

UNIVERSITE DES SCIENCES JURIDIQUES, POLITIQUES ET SOCIALES DE LILLE II

Année Universitaire 1999-2000

**MEMOIRE DE D.E.A.**

**DROIT MENTION « DEFENSE NATIONALE ET SECURITE EUROPEENNE »**

**DEUXIEME PRIX SCIENTIFIQUE DE L'IHEDN 2001 – CATEGORIE DEA**

SOUTENU PAR :

Alexander Walden

**Le Renseignement Humain**  
**Face au**  
**Développement des Nouvelles**  
**Technologies**

**Directeur : Monsieur le Professeur Gros**  
**Co-Directeur : Général Deconinck †**

## INTRODUCTION

### **PARTIE 1<sup>ERE</sup> – LES LIMITES A L’EFFICACITE DU « TOUT TECHNOLOGIQUE »**

#### TITRE 1- LES DIFFICULTES LIEES A LA MASSE D’INFORMATIONS OBTENUES TECHNIQUEMENT

##### CHAPITRE 1- LA MULTIPLICATION DES RENSEIGNEMENTS D’ORIGINE TECHNIQUE

###### SECTION 1- DES MOYENS DISCRETS ET VARIES

###### §1-LES DIFFERENTS TYPES DE RENSEIGNEMENT D’ORIGINE TECHNIQUE

###### §2- LES MOYENS DE L’ACQUISITION

###### Section 2- Les agences de renseignement technique

###### §1- LES ETATS-UNIS D’AMERIQUE

###### §2- LA FEDERATION DE RUSSIE

###### §3- LE ROYAUME-UNI

###### §4- LA FRANCE

##### CHAPITRE 2- LES DEFAILLANCES INHERENTES A LA RECHERCHE ET A L’EXPLOITATION DU RENSEIGNEMENT D’ORIGINE TECHNIQUE

###### SECTION 1- LES MOYENS DE DISSIMULATION DE L’INFORMATION

###### §1- LE CAMOUFLAGE

###### §2- LA CRYPTOGRAPHIE

###### SECTION 2- LE MANQUE D’EXPLOITATION ET DE VALORISATION DES DONNEES

###### §1- LE MANQUE D’EXPLOITATION DES INFORMATIONS

###### §2- LA VALEUR A DONNER AU RENSEIGNEMENT

###### SECTION 3- LES RATES DES PUISSANTES CENTRALES OCCIDENTALES

###### §1- LES ESSAIS NUCLEAIRES INDIENS

###### §2- LA FUSEE NORD-COREENNE

###### §3- ECHELON OU L’ECHEC ANNONCE D’UN PROGRAMME TROP AMBITIEUX

### **TITRE 2- LA QUESTION DES ATTEINTES AUX LIBERTES PUBLIQUES DANS LES DEMOCRATIES**

#### Chapitre 1- La nature des libertés menacées

##### SECTION 1- LES ATTEINTES A LA PERSONNALITE

###### §1- LE DROIT A L’IMAGE ET A LA VOIX

###### §2- LE CAS DES ECOUTES TELEPHONIQUES EN FRANCE

##### SECTION 2 – LES QUESTIONS RELATIVES AUX DONNEES NOMINATIVES

###### §1- DEFINITION

§2- LA CONSTITUTION DE FICHIERS

SECTION 3- LES INTRUSIONS DANS LES SYSTEMES INFORMATIQUES

§1- LES PIRATES INFORMATIQUES

§2- LES PROTECTIONS CONTRE LES ATTAQUES INFORMATIQUES

CHAPITRE 2- L'ACCENTUATION DU CONTROLE DEMOCRATIQUE DES SERVICES SPECIAUX

SECTION 1- L'ETENDUE DU CONTROLE DANS LES PRINCIPALES DEMOCRATIES

§1- L'APPLICATION D'UN STRICTE CONTROLE AUX ETATS-UNIS

§2- LA REVOLUTION BRITANNIQUE

§3- LE FAIBLE CONTROLE DU PARLEMENT AU CANADA

SECTION 2- VERS UNE ACCENTUATION DES CONTROLES DES ACTIVITES DE  
RENSEIGNEMENT EN FRANCE

§1- LES COMMISSIONS DE CONTROLE RELATIVES AU RENSEIGNEMENT TECHNIQUE

§2- L'INEXISTENCE D'UN VERITABLE CONTROLE PARLEMENTAIRE EN FRANCE

\*\*\*\*\*

**PARTIE 2<sup>EME</sup> – LA NECESSAIRE PRESENCE DE L'HOMME DANS LE CYCLE DU RENSEIGNEMENT**

TITRE 1<sup>ER</sup> - UNE MEILLEURE APPROCHE DES ACTIVITES DE RENSEIGNEMENT

CHAPITRE 1- LA REDEFINITION DES OBJECTIFS

Section 1- Les récents bouleversements géopolitiques

§1- L'APPARITION D'UNE NOTION NOUVELLE : LA GUERRE ECONOMIQUE

§2- LES RISQUES EMERGENTS EN MATIERE DE SECURITE

Section 2- La nécessaire construction d'une culture du renseignement

§1- UNE CULTURE ACQUISE DANS DE NOMBREUX PAYS

§2- VERS UN CHANGEMENT DE LA MENTALITE FRANÇAISE

CHAPITRE 2- L'IMPORTANCE DE LA COORDINATION EN MATIERE DE RENSEIGNEMENT

Section 1- L'exemple américain

§1- LE CONSEIL NATIONAL DE SECURITE

§2- LE *DIRECTOR OF CENTRAL INTELLIGENCE*

Section 2- L'état de la coordination en France

§1- LA GUERRE DES SERVICES

§2- LES STRUCTURES DE COORDINATION

§3- VERS LA CREATION D'UN CONSEIL NATIONAL DE SECURITE

## TITRE 2- LA REHABILITATION DE L'ACTION HUMAINE SUR LE TERRAIN

### CHAPITRE 1- LES MOYENS DU RENSEIGNEMENT HUMAIN

#### SECTION 1- LA QUETE DE RESSOURCES HUMAINES EFFICACES

§1- LE RECRUTEMENT OFFICIEL

§2- LA FORMATION

#### SECTION 2- TYPOLOGIE DES AGENTS DE RENSEIGNEMENT

§1- CATEGORISATION DES AGENTS DE RENSEIGNEMENTS

§2- LES QUALITES PROPRES AUX CAPTEURS HUMAINS

### CHAPITRE 2- LA MISE EN ŒUVRE DES MOYENS

#### SECTION 1- L'IMPORTANCE DU RESEAU DIPLOMATIQUE

§1- LES AVANTAGES DIPLOMATIQUES

§2- LES COMPOSANTES DU RESEAU

#### SECTION 2- LE DEVELOPPEMENT DES RESEAUX CLANDESTINS

§1- LES CONSEQUENCES BENEFIQUES DE LEUR MISE EN ŒUVRE

§2- ORGANISATION D'UN RESEAU CLANDESTIN

CONCLUSION

BIBLIOGRAPHIE

## INTRODUCTION

Les Hommes ont toujours eu le besoin de connaître, par nécessité ou par simple curiosité, ce qui se passait dans leur environnement proche ou plus éloigné. Bien sûr, la nature des informations recherchées a certainement évolué dans le temps, mais la finalité n'a jamais changé au fil des siècles. L'Homme pourrait ainsi être considéré comme un *homo curiosus*<sup>1</sup> ne pouvant se satisfaire de sa propre sphère de connaissances. La quête de l'information inconnue, inaccessible ou difficilement accessible, dissimulée volontairement, ou encore totalement inexistante, mais dont la légende ou les bruits de couloir l'ont érigé en probable réalité, constitue une pratique souvent inconsciente, en raison peut-être de son caractère inavouable, mais pourtant de plus en plus usitée.

