l'exploiter en interne. Mais beaucoup préfèrent recourir à des services externes délivrés par des sociétés spécialisées. Ainsi sont apparus des Opérateurs de Services de Confiance qui opèrent une ICP multi clients et peuvent fournir une multitude de services associés : gestion du cycle de vie des certificats, horodatage, coffre fort électronique, personnalisation de cartes à puces pour porter les certificats. Des offres nationales de qualité existent.

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

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

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

3.1.6.1 Les objectifs de ces initiatives

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

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

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

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

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

Les menaces possibles

Pour certains, ces limitations d'usage sont justifiées par le développement du commerce électronique et la gestion sûre des droits de propriété intellectuelle des œuvres numériques. L'industrie des médias et des services la réclame. Mais en restreignant les droits de l'utilisateur, NGSCB donne **un droit de regard aux constructeurs de matériels et de logiciels, de l'usage fait des ordinateurs personnels.** Il permet de contrôler l'accès des logiciels aux ressources matérielles.

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

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

3.1.7 Synthèse sur l'offre et le marché de la SSI

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

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

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

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

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

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

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

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

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

De plus, un niveau de sensibilisation inférieur devant nos partenaires européens et une certaine résignation face aux Américains, voire aux Asiatiques, suite à notre incapacité à

fédérer une industrie informatique européenne font que les grands acteurs sont peu nombreux.

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

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

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

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

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

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

- **L'offre nationale et européenne éclatée : de nécessaires rapprochements**

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

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

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

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

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

En ce qui concerne l'Etat :

- ANR : la sécurité est un des thèmes des RRIT (Réseaux de recherche et d'innovation en technologie) communs aux ministères de l'industrie et de la recherche, notamment ceux sur les télécommunications (RNRT) et le logiciel (RNTL). Dans les appels à projets 2005 de l'ANR, la sécurité a été traitée dans le RNRT, mais fait également l'objet avec les mémoires de masse, d'une thématique additionnelle dotée de 10M€. Entre 5 et 10 projets devraient être retenus pour un montant de 4 à 8 M€. Entre l'ensemble des dispositifs du ministère de la recherche, environ 23M€ entre 2001 et 2004 ont été consacrés au thème SSI[110].

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

- MINEFI :

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

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

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

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

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

[110] Source Ministère de la Recherche

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

En ce qui concerne la Commission européenne :

Le 6è PCRD comporte des programmes dans le thème « technologies de la société de l'information » qui est doté d'un budget de 4 milliards d'euros environ[111]. De plus la Commission a lancé une action préparatoire, en vue du 7ème PCRD, dotée d'un budget prévisionnel de 65 millions d'euros pour la période 2004 – 2006, concernant la recherche de sécurité :

- 6è PCRD : la SSI est au cœur de différentes actions (environnement sécurisé, sûreté des réseaux électroniques pour les transports aériens et automobiles, management des risques,...) pour un montant évalué à environ 140 millions d'euros sur la période[112] ;
- action préparatoire : couvrant les domaines de la sécurité globale (protection des frontières, bioterrorisme, SSI, ...), les projets SSI ont concerné par exemple les communications sécurisées ou la protection des infrastructures critiques. Les montants affectés à la SSI n'ont pas été précisés ;
- 7è PCRD : le thème de la sécurité apparaît comme une priorité de ce plan qui dépendra cependant des résultats de l'action préparatoire sur les actions à lancer. Le budget envisagé est de **1 milliard d'euros**.

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

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

Des industriels et des centres de recherche français[113] ont engagé des réflexions sur la mise au point de produits de confiance, par exemple :

- aujourd'hui, la maîtrise de la partie logicielle des produits ne permet pas de garantir la sécurité si le hardware sur lequel elle s'exécute n'est pas maîtrisé. Il est donc nécessaire de lancer des programmes technologiques pour mettre au point des circuits intégrés sécurisés ;
- le lancement d'un projet **structurant** dans les usages et la gestion sécurisée de l'identité, avec comme enjeu l'intégration du citoyen et la préservation de ses droits (individu numérique).