### I- Du renseignement

Chaque être humain cherche constamment à connaître ce qu'il ignore. Il le fait généralement de manière constructive, témoignant ainsi d'une activité cérébrale, ce qui le différencie des animaux. Ces derniers bénéficient de leur instinct de survie, et leur quête du renseignement se limite à localiser l'endroit susceptible d'abriter une proie pour les nourrir. Mais en aucun cas, cette recherche n'est la conséquence d'une réflexion. Seul l'Homme est capable de se rendre compte qu'il engage une démarche intellectuelle à plus ou moins grande échelle, selon les capacités de chacun. Les activités les plus anodines telles que la visite d'un membre de sa famille un dimanche après-midi fait l'objet d'une recherche d'informations : connaître l'adresse de l'habitation, se procurer des cartes géographiques de la région, déterminer le chemin le plus court ou le plus convivial pour s'y rendre, savoir si la grand-mère préfère les roses rouges ou jaunes, etc... Le résultat de ces recherches, leur analyse, leur traitement fait apparaître un renseignement<sup>2</sup>. Mais avant d'aller plus loin dans notre exposé, nous allons proposer quelques définitions.

---

<sup>1</sup> Par analogie aux écrits de Schumpeter selon lesquels l'Homme est un *homo furiosus* avide de guerre et de conquêtes.

<sup>2</sup> WARUSFEL (B.), *Le renseignement stratégique*, Conférence donnée à l'IHEDN le vendredi 3 mars 2000 : « *Le renseignement est le traitement de l'information* ».

## **1- Définitions**

Le dictionnaire Larousse donne la définition suivante du terme « renseignement » : « *indication, éclaircissement servant à faire connaître une chose ; Connaissances de tous ordres sur un adversaire potentiel, utiles aux pouvoirs publics et au commandement militaire* ». Selon Mr Warusfel, le renseignement « *est au commencement de toute action de défense ou de sécurité. Il permet de déterminer l'objectif, d'apprécier les moyens et le dispositif de l'adversaire (donc de dimensionner les forces dont on aura besoin). L'absence ou l'insuffisance de renseignement expose à des risques inutiles. C'est l'instrument de décision.* ». Selon Pierre Joxe, ancien ministre de la Défense, il s'agit également d'un « *instrument de survie, de puissance et de cohérence* ».

Il apparaît donc que le renseignement est devenu un instrument non seulement de curiosité, de traitement de l'information, mais aussi un élément essentiel de la politique de défense d'un pays. Il intervient quotidiennement dans un contexte pacifique mais aussi de plus en plus souvent dans un environnement belliqueux. Ainsi est-il fait référence à « l'adversaire » dans la seconde définition proposée. Le renseignement, tel qu'envisagé à notre époque, ne se conçoit plus guère que dans un cadre de rapports de forces entre diverses puissances militaires, économiques ou diplomatiques. Il n'est dès lors plus permis de ne pas savoir ce qui se passe ailleurs sous peine de ne plus être capable de réagir et d'adapter son action sur la scène nationale ou internationale. L'acquisition du renseignement ne concerne plus seulement les Etats. Les entreprises commerciales sont de plus en plus intéressées par le concept d'intelligence économique et parfois touchées par des actions d'espionnage industriel. Mais dans ces deux cas de figure, l'objectif est le même : tenter de tout connaître sur son adversaire car celui-ci s'évertue à dissimuler au mieux les informations qu'il jugera sensibles.

## **2- La dissimulation d'informations**

Il peut paraître étonnant à notre époque de nous interroger sur la légitimité ou non des Etats, ou des entreprises, d'abriter des regards indiscrets certaines données pouvant avoir un caractère parfois vital. Mais ce sujet a été débattu, et a fait l'objet de réflexions, notamment celles de Spinoza, précisant, au sujet des « mensonges et tromperies entre

Etats », qu'ils se pratiquent au nom des intérêts de l'Etat<sup>3</sup>, établissant ainsi son caractère licite. De même, l'usage de la ruse et l'acquisition de renseignements dissimulés ont-t-ils été discutés dans divers documents. Ainsi l'article 24 de la Convention de la Haye du 18 octobre 1907 sur les lois et coutumes de la guerre dispose que « *les ruses de guerre et l'emploi des moyens nécessaires pour se procurer des renseignements sur l'ennemi et sur le terrain sont considérés comme licites* ». Mais bon nombre d'intellectuels de l'époque des Lumières considéraient l'acte de dissimulation comme « blâmable »<sup>4</sup>. Il faut cependant constater que la dissimulation est devenue une pratique usitée par tous et qu'elle a pour conséquence la mise en œuvre d'une politique de renseignement dont les objectifs sont de plus en plus nombreux.