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

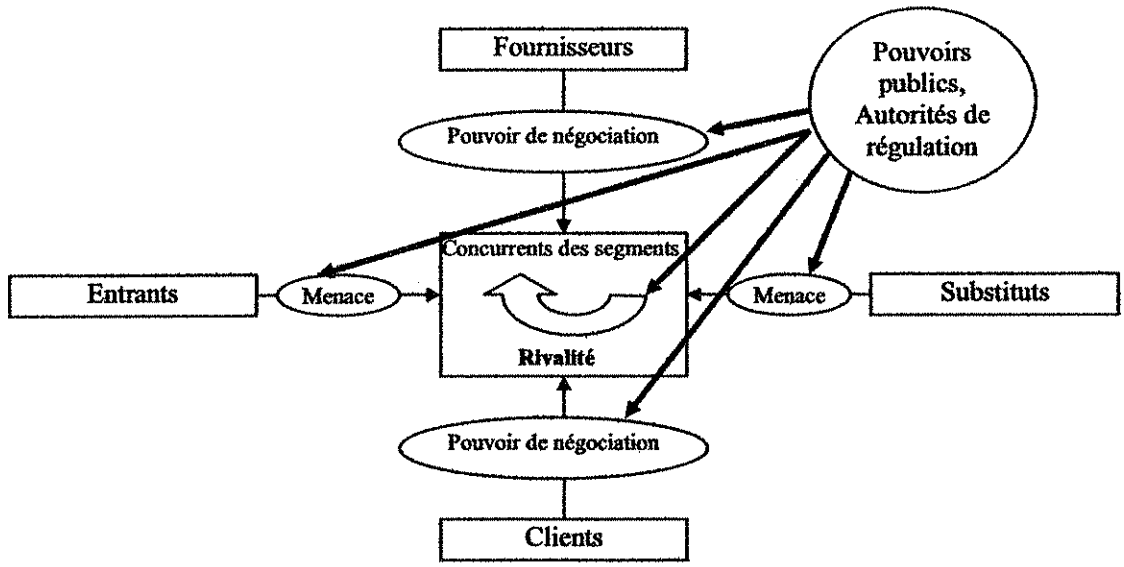
3.2.2 La situation des PME fournisseurs de produits et services SSI est très critique

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

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

3.2.2.1 Un marché de la SSI particulièrement difficile pour les PME françaises

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



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

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

- **Pouvoir de négociation des fournisseurs**

Les PME prestataires de services en SSI, sont amenées parfois à intégrer des produits provenant d'acteurs de taille plus importante, en situation de quasi-monopole, ce qui les place en situation de faiblesse à l'achat. Ces entreprises se trouvent de facto fortement dépendantes. Le problème disparaît pour des PME qui développent des produits.

L'Etat **doit favoriser l'existence et le développement d'offres alternatives pour contrebalancer ce déséquilibre** en particulier par une politique incitative de financement de développement de produits et de technologies, et une politique d'achat appropriée.

- **Pouvoir de négociation des clients**

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

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

- **Rivalité entre les concurrents**

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

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

Près de 900[114] entreprises technologiques dans le monde interviennent dans la SSI, dont 70% sont d'origine américaine. Leur chiffre d'affaires ne dépasse pas en général 30 M$. Le marché est donc surtout composé de nombreuses petites sociétés et de quelques grandes entreprises.

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

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

- **Difficultés pour les nouveaux entrants**

Les barrières à l'entrée pour les PME **sont fortes** sur ce secteur en raison :
- de l'expérience forte des teneurs du marché ;
- des besoins importants en capitaux pour un secteur où les stratégies sont mondiales ;
- de l'accès compliqué aux circuits de distribution pour les PME ;
- des avantages spécifiques (brevets,...) détenus par les leaders présents ;
- de l'insuffisance de l'appui par les pouvoirs publics de l'offre européenne.

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

- **La menace des produits substituables**

Elle est soutenue sur ces secteurs compte tenu d'une **évolution permanente des technologies** consécutives à l'évolution des besoins. Par exemple, l'avancée de l'Ipv6 et de la post 3G aura des conséquences fortes sur le tissu national spécialisé dans les TIC et donc sur celui spécialisé en SSI.

[114] Source auditions

Pour y répondre, un effort intense et continu de R&D est nécessaire, en particulier au sein des PME innovantes. Un effet de levier important par le financement public national et européen est naturellement indispensable et doit être accentué. Mais sans un **accroissement significatif des financements privés, notamment des grands donneurs d'ordres**, les montants consacrés seront insuffisants pour rester au meilleur niveau.

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

Les pouvoirs publics et les autorités de régulation influent directement sur le marché. Ainsi, peuvent-ils faire jouer leur influence sur les pouvoirs de négociation des fournisseurs et des clients (réglementations en matière de délai de paiements, ou de sous-traitance obligatoire à des PME dans le cadre de contrats publics,...), sur les menaces des nouveaux entrants (autorisations d'exercer notamment dans la SSI, existence de normes spécifiques,...). L'Union européenne peut également intervenir, en particulier dans le financement de la R&D et en matière réglementaire (textes pro-PME, normalisation favorable à l'offre issue de l'Union européenne,...) pour favoriser l'environnement de ces PME SSI.

L'Etat doit prendre conscience de son rôle moteur indispensable dans ce domaine particulier qu'est la SSI. **Son rôle ne doit pas se limiter à une politique de financement et d'incitations fiscales.**

3.2.2.2 Contraintes complémentaires issues de l'environnement

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

- **Marché européen fragmenté et souverainetés nationales**

Contrairement aux Etats-Unis qui dispose d'un marché de la SSI unique et important en volume, celui de l'Europe est fragmenté. Chaque pays, pour des questions de souveraineté, privilégie des solutions nationales, quand elles existent.

On observe que le marché accessible à une PME étant restreint, son potentiel de développement limité, ce qui la rend peu attractive pour des investisseurs.

Favoriser une offre européenne apte à vendre aux Etats et aux grands donneurs d'ordres européens sans barrières spécifiques **doit être un objectif de l'Etat** français en coopération avec ses partenaires européens les plus proches sur les questions de SSI.

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

L'absence de leaders mondiaux sur le territoire national et européen entraîne un manque de stimulation pour toute la chaîne de fournisseurs et pour l'environnement de recherche. Ainsi, nos entreprises et nos laboratoires se trouvent-ils éloignés de ceux qui ont une vision claire de leurs marchés et de ses évolutions à venir. Ils auront de ce fait un temps de retard par rapport à des PME et laboratoires installés à proximité des grands donneurs d'ordres américains.

- **Montée en puissance de l'Asie**

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

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

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

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

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

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

Le gouvernement a certes pris quelques mesures :

- action auprès des partenaires européens pour une renégociation du traité OMC et de la législation européenne ;
- installation d'un observatoire de la commande publique le 15 novembre 2005 ;
- lancement d'une concertation pour optimiser la passation des appels d'offres à des PME ;
- **pacte PME** proposé par le Comité Richelieu en association avec OSEO-Anvar, dont l'objectif est de faciliter les relations entre les grands comptes et les PME innovantes.

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

Les ministères devraient mener une politique d'achat en cohérence avec leurs axes stratégiques, notamment en matière de sécurité nationale. Il est intéressant de citer la politique d'acquisition du ministère de la Défense, fondée sur un principe **d'autonomie compétitive** qui s'articule autour de deux objectifs complémentaires :

- garantir la meilleure efficacité économique des investissements réalisés pour satisfaire les besoins des forces armées ;
- assurer un accès aux capacités industrielles et technologiques qui conditionnent la satisfaction **à long terme** des besoins des forces armées.

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

Il est à noter à cet effet que le PRSSI[115] recommandait dans sa mesure I1:

« de garantir une diversité d'approvisionnement en produits de sécurité en stimulant le développement de produits industriels innovants et répondant à des besoins identifiés, en s'adressant à un tissu d'industriels de confiance notamment de PME. »

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

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

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

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

Les critères de sélection des grandes entreprises n'intègrent pas suffisamment le caractère innovant des PME, facteur d'innovation pour leurs propres produits, et les enjeux de sécurité que représente une offre européenne viable sur le long terme. La résistance des acheteurs à l'innovation semble réelle et presque de nature culturelle. A cela s'ajoute les grandes entreprises qui cherchent à diminuer fortement le nombre de leurs interlocuteurs et à faire partager les risques de développement à leurs sous-traitants. Ces objectifs sont des freins de plus en plus importantes pour les PME.

A l'exception du **Pacte PME**, il n'y a pas de réelles dynamiques de la part des grands donneurs d'ordres. Une politique d'achat à des entreprises françaises ou européennes de confiance peut être effective sans nécessairement entraîner un surcoût mais sous réserve d'une **volonté forte de changement** des grands donneurs d'ordres.

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

- **Le financement**

L'accès aux ressources financières est naturellement un point essentiel et recouvre : les fonds propres, les crédits bancaires, le financement de projet ou à l'exportation[116] et la transmission / cession [117].

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

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

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

[116] Financement projet : difficile compte tenu de la pression des donneurs d'ordres pour partager le risque avec les sous-traitants. Un effet de levier serait nécessaire. Le financement de l'exportation : il n'existe pas à ce jour de réponse efficace en termes de cautions bancaires.

[117] nécessite une attention particulière afin de favoriser des solutions européennes permettant progressivement l'émergence de PME de plus grande taille, aptes à intervenir au niveau mondial

- incitation auprès des assureurs français à investir 6 G€ dans les PME ;
- politique en matière d'amorçage et d'incubation qui a le mérite d'exister même si, pour l'instant, les résultats ne sont pas toujours très positifs ;
- concours création d'entreprises du ministère de la Recherche, renforcement d'Oséo.