### **3- Les objectifs du renseignement**

Les objectifs sont multiples et ont tendance à se multiplier en fonction de la complexité organisationnelle de l'adversaire. Un petit Etat comme la Papouasie Nouvelle Guinée demandera moins d'efforts de collecte d'informations et de traitement qu'un empire tel que les Etats Unis d'Amérique. Ceci est vrai sur le plan quantitatif et qualitatif. Quantitatif car les données concernant un Etat puissant et présent partout sur le globe sont beaucoup plus nombreuses qu'un pays dont la sphère d'influence se limite à un niveau régional. Qualitatif car l'intérêt de connaître un adversaire est plus ou moins important selon que ce dernier est fort ou faible et que son influence est plus ou moins vaste.

L'objectif principal est donc de connaître son ou ses adversaires. Pendant la guerre froide, qui avait opposé le camp occidental et le camp soviétique, on ne parlait que très rarement d'adversaires. On évoquait plus facilement le terme « ennemi ». Celui-ci était clairement identifié et la quasi totalité des activités de renseignement, de la part des grandes puissances, étaient portées sur « l'ennemi », qu'il soit d'un côté ou de l'autre, selon le point de vue duquel on se place. Or, de nos jours, les données sont différentes. La guerre froide n'a plus lieu, et depuis la dislocation du géant soviétique, les menaces sont moins bien

---

<sup>3</sup> SPINOZA, *Traité des autorités théologique et politique*, Chapitre XVI.

<sup>4</sup> DEWERPE (A.), *Espion – Une anthropologie historique du secret d'Etat contemporain*, Gallimard, Paris, 1994, p.40.

identifiables et beaucoup plus diffuses. Quels Etats doivent faire l'objet d'une attention plus particulière ? Pourquoi ?

De plus, ces derniers temps, les objectifs du renseignement ont été réorientés vers le monde économique. Une véritable « guerre économique »<sup>5</sup> mondiale, globale, a commencé et sans aucune déclaration préalable. L'affrontement n'est plus strictement inter-étatique. Des entreprises de toutes natures sont devenues les acteurs de cette guerre, et il n'est pas rare de voir se concurrencer sur un marché des entreprises d'un même pays. Le débat est permanent sur le bien fondé ou non de la mondialisation. Cela étant, ce phénomène existe et il faut en tenir compte pour tenter de comprendre plus précisément les différentes conséquences qu'il engendre. Dans le cadre d'une bataille militaire, le vainqueur risque d'être celui qui a le meilleur équipement et les renseignements les plus pointus. Dans le monde des entreprises, le raisonnement est à peu de choses près identique. Pour être compétitive, une entreprise doit bénéficier de structures efficaces et rapidement adaptables aux évolutions, d'informations fiables concernant l'état du marché et les différents acteurs économiques, afin de proposer des produits susceptibles de rencontrer l'adhésion de la demande. En cette ère « révolutionnaire » de la communication omniprésente, l'objet de valeur le plus recherché est sans aucun doute l'information et donc le renseignement mis à la disposition des décideurs. Celui qui ne sait pas ce qui se passe est aveugle et la cécité dans le monde des affaires est un défaut dont les conséquences sont très claires : la disparition à court terme de la scène économique. Alors les entreprises doivent s'informer et elles engagent dans ce but des stratégies diverses. Pour cela elles doivent se fixer des objectifs, non pas purement commerciaux, mais concernant davantage l'acquisition de renseignements.

Dès que le type d'adversaire est identifié, il est nécessaire de cerner l'environnement de son adversaire. Quelle est sa position géographique ? Avec quels inconvénients ou avantages topographiques doit-il compter ? Comment fonctionne-t-il ? Quelles sont ses ressources ? Quelles sont les entreprises les plus importantes ? Comment se défend-il militairement ? Toutes les réponses à ces interrogations vont aider à déterminer les intentions et la ligne de conduite que cet adversaire pourrait adopter. Ainsi, sera-t-il possible

---

<sup>5</sup> Déclaration de William Clinton, Président des USA : « la guerre économique est une réalité. Il nous faut nous donner tous les moyens pour la gagner »

d'anticiper ses actions, et d'éventuellement les contrer si elles portent atteinte à des intérêts déterminés. Mais afin d'espérer obtenir des réponses aux questions que l'on se pose à propos d'un objectif, il va falloir faire appel à différents types de renseignements.

#### 4- Les différentes catégories de renseignements

Il ne s'agit pas ici d'opérer une classification des méthodes d'acquisition du renseignement, mais d'essayer de différencier les différentes natures de renseignements susceptibles d'être obtenus. Selon Jacques Baud<sup>6</sup>, il existe une dizaine de types de renseignements :

- **Basique** : concerne les données les plus connues et généralement inscrites dans une encyclopédie.
- **Au combat** : se réfèrent aux informations militaires obtenues sur le terrain et situées au niveau tactique.
- **Biographique** : rassemble le plus d'informations possible sur une personne civile ou militaire: études effectuées, fonctions actuelles, opinions, habitudes, faiblesses, etc.
- **Economique** : concerne toutes les informations à caractère économique d'un pays, d'une entreprise, d'une organisation : évaluation générale et potentiel économique.
- **Electronique** : catégorie de plus en plus mise en exergue regroupant toutes les interceptions ou acquisitions effectuées au moyen de matériels électroniques.
- **Géographique** : ensemble de données concernant la géographie physique, humaine et sociale.
- **Militaire** : informations inhérentes aux forces armées (ordres de bataille, équipements, stratégies, tactiques, logistique, instruction, potentiel).
- **Des objectifs** : concerne l'acquisition, l'analyse et la sélection des objectifs dans le cadre d'un conflit de type nucléaire.

---

<sup>6</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, pp.403-424.

- **De situation** : regroupe les informations traitées quasiment en temps réel sur la situation actuelle d'un pays ou, plus précisément, d'une zone de bataille.
- **Technologique** : rassemble les acquisitions de capacités technologiques et la connaissance du niveau d'un pays dans ce domaine.

La grande variété de ces informations doit cependant être considérée dans une politique globale de recherche du renseignement initiée par le gouvernement ou l'état-major d'une entreprise. Cette politique se retrouve dans ce qu'on appelle le cycle du renseignement dont nous allons observer les grandes lignes.

## **5- Le cycle du renseignement**

Le cycle varie plus ou moins selon les différents Etats. Mais il est généralement quasiment identique, et décrit le plus souvent un processus divisé en quatre étapes et consistant à décider de l'obtention de certaines informations brutes, et d'en concevoir, après traitement, un renseignement utilisable par les commanditaires.

**1<sup>ERE</sup> ETAPE : LA PLANIFICATION<sup>7</sup>**. Elle s'applique à l'ensemble du processus de production du renseignement et consiste à établir des plans faits pour répondre aux exigences du gouvernement en matière de renseignement de sécurité. On définit alors une approche stratégique coordonnée en tenant compte des besoins des demandeurs. Puis on diffuse aux services spécialisés l'objet de la demande et l'autorisation de procéder à sa recherche.

**2<sup>EME</sup> ETAPE : LA COLLECTION**. Il s'agit ici de rassembler un maximum d'informations disponibles. Elles peuvent se trouver auprès de nombreuses sources de natures différentes : sources ouvertes, c'est à dire libre d'accès et sans restriction de type « confidentiel » ou « secret ». Il s'agit de la presse, de documentations disponibles sur Internet (malgré leur caractère parfois peu fiable), d'ouvrages, d'émissions radiophoniques ou télévisuelles, etc. Mais il existe également des sources moins accessibles et très protégées. L'acquisition de tels renseignements fait souvent appel à des méthodes

---

<sup>7</sup> Informations obtenues sur les sites Internet des services de renseignements canadiens et américains, le SCRS et la CIA : [www.csis-scrs.gc.ca](http://www.csis-scrs.gc.ca) et [www.odci.gov/cia](http://www.odci.gov/cia).

clandestines car illégales. Lorsque les informations recueillies sont jugées suffisantes, il est procédé à leur exploitation.

**3<sup>EME</sup> ETAPE : L'EXPLOITATION OU L'ANALYSE.** C'est à ce moment que l'information brute devient un renseignement exploitable, après un traitement durant laquelle elle est évaluée, recoupée avec d'autres éléments contenues dans divers fichiers, analysée, synthétisée et finalement interprétée<sup>8</sup>. Dès lors, le renseignement est envoyé au décideur qui en avait fait la demande.

**4<sup>EME</sup> ETAPE : LA DIFFUSION.** A ce moment du cycle, le commanditaire obtient en général la réponse à ses interrogations. Cette étape se traduit par la production de documents sous des formes diverses (écrits, photos satellites, documents sonores, graphiques ou même diffusion orale lorsque le sujet est très sensible).

Cette organisation de la recherche de l'information est incontournable. Elle se manifeste dans tous les domaines d'activités du renseignement.

## **6- Les différentes activités du renseignement**

Il existe deux activités principales : le renseignement extérieur et le contre-espionnage.

- ***Le renseignement extérieur*** : la définition la plus complète est sans doute celle donnée par le *Executive Order* n°12036 de janvier 1978 sur les activités de renseignement des Etats-Unis d'Amérique : « *Renseignement concernant les capacités, intentions et activités de puissances, d'organisations ou de personnalités étrangères. Il ne comprend pas le contre-renseignement, à l'exception des renseignements sur les activités terroristes* ». Il peut se pratiquer de manière légale en usant de sources ouvertes, comme nous l'avons vu avant. Mais il concerne aussi l'espionnage c'est à dire la collecte discrète d'informations secrètes.

---

<sup>8</sup> BAUD (J.), *op.cit.*, p.142.

➤ *Le contre-espionnage (CE)* : trois sens, peuvent être attachés à ce concept<sup>9</sup>.

- Le CE actif ou répressif : il s'agit de la recherche et de l'arrestation d'espions ou d'agents étrangers en opération sur le territoire concerné. En France, cette activité est effectuée dans le cadre d'une procédure judiciaire officielle.
- Le CE passif ou défensif : il vise à gêner ou empêcher les activités d'espionnage d'un groupuscule étranger (que ce soit un gouvernement ou une entreprise pratiquant l'espionnage industriel). Il peut être entrepris sur le territoire national ou à l'étranger.
- Le CE offensif : il cherche à obtenir des informations sur les services de renseignement étrangers afin de mieux connaître leurs méthodes et leurs intentions. Il tente aussi de les intoxiquer en diffusant des informations erronées. Ces objectifs sont possibles soit en recrutant un membre « en-place » de ces services, soit en y plaçant un agent-double.

La demande des différents gouvernements en renseignements, et la masse de données à récupérer et traiter a eu pour conséquence la création, vers la fin du XIX<sup>ème</sup> siècle, de services spécialisés dans ce domaine.

## **7- L'institutionnalisation du renseignement**

Cette institutionnalisation consiste à organiser l'établissement d'organismes administratifs, dépendants des autorités gouvernementales, chargés de mener les enquêtes ou les activités de renseignement. Ce phénomène a été observé pendant la période séparant la guerre franco-prussienne de 1870 et le premier conflit mondial de 1914, et surtout sur le continent européen<sup>10</sup>. Nous pouvons toutefois noter l'existence, au XVIII<sup>ème</sup> siècle, d'un état-major français spécialisé dans le renseignement, notamment au cours des guerres révolutionnaires, mais dont la durée de vie se limitait à la campagne militaire<sup>11</sup>. C'est au

---

<sup>9</sup> D'AUMALE (G.), FAURE (J-P.), *Guide de l'espionnage et du contre-espionnage*, Le cherche midi éditeur, Paris, 1998, p.105.