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

En effet, la tendance du marché du capital d'investissement se caractérise par :
- une prédominance des opérations de LBO[119] ;
- une faiblesse structurelle des fonds de capital risque à lever des fonds ;
- une orientation croissante des FCPI vers le marché coté.

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

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

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

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

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

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

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

Les PME des secteurs technologiques et notamment des TIC, sont confrontées à une **évolution en ciseau** avec, d'une part, une très forte croissance des besoins de financement

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

de la R&D et, d'autre part, un plafonnement des ressources traditionnelles que sont les financements gouvernementaux et des grandes entreprises européennes continentales.

En effet, pour être en mesure de suivre l'évolution technologique permanente de ces marchés, les entreprises doivent consacrer en moyenne jusqu'à 15% de leur CA en R&D. Or, la **France et ses entreprises ne sont pas suffisamment actives dans le domaine des TIC**[120] :

- en 2003, le financement de la R&D en TIC était de 90 $ par habitant en France, contre 220-240 $ aux Etats-Unis ou au Japon ;
- la même année, l'effort de R&D global en TIC ramené au PIB était de 0,31 % en France, contre 0,65 % aux Etats-Unis et 0,76 % au Japon. Pour l'effort de R&D des entreprises, les ratios sont similaires ;
- l'effet de levier de la dépense publique en TIC sur les entreprises, c'est-à-dire le ratio entre la R&D exécutée par les entreprises et les fonds publics qui y sont consacrés, est très nettement inférieur en Europe (5,2) qu'aux Etats-Unis (7,1), la **France étant encore en retrait avec 4,3**, loin derrière des pays où le ratio se situe entre 10 et 12 (Canada, Corée, Finlande et Suède notamment).

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

Des mesures gouvernementales de nature générale ou sectorielle ont ainsi été prises :

- renforcement du crédit impôt recherche[121] ;
- augmentation des moyens financiers d'Oséo annoncée en juillet 2005 ;
- accès des PME aux projets financés par l'Agence de l'Innovation Industrielle (mais il n'y a pas de part réservée aux PME), ainsi qu'à ceux de la Commission (les PME n'ont pas toujours les moyens et le temps à consacrer aux réponses aux appels à projets) ;
- accès aux programmes de développement de la DGA (PEA[122],...) ;
- Programmes sectoriels avec :
  - Oppidum (Minefi) ;
  - Abondement par la DCSSI ou la DGA d'avances remboursables accordées par Oséo Anvar à des projets les intéressant (SSI, technologies duales,...) pour des montants trop faibles.

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

- **Des ressources humaines qualifiées insuffisantes**

Les PME françaises ne disposent pas toujours des compétences nécessaires pour attirer des investisseurs et rassurer les clients, alors qu'il s'agit d'un critère essentiel. **Aujourd'hui la question n'est pas tant de savoir si de bons projets sont développés ou non, en France, mais plutôt, si de bonnes équipes existent** pour les exécuter.

A l'exception d'Oseo Anvar qui propose un dispositif spécifique de prise en charge d'une partie des charges liées à l'emploi de chercheurs, il n'y a pas à ce jour de mesures

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

particulières pour favoriser le recrutement de compétences par des PME, notamment en marketing des technologies[123], alors que les freins au recrutement sont déjà forts.

En outre, **le vieillissement général** des dirigeants en France entraînera des conséquences qui ne peuvent être ignorées. En l'absence de solutions facilitant les transmissions, les solutions de reprise par des fonds d'investissement s'imposeront. Aussi, progressivement, le capital des PME françaises sera-t-il de plus en plus maîtrisé par des fonds disposant des capitaux nécessaires, aujourd'hui principalement anglo-saxons.

- **Un environnement juridique et fiscal perfectible**

L'environnement français est peu attractif. Certaines mesures fiscales récentes vont toutefois dans le bon sens :

- évolutions favorables en matière d'ISF ;
- création du statut de JEI (Jeune Entreprise Innovante) intégrant des exonérations de charges sociales et d'impôts (même si le rachat d'une JEI par une JEI a pu aboutir à des redressements fiscaux)[124] ;
- création du statut de SUIR (Société Unipersonnelle d'Investissement à Risque).

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

3.2.3 Les centres de recherche orientés sur la SSI insuffisamment présents

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

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

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

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

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

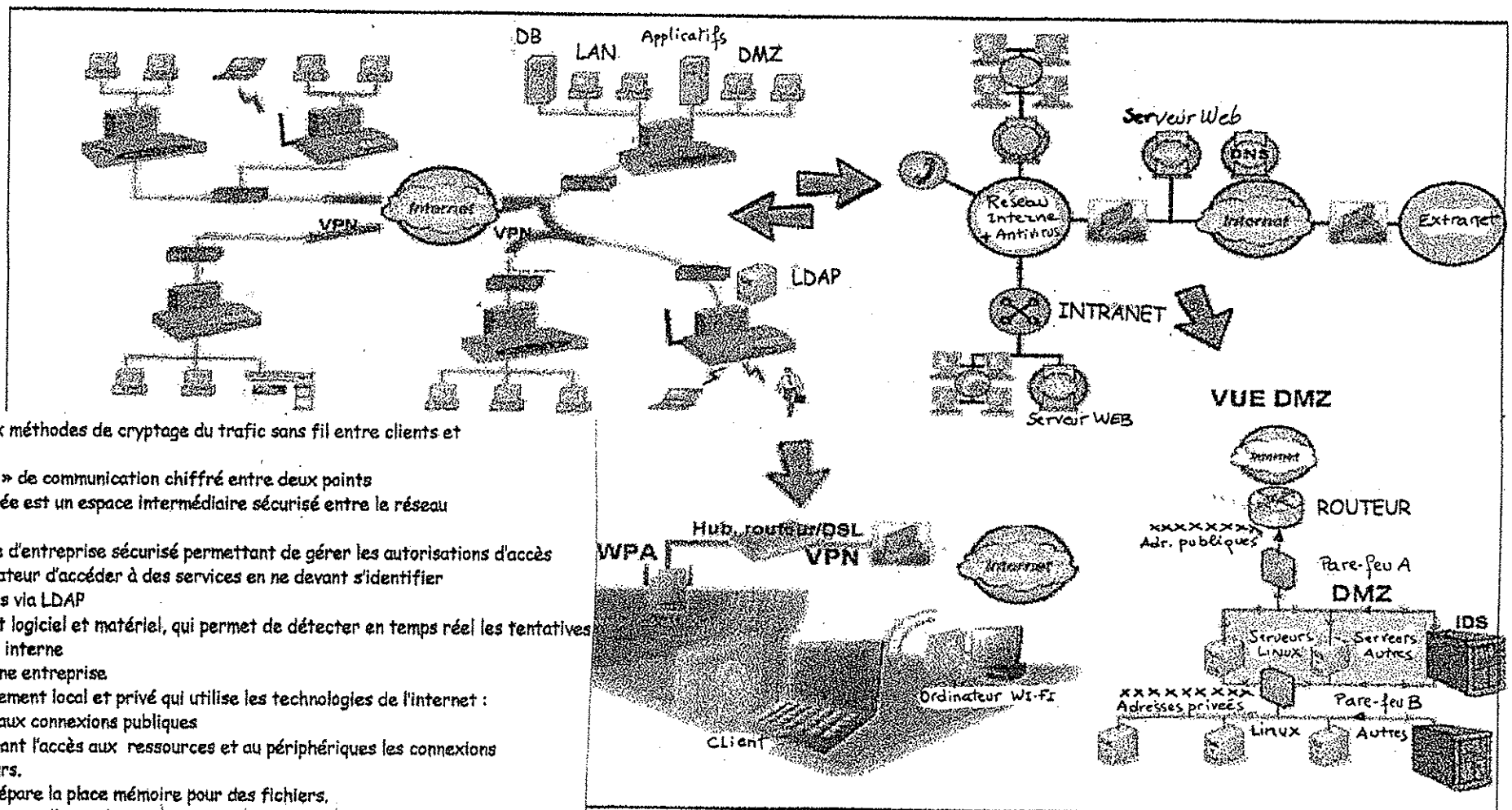
[123] Source auditions
[124] Source auditions