<sup>10</sup> Les anglais constituent une exception car ils avaient très tôt pris conscience de l'importance à donner à l'organisation institutionnelle du renseignement.

<sup>11</sup> DEWERPE (A.), *op.cit.*, p.122 : « En 1796, Berthier, chef d'état-major de Bonaparte à l'armée d'Italie, prévoit dans un document sur le service d'état-major général de l'armée des Alpes que le troisième des quatre adjudants généraux qui seconderont le chef d'état-major soit chargé du renseignement ».

cours du XIX<sup>ème</sup> siècle que cette activité nouvelle, en tant que concept organisé et dirigé soit vers l'étranger, soit contre les éléments considérés comme subversifs au sein même de l'Etat, est devenue autonome, afin d'être ultérieurement confiée à un service spécialisé agissant en permanence et non plus uniquement en temps de guerre. C'est ainsi qu'en France, le deuxième bureau de l'état-major centralisait les informations provenant des ministères à même d'obtenir des informations de l'extérieur : ceux de la Guerre et des Affaires étrangères.

La création, à travers le monde, de services « spéciaux », a donné naissance à une véritable communauté du renseignement, dont les effectifs croissent d'année en année. Chaque Etat en dispose. Ils sont plus ou moins nombreux selon l'importance donnée par un gouvernement à cette activité. Ainsi, la communauté américaine de « l'intelligence » s'élève à près de 150.000 membres. A titre de comparaison, la France n'en compterait qu'une dizaine de milliers. La conséquence de cette institutionnalisation est ce qu'Alain Dewerpe dénomme « la bureaucratisation du secret ». Etant donnée le caractère particulier de ces services, ces derniers sont régulièrement qualifiés d'Etat dans l'Etat, non seulement en raison de leur influence sur les décideurs mais aussi du fait des nombreuses précautions mises en œuvre afin de les protéger d'éléments nuisibles. Ainsi est-il nécessaire de créer des procédures d'habilitation du personnel et de classification des informations provenant de toutes sortes de documents établis au sein de ces administrations.

Le renseignement représente donc un ensemble de facteurs très nombreux, variés et complexes. Il faut cependant garder à l'esprit que son existence (et donc sa valeur et son caractère déterminant dans l'orientation des décideurs) dépend principalement des moyens d'acquisition des informations dont il est issu. Ce qui pose le problème des moyens mis en œuvre à cet effet, c'est à dire « *l'ensemble des ressources (personnes, groupes, relations, appareils ou installations) à la disposition d'un service de renseignements* »<sup>12</sup>. La nature de ces moyens ont sensiblement évolué, notamment depuis l'apparition d'instruments technologiques, plus ou moins efficaces, au cours de ce dernier siècle.

---

<sup>12</sup> BAUD (J.), *op.cit.*, p. 346.

## II- Evolution historique des moyens d'acquisition du renseignement

La question de l'acquisition d'informations protégées, ou disponibles ouvertement est une préoccupation majeure des responsables du renseignement. L'idéal serait sans doute de tout savoir. Tous les spécialistes des services spéciaux ont conscience du caractère utopique de cette affirmation. Ils sont d'ailleurs les premiers à se savoir constamment en état d'ignorance et ne démentiraient certainement pas Montaigne qui écrit que « *l'ignorance qui se sait, qui se juge et qui se condamne, ce n'est pas une entière ignorance : pour l'être, il faut qu'elle s'ignore soi-même* »<sup>13</sup>. En fait, il s'agirait plutôt de connaître tout ce qui est intéressant. Pour cela, nous l'avons dit plus haut, il faut pouvoir utiliser des capteurs. Aujourd'hui, ces derniers sont, théoriquement, nombreux. Ils n'ont cependant pas toujours été aussi abondants. C'est la raison pour laquelle l'Homme a longtemps constitué l'unique moyen de renseignement des différents gouvernements et armées.

### 1- L'espion comme unique source de renseignement

Le terme « espion » est apparu dans la langue française au XVIIIème siècle. Il vient, et a été dérivé, du mot *spiare* qui signifie épier. Dans la perse Antique, les espions étaient « *les yeux et les oreilles du Grand Roi* », montrant ainsi les relations entre le monde de l'ombre et la puissance publique<sup>14</sup>. La dictionnaire Larousse précise que l'espion est une « *personne chargée de recueillir des renseignements sur une puissance étrangère, qui épie, observe, cherche à surprendre les secrets d'autrui* ». Celui qui remplit cette mission a donc une tâche difficile à accomplir et parfois aussi à vivre.

Les métiers du renseignement ont été décriés et le sont encore de nos jours. Le Dictionnaire de l'Académie participa, à son époque, en 1694, aux critiques : « *celui qui espie, observe secrètement et adroitement quelqu'un pour luy nuire* » est un être méprisable. D'autres figures marquantes du XVIIème siècle, tel que Vattel, clamaient qu'un « *homme d'honneur, qui ne veut pas s'exposer à périr par la main du bourreau, ne fait point le métier d'espion ; ce métier ne peut s'exercer sans quelque espèce de trahison* » ; de même Montesquieu fustige par une phrase détonante cette activité : « *L'espionnage seroit peut-*

---

<sup>13</sup> MONTAIGNE, *Essais*, II, 12.

<sup>14</sup> D'AUMALE (G.), FAURE (J-P.), *op.cit.*, p.154.

*être tolérable s'il pouvoit être exercé par d'honnêtes gens ; mais l'infamie nécessaire de la personne peut faire juger de l'infamie de la chose »*<sup>15</sup>. Cette réprobation s'est manifestée par la suite dans la plupart des œuvres littéraires célèbres. Ceci explique sans doute une autre raison de la grande discrétion du métier. L'espion est toutefois un « mal nécessaire » et l'opinion publique commence à considérer au XX<sup>ème</sup> siècle que le nécessaire prend l'avantage sur le mal.

La discussion relative au caractère moral ou non de l'espionnage s'est nettement essoufflée entre les deux guerres mondiales, pour finalement disparaître presque totalement à l'issue du second conflit, en 1945. On estime dès lors que la finalité patriotique du renseignement possède une légitimité supérieure à toute autre considération moraliste. En effet, l'espion est d'une certaine manière «sauvé » par le service rendu à la patrie. Il devient même honorable<sup>16</sup>. Il ne pratique pas son métier dans un but lucratif mais au service d'un idéal, d'une conviction, notamment celle d'appartenance à une unité sociale à laquelle il est attaché. Allen Dulles, Directeur de la CIA de 1953 à 1963, avait écrit à leur sujet : « *Nos gens ne se dirigent pas vers le renseignement pour en tirer une récompense financière, ou parce que le service, en échange de leurs travaux, peut leur donner un grade élevé ou les faveurs du public. Ils sont là parce que l'occasion leur est offerte de servir leur Patrie, parce que ce travail est passionnant, parce qu'ils croient que, dans ce service, ils peuvent personnellement contribuer à la sécurité de notre nation »*<sup>17</sup>.

Les fictions littéraires ou cinématographiques ont même fait de l'espion une sorte de héros, capable de se sortir de tous les troubles et de parvenir à ses fins, malgré les nombreux obstacles dressés sur son chemin. Ces productions intellectuelles ont assurément servi de propagande à une époque où la guerre froide, ne pouvant se jouer sur le terrain militaire en raison de la dissuasion nucléaire, avait déplacé le terrain d'affrontements au niveau de la manipulation des esprits.

Cela étant, si l'espion est célébré comme un héros dans son propre camp, il est en général considéré comme une future victime du poteau d'exécution, sans aucune autre

---

<sup>15</sup> DEWERPE (A.), *op.cit.*, p.22.

<sup>16</sup> On utilise par exemple l'expression « honorable correspondant » pour évoquer les agents travaillant au service des services spéciaux français.

<sup>17</sup> ETIENNE (G.), MONIQUET (C.), *Histoire de l'espionnage mondial*, Editions du Félin, Paris, 1997, p.3.

forme de procès. Par chance, ou plutôt par maturation spirituelle, certains juristes ont amélioré le « statut » de l'espion. Ainsi l'article 30 de la Convention de La Haye de 1907 dispose que « *l'espion pris sur le fait ne pourra être condamné sans jugement préalable* ». Que ce soit en temps de guerre ou de paix, l'action de voler des informations est légitimement condamnable. Il faut cependant différencier les deux types d'espions condamnables en cas de flagrant délit. Si l'agent pris est étranger, il risquera la peine destinée à le châtier en tant que tel. Mais si l'espion est un traître, les conséquences sont multiples puisqu'il devra subir la peine maximale et, de surcroît, la flétrissure de toute une nation, d'autant plus forte que le pays est totalitaire. Même en France, au Moyen Age, on punissait de manière radicale les traîtres. Ainsi en fut-il ainsi lorsque, pendant la guerre de Cent Ans, opposant la France et l'Angleterre, un conflit d'intérêts entre Armagnacs, soutenant la famille royale française, et les Bourguignons, favorables aux Anglais, fit rage en France. La prise du pont de Saint-Cloud par les Armagnacs avait été facilitée par la trahison du dénommé Colinet de Puiseux. Après son arrestation, celui-ci fut « *amené à l'échafaud, dépouillé, mis tout nu et décapité. Il fut dépecé et ses quatre membres furent suspendus chacun à l'une des portes principales de Paris, et son corps fut mis dans un sac au gibet* »<sup>18</sup>.

L'espion, dont l'image peut parfois être associé, à tort, à un surhomme, n'en est pas moins un Homme. Car jusqu'à très récemment, au regard de l'ancienneté de l'Histoire de l'humanité, l'Homme a été l'unique source et le seul intercepteur d'informations dans le monde du renseignement.

Les premiers textes évoquant les activités d'espionnage datent de l'Antiquité. A cette époque, le seul intérêt de l'espion est de récupérer des informations de type militaire<sup>19</sup> : géographie physique, cartographie, armement ennemi. Ramsès II d'Égypte luttant, au XII<sup>e</sup> siècle av. JC, contre ses ennemis d'Anatolie centrale, les Hittites, avait à son service des espions chargés d'intoxiquer l'ennemi. Les stratèges de la Grèce Antique s'intéressaient aussi aux techniques de renseignement. Xénophon<sup>20</sup> insiste dans *L'Hipparque* sur l'importance des espions : ils doivent se familiariser dès le temps de paix à la fois avec le

---

<sup>18</sup> ETIENNE (G.), MONIQUET (C.), *op.cit.*, p.27.

<sup>19</sup> Il faut se rappeler qu'en ces temps, seules peu de personnes voyageaient au-delà des frontières de leur village, à l'exception des marchands ambulants et des espions.

<sup>20</sup> 426-354 av. JC.

pays ami et le pays ennemi. Il faut aussi avoir à son service des agents dans les Etats neutres et parmi les marchands.

De même Jules César fit-il un usage intensif des espions. Réputé pour ses succès militaires, celui-ci a pour habitude de ne pas envoyer ses légions à la guerre sans avoir auparavant pris la précaution d'envoyer des éclaireurs particuliers. Un de ses officiers, Volusénus Quadratus, se rendit célèbre par la qualité de ses observations de la Bretagne, île très peu explorée à cette époque (la Grande-Bretagne actuelle). Mais César, à l'instar des égyptiens, faisait aussi régulièrement appel aux marchands, à qui il demandait de rapporter des informations classiques, mais également politiques : coutumes, institutions, etc. Cette avance conceptuelle des romains en matière de renseignement est à mettre en parallèle avec les gaulois qui avaient une idée différente de la guerre. Selon certains spécialistes, les gaulois ne craignaient pas la mort, ce qui se reflétait sur leur techniques de combat consistant à se ruer en masse sur leur ennemi. «*S'ils étaient vaincus, c'est que les Dieux les avaient abandonnés et n'approuvaient pas leur résistance ; il ne restait donc qu'à se soumettre* »<sup>21</sup>. Il semble pourtant que Vercingétorix ne céda pas toujours au fatalisme de leurs croyances, et faisait, lui aussi, appel à des éclaireurs, mais pas de manière systématique.

L'Empire byzantin a également entretenu des réseaux d'informations. Un de ses points forts consistait en la mise sur pied d'opérations de guerre psychologique afin de diviser et affaiblir ses adversaires. Mais ils ont également contribué à la théorisation de l'espionnage. Un des empereurs de Byzance, Maurice (582 à 602), avait écrit un ouvrage de stratégie militaire, le *Strategikon*, dans lequel il note qu'il «*faut envoyer constamment et à intervalles réguliers des éclaireurs vigilants, des espions et des patrouilles pour obtenir des renseignements sur les mouvements de l'ennemi, ses forces et son organisation, de façon à se prémunir contre les surprises* »<sup>22</sup>. De même le souverain Léon VI (865-911) porte de l'intérêt pour les traîtres : «*Tenez-leur vos promesses s'ils vous disent la vérité, non seulement à cause d'eux, mais afin de vous en attirer d'autres. L'utilité qu'on retire d'un bon espion est beaucoup au-dessus de ce qu'on lui donne* »<sup>23</sup>.

---

<sup>21</sup> GRENIER (A.), Les Gaulois, Payot, Paris, 1970, p. 163.

<sup>22</sup> CHALIAND (G.), Des origines au nucléaire, Robert Laffont, Paris, 1990, p.220.

<sup>23</sup> *idem*, p.239.

En Occident, au Moyen Age, seuls peu de documents nous sont connus sur les techniques de renseignement utilisées. Il apparaît cependant que les réseaux entretenus par les Templiers étaient d'une remarquable efficacité puisque le Pape Clément V, avant d'engager une Croisade en 1306, avait convoqué Jacques de Molay, Grand Maître de l'ordre du Temple, fin connaisseur de l'Orient, en raison des bons rapports entretenus par les Templiers avec le monde musulman.

En ce qui concerne le royaume d'Angleterre, celui-ci eut très tôt le sentiment de l'utilité d'un service de renseignement permanent, contrairement à la plupart des autres pays européens. Il en fut ainsi sous le règne d'Elizabeth en raison du contexte politique de l'époque<sup>24</sup>. Les guerres de religion entre les pays catholiques et ceux favorables au protestantisme vont se régler non seulement sur les champs de bataille, mais aussi dans l'ombre. Afin de se tenir informée des intentions des ennemis de l'île, la reine va demander au grand Trésorier et chef de son Conseil privé, William Cecil, baron Burgley, de recueillir des informations. Celui-ci fonda donc un service d'espionnage et de contre-renseignement moderne, la « Défense de l'Etat »<sup>25</sup>. Ses agents étaient recrutés d'une manière innovante et dont le Royaume Uni du Xxème siècle se sert encore. Ainsi les meilleurs éléments du service étaient-ils remarqués dans les prestigieuses universités du pays ce qui, beaucoup plus tard, inspirera les services spéciaux russes qui y recruteront les «Cinq de Cambridge », Burgess, Mac Lean, Philby, Blunt et Cairncross, cinq britanniques qui accepteront, par idéologie pro-communiste, de trahir leur pays.

Nous ne pouvons pas nier dans cette rapide rétrospective, consacrée à l'espion, le rôle des femmes dans le renseignement. Leur apparition dans le monde assez masculin des affaires de l'ombre correspond avec une certaine idée de la modernisation des esprits. Longtemps, les femmes ne bénéficiaient pas dans leur vie d'un statut équivalent à celui du *pater familias*, reléguant l'épouse à un rôle secondaire dans les affaires familiales, hormis pour les tâches domestiques. Ce fut aussi le cas pour leur implication dans la recherche

---

<sup>24</sup> L'Eglise catholique romaine est vivement mise en cause en raison de sa corruption et de son opulence. Des réformes proposées par Calvin et Luther ont donné naissance à un nouveau courant dans la chrétienté, le protestantisme. L'Angleterre s'en fait un des défenseurs et se heurte à une Espagne très catholique grande puissance maritime.

<sup>25</sup> ETIENNE (G.), MONIQUET (C.), *op.cit.*, p. 37.

discrète de l'information. Si les premières affaires mettant à l'œuvre des femmes patriotes et idéalistes datent de la Révolution française, des situations beaucoup plus anciennes ont montré que les espionnes étaient caractérisées par leur esprit vénal, aventurier et manipulateur<sup>26</sup>. C'est ainsi que la Bible retrace l'histoire de Samson qui, ensorcelé par les charmes de Dalila, avoua le secret de sa force et ne put ainsi remplir sa mission de sauveur d'Israël.

L'action des femmes dans la guerre est toutefois intéressante. Rares sur le champ de bataille et ne portant par conséquent pas d'uniformes, elles étaient plus logiquement encouragées à se porter sur le travail clandestin. Ce fut notamment le cas pendant la seconde guerre mondiale durant laquelle Marie-Madeleine Fourcade se trouvait à la tête du réseau Alliance, un de ceux chargé du renseignement militaire en France, et renforcé par la présence de quelque trois mille agents et de matériels d'émission radio.

Beaucoup ont critiqué leur apparition dans le « domaine réservé » que constituait celui de la guerre. Le Général de Gaulle ne les aimait apparemment pas, « *l'idée de parachuter de jeunes anglaises du SOE en France occupée ne lui plaisait pas* ». De même, selon l'espion soviétique Richard Sorge, « *la femme est incapable de tout travail sérieux d'espionnage (...) trop émotive, trop dépourvue de raison et de sang-froid* »<sup>27</sup>. Cette dernière remarque peut ne pas être totalement dénuée de bon sens, mais elle peut aussi être réfutée catégoriquement, puisque quel que soit l'agent, masculin ou féminin, le manque d'entraînement pour ce type de missions particulières peut avoir les mêmes conséquences catastrophiques. Malgré les déclarations de Sorge<sup>28</sup>, les soviétiques se montrèrent plus clairvoyants sur le rôle important susceptible d'être joué par les femmes. Ainsi le KGB et les autres services spéciaux russes n'hésitèrent-ils pas à recruter des agents féminins, contrairement au FBI américain interdisant son accès aux femmes jusqu'en 1972.