ANNEXE 1

Organismes

- ADAE : Agence pour le Développement de l'Administration Electronique ;
- BRCI : Brigade Centrale de la Répression de la Criminalité Informatique ;
- CCSDN : Commission Consultative du Secret de la Défense Nationale ;
- CEMA : Chef d'Etat Major des Armées ;
- CEMAA : Chef d'Etat Major de l'Armée de l'Air ;
- CEMAT : Chef d'Etat Major de l'Armée de Terre ;
- CMM : Chef d'Etat Major de la Marine ;
- CERT-RENATER : centre d'alerte et de réponse aux attaques informatiques dédié aux membres de la communauté GIP-RENATER – REseau National de télécommunication pour la Technologie, l'Enseignement et la Recherche ;
- CERTA : Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatisées – relié au DCSSI ;
- CESTI : Centres d'Evaluation de la Sécurité des Technologies de l'Information reconnus par la DCSSI ;
- CFSSI : Centre de formation à la Sécurité des Systèmes d'Information ;
- CIGREF : Club Informatique des Grandes Entreprises Françaises ;
- CIRT- IST : CERT privé réalisé par Alcatel, le CNES, Total et France Télécom ;
- CISI : Comité Interministériel pour la Société de l'Information ;
- CISSI :Commission Interministérielle pour la Sécurité des Systèmes d'Information
- CLUSIF : Club de la Sécurité Informatique des systèmes d'information Français ;
- CNIL : Commission Nationale Informatique et Libertés ;
- CNIS : Commission Nationale de Contrôle des Interceptions de Sécurité ;
- COSSI : Centre Opérationnel de la Sécurité des Systèmes d'Information
- DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information ;
- DGA : Délégation Générale pour l'Armement ;
- DGGN : Direction Générale de la Gendarmerie Nationale ;
- DGSE : Direction Générale de la Sécurité Extérieure ;
- DPSD : Direction de la Protection et de la Sécurité de la Défense ;
- DST : Direction de la Surveillance du Territoire ;
- DSTI : Direction des Systèmes terrestres et d'Information ;
- INHES : Institut National des Hautes Etudes de Sécurité (ex IHESI) ;
- INPS : Institut National de Police Scientifique ;
- OCLCTIC : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication ;
- OPVAR : Organisation permanente de veille alerte réponse ;
- OSSIR : Observatoire de la Sécurité des Systèmes d'Information & des Réseaux ;
- PAGSI : Programme d'Action Gouvernemental pour l'entrée de la France dans la Société de l'Information ;
- RECIF : Recherches et Etudes sur la Criminalité Informatique Française ;
- STSI : Service des Technologies et de la Société de l'information (Minefi/DGE) ;
- SEFTI : Service d'Enquête des Fraudes aux Technologies de l'Information;
- SGA : Secrétariat Général pour l'Administration ;
- SGDN : Secrétariat Général de la Défense Nationale.

- Schéma de principe des systèmes d'information



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

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

DMZ ou zone démilitarisée est un espace intermédiaire sécurisé entre le réseau extérieur et intérieur

Serveur LDAP : annuaire d'entreprise sécurisé permettant de gérer les autorisations d'accès

SSO : permet à un utilisateur d'accéder à des services en ne devant s'identifier q'une seule et unique fois via LDAP

IDS : système combinant logiciel et matériel, qui permet de détecter en temps réel les tentatives d'intrusion sur un réseau interne

LAN : réseau interne d'une entreprise

Extranet : réseau strictement local et privé qui utilise les technologies de l'internet : web, e-mail, non ouvert aux connexions publiques

Serveur : ordinateur gérant l'accès aux ressources et au périphériques les connexions des différents utilisateurs.

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

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

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

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

ANNEXE 3

– Sensibilité de l'information : exemples de la DCSSI et de l'AFNOR

Classifier l'information

La recommandation N°901 de la DCSSI s'attache quant à elle à distinguer 2 niveaux d'informations pour tout ce qui concerne les informations non classifiées défense :

- les informations sensibles, qui englobe tous les documents dont la consultation ou la communication mettrait en cause la responsabilité pénale du propriétaire ou du dépositaire, ou causerait un préjudice à eux-mêmes ou à des tiers matérialisé par :
  - les informations énumérées à l'article 6 de la loi n° 78-753 du 17 juillet 1978, modifiée par la loi 2000-321 du 12 avril 2000 ;
  - les informations qui ne présentent pas un caractère de secret, mais qui restent soumises à l'obligation de réserve ou de discrétion professionnelle ;.
  - les informations constitutives du patrimoine scientifique, industriel et technologique.

- les informations vitales pour le fonctionnement d'un système.
Le traitement des données par un système nécessite la mise en œuvre d'une suite d'actions élémentaires internes dont l'association assure les fonctionnalités du système d'information. Ainsi un site Internet est un ensemble de documents (fichiers .php, fichiers .sql qui sont interprétés par le serveur ou le navigateur et permettent d'afficher une page web). L'accès à certains de ces documents mal protégés (droits étendus sur un fichier config.php par exemple) permet d'obtenir rapidement un contrôle total sur un site internet.

La classification des informations selon l'AFNOR

Les informations sont le plus souvent consignées dans des documents papier ou numérisés. Toutefois, des objets (maquettes, prototypes, machines,...), des installations, des procédés, des techniques, des méthodes commerciales, des organisations, des projets de publicité, le savoir-faire de l'entreprise, etc., sont d'autant d'indications qui constituent des informations.

Aussi, une démarche de protection de l'information commencera par l'identification des informations, quelque soit leur forme, dont la confidentialité doit être protégée, en raison :

- Des avantages que leur divulgation procurerait à la concurrence ou aux partenaires ;
- Des exigences légales et réglementaires encadrant ces informations.