L'Homme a donc longtemps été le seul moyen d'acquisition de l'information secrète. L'espion n'avait donc d'autre choix que de mettre en œuvre des méthodes souvent risquées afin d'accomplir ses missions. Le monde du renseignement a toutefois changé ses

---

<sup>26</sup> ETIENNE (G.), MONIQUET (C.), *op.cit.*, p.218.

<sup>27</sup> *idem*, p.217.

<sup>28</sup> Déclarations sans doute destinées à intoxiquer l'adversaire.

méthodes d'acquisitions depuis l'apparition des nouvelles techniques et technologies, ce qui a pu, dans certains cas, faciliter grandement la vie de l'espion.

## 2- L'apparition des moyens techniques dans le renseignement

C'est au début du Xxème siècle que les scientifiques de nombreux pays européens commencèrent à faire des découvertes intéressantes pour les services de renseignement. En effet, les mises au point dans les domaines des transmissions ont permis de communiquer plus facilement entre deux points géographiques distants. Les avantages en furent conséquents en matière militaire, notamment dans la transmission des ordres du commandement. Mais les ondes, transitant par les airs, ne sont pas, dans un premier temps, protégées. C'est ainsi qu'a pu être développée l'interception des communications, plus communément appelée COMINT (communication intelligence), et de signaux de toutes natures (électriques, magnétiques, etc...). Cette technique permet le recueil puis l'analyse de communications émises par quiconque, sans troubler l'émission et donc attirer l'attention du destinataire.

Les pionniers dans ce domaine ont été les services spéciaux français (le 2<sup>ème</sup> Bureau) et autrichiens ( Evidenzbüro ) qui, en 1908, menèrent une opération de ce genre à l'encontre des troupes italiennes. Ces interceptions se sont ensuite développées durant la première guerre mondiale sur le front du Nord-est, les troupes françaises ayant ainsi été chargées d'écouter les communications allemandes. A cette époque, les allemands développèrent aussi ces moyens par l'intermédiaire de la 8<sup>ème</sup> Armée qui permit au général von Hindenbourg de prendre l'avantage sur les russes pendant la bataille de Tannenberg, en août 1914. Ces techniques furent aussi à l'origine de l'entrée en guerre des Etats-Unis, en 1917, en raison de l'interception de la dépêche du sous-secrétaire allemand aux Affaires Etrangères, Arthur Zimmermann, adressée à l'ambassadeur d'Allemagne à Mexico<sup>29</sup>.

Les interceptions ont aussi joué un rôle important pendant le second conflit mondial. Mais avec le temps, ces interceptions se sont heurtées aux développements des moyens de

---

<sup>29</sup> Cette dépêche annonçait : « Nous commencerons le 1<sup>er</sup> février une campagne sous-marine sans restriction. Nous espérons néanmoins que les Etats-Unis resteront neutres. Si nous ne réussissons pas en cela, nous proposerons au Mexique une alliance [...]. Nous accorderons notre concours financier et nous stipulerons que le Mexique devra récupérer les territoires du Nouveau Mexique et de l'Arizona perdus en 1848 [...] ».

cryptographie qui consistent à changer la forme d'un message à partir des lettres et des chiffres qui le compose initialement, en le rendant a priori incompréhensible pour celui qui l'intercepte, mais pas pour le détenteur des codes de déchiffrement.

Les américains sont allés plus loin dans la recherche des interceptions de signaux, notamment depuis le second conflit mondial. L'Amiral Nimitz avait évalué le rôle de ce type d'interceptions dans les batailles du Pacifique, affirmant que le fait de posséder de telles techniques équivalait au fait d'avoir une flotte supplémentaire<sup>30</sup>. Dès lors, les choix des américains ont été clairs. La création d'une agence de renseignement technique, la *National Security Agency*, en 1952, témoigna de cette orientation. Ils commencèrent par développer des avions espions volant à très haute altitude, puis, bénéficiant de budgets très importants et de scientifiques compétents<sup>31</sup>, des satellites : ainsi le programme WS-117L fut-il approuvé par le président Eisenhower en 1954. Le premier appareil de renseignement électronique, « SCOTOP », fut mis en orbite en août 1960. Celui-ci était chargé d'enregistrer les signaux provenant des radars soviétiques chargés de suivre les objets spatiaux américains.

D'autres techniques de renseignement se développèrent en même temps. Ainsi en fut-il de l'observation du terrain ennemi par la voie aérienne, donnant naissance à l'IMINT ( imagery intelligence ). Cette technique débuta avec l'utilisation des premiers ballons. Pendant la première guerre mondiale, ces moyens ont permis une meilleure précision dans les tirs d'artillerie à longue distance ainsi que la reconnaissance des positions ennemies. La photo a aussi permis la possibilité d'interprétation des clichés par des spécialistes de l'armement de l'adversaire et des stratégies de combat. L'apparition des avions puis des satellites a permis, à l'instar des interceptions de signaux, l'observation plus pointue et moins risquée de la zone ennemie, en raison de leur altitude et de leur rapidité de passage.

Les moyens techniques sont aujourd'hui considérables. En effet, les progrès scientifiques constants durant tout le Xxème siècle ont largement contribué à ce phénomène d'explosion du renseignement d'origine technologique. Mais ces moyens d'espionnage à

---

<sup>30</sup> ANDRONOV (A.), *American geosynchronous SIGINT satellites*, Zarubezhnoye voyennoye obozreniye, n°12, 1993, p.37.

<sup>31</sup> Dont un certain nombre