C'est aussi l'analyse de risques qui permet de déterminer le nombre de niveaux de protection nécessaire à chaque structure.

Exemple de système de classification des informations :

Niveau	3 : secret	2 :confidentiel	1 :diffusion contrôlée
Préjudice potentiel	Préjudice inacceptable Séquelles très graves et durables	Préjudice grave Séquelles compromettant l'action à court et moyen terme	Préjudice faible Perturbations ponctuelles
Risques tolérés	Aucun risque même résiduel n'est acceptable	Des risques très limités peuvent être pris	Des risques sont pris en connaissance de cause
Protection	Recherche d'une protection maximale	Prise en compte de la notion de probabilité d'occurrence	La fréquence et le coût du préjudice potentiel déterminent les mesures prises

Recommandations :

Une attente particulière est apportée aux possibilités de compilation ou de croisement des données. En effet, la consolidation de données, à priori peu sensibles lorsqu'elles sont prises séparément, peut constituer une information confidentielle.

Afin d'assurer un niveau de protection homogène et juste nécessaire –ni trop, ni pas assez – il est recommandé de désigner explicitement les personnes responsables de la classification des informations (*), de leur fournir un vade-mecum pour les aider dans cette mission et d'actualiser régulièrement ce document.

(*) L'attribution de cette responsabilité variera suivant la taille de l'entreprise, son organisation, l'origine, la forme ou la finalité des informations, etc. Par exemple, dans des structures de taille importante, un responsable dans chaque secteur d'activité peut être en charge de la classification et de l'application des mesures de protection, dans d'autres chaque personne à l'origine d'une information est responsable de sa protection.

ANNEXE 4

– Les 12 clés de la sécurité selon l'AFNOR

D'après le Référentiel de bonnes pratiques de l'AFNOR - Août 2002
Sécurité des Informations Stratégiques – Qualité de la confiance
Comment préserver la confidentialité des informations

1. Admettre que toute entreprise possède des informations à protéger (plans de recherche, prototypes, plans marketing, stratégie commerciale, fichiers clients, contrats d'assurance,...) ;

2. Faire appel à l'ensemble des capacités de l'entreprise (chercheurs, logisticiens, gestionnaires de personnel, informaticiens, juristes, financiers,...) pour réaliser l'inventaire des informations sensibles, des points faibles, des risques encourus et de leurs conséquences ;

3. Exploiter l'information ouverte sur l'environnement dans lequel évolue l'entreprise, observer le comportement des concurrents, partenaires, prestataires de service, fournisseurs, pour identifier les menaces potentielles ;

4. S'appuyer sur un réseau de fournisseurs de confiance pour ceux d'entre eux qui partagent ou accèdent à des informations sensibles ;

5. Ne pas chercher à tout protéger : classifier les informations et les locaux en fonction des préjudices potentiels et des risques acceptables ;

6. Mettre en place les moyens de protection adéquats correspondant au niveau de sensibilité des informations ainsi classifiées, s'assurer qu'ils sont adaptés et, si besoin, recourir à des compétences et expertises extérieures ;

7. Désigner et former des personnes responsables de l'application des mesures de sécurité ;

8. Impliquer le personnel et les partenaires en les sensibilisant à la valeur des informations, en leur apprenant à les protéger et en leur inculquant un réflexe d'alerte en cas d'incident ;

9. Déployer un système d'enregistrement des dysfonctionnements (même mineurs), et analyser tous les incidents ;

10. Ne pas hésiter à porter plainte en cas d'agression ;

11. Imaginer le pire et élaborer des plans de crise, des fiches « réflexe » afin d'avoir un début de réponse au cas où... ;

12. Evaluer et gérer le dispositif, anticiper les évolutions (techniques, concurrentielles,...) et adapter la protection en conséquence en se conformant aux textes législatifs et réglementaires en vigueur.

ANNEXE 5

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

Les chartes d'utilisation des systèmes d'information, dont quelques points clés sont indiqués ci-après, se diffusent désormais de manière croissante dans les entreprises et au sein de l'Etat.

Quelques points clés :

- **Les objectifs de ces chartes :** définir les bonnes pratiques comportementales devant être respectées et qui relèvent :
  - du comportement loyal et responsable de chacun. La responsabilité individuelle est la base de la SSI ;
  - de règles déontologiques et de législations applicables ;
  - de règles principales de sécurité.

- **Bases juridiques des chartes :**
  - elles peuvent faire l'objet d'une consultation des Comités d'Entreprises (CE) et d'une déclaration auprès de la CNIL ;
  - elles peuvent engager, pour certaines, les salariés à des sanctions en cas d'usage abusif ;
  - elles sont annexées dans certains cas au contrat de travail ou au règlement intérieur de l'entreprise ;
  - dans certaines administrations, l'utilisateur peut être amené à signer une reconnaissance de responsabilité.

- **Quelques principes directeurs :**
  - Les chartes **s'appliquent à tous les utilisateurs quel que soit leur niveau hiérarchique** : dirigeants, salariés, intérimaires, stagiaires, consultants, prestataires,... ;
  - Les utilisateurs **doivent prendre connaissance** des règles qui sont définies dans les documents de politique de sécurité des entreprises destinés à garantir la bonne gestion ainsi que la sécurité des ressources informatiques et de communication ;
  - Un rappel de la **législation en vigueur** relative par exemple à la fraude informatique, aux atteintes à la personnalité et aux mineurs et les infractions à la propriété intellectuelle (copies illicites,...) est fourni avec les chartes. Les utilisateurs doivent en prendre connaissance et **s'engager** à user des ressources informatiques dans le respect de ces lois et réglementations ;
  - L'utilisateur **fait de la sécurité une priorité** et met en œuvre les règles pratiques de sécurité comme :
    - la protection de l'accès à son poste de travail et à ses données (mots de passe, mise en veille avec mot de passe,...) ;

[139] Sources auditions

- se protéger contre le vol ;
- éviter les doubles connexions Intranet-Internet ;
- une protection spécifique lors des déplacements notamment à l'étranger.

- Les ressources informatiques et de communication sont destinées à un **usage professionnel**. L'usage privé peut être toléré, s'il n'affecte pas la circulation normale de l'information ;

- Les utilisateurs s'engagent à **respecter la configuration** de leur poste de travail et à ne pas installer leurs propres logiciels ou matériels ;

- Les utilisateurs ont une **obligation de confidentialité** sur les informations stockées ou transmises au moyen des ressources informatiques qui lui sont affectée ;

- L'utilisateur doit faire preuve de **vigilance** vis-à-vis des informations recueillies sur Internet ou reçues par messagerie (possibilité de désinformation, s'assurer de l'émetteur,...) ;

- Chaque utilisateur doit être conscient que certains échanges avec des tiers **peuvent engager** l'entreprise (contractuellement éventuellement) ou porter atteinte à son image. Le respect des délégations de pouvoirs établies doit s'appliquer également.

- ...

Concours spécialité « ingénieur paysagiste D.P.L.G » :

Sujet commun pour les différents candidats.
Le choix du site est au choix du candidat.

Sujet 1 : Analyse d'un grand site touristique :

- justification de votre choix ;
- critères d'analyse ;
- propositions d'aménagement en vous appuyant sur des schémas.
-

Schémas sur papier A3 et feutres couleur
Durée de présentation : 15 mn

POLYNESIE FRANÇAISE

MINISTERE
DU DEVELOPPEMENT DURABLE,
DE L'AMENAGEMENT, DE L'ENVIRONNEMENT,
DE LA QUALITE DE LA VIE
chargé de la prévention des risques naturels
SERVICE DE L'URBANISME

PAPEETE, le 29 mai 2006

SUJETS DE L'EPREUVE D'ADMISSIBILITE DU CONCOURS DE RECRUTEMENT D'UN INGENIEUR RISQUES NATURELS

1. Les risques naturels en Polynésie : phénomènes en jeu et spécificités des différents archipels de Polynésie française, notamment concernant les enjeux et les risques encourus.
2. La problématique de l'aléa mouvements de terrain en Polynésie française
3. La problématique de l'aléa cyclonique en Polynésie française
4. Les tsunami en Polynésie française : origine des phénomènes, risques associés et prévention
5. Le réchauffement climatique : quelles conséquences pour la Polynésie française
6. Les particularités de la gestion des risques naturels en Polynésie par rapport à la France métropolitaine
7. Les Plans de Prévention des Risques Naturels Prévisibles en Polynésie française : relation avec la réglementation nationale, contenu, date d'instauration, articulation avec les PGA, objectifs recherchés, modalités de mises en œuvre et état d'avancement.
8. Aléas, risques, enjeux, vulnérabilité : définitions et illustrations propres à la Polynésie française
9. Les acteurs institutionnels de la gestion des risques naturels en Polynésie française
10. La prévention des risques naturels en Polynésie française : présenter les différents aspects des actions à conduire en matière de prévention des risques naturels ; faire la différence entre les actions de l'Etat et de la Polynésie.

SERVICE DE L'URBANISME * PIHA TORO'A FAANAHORAA FENUA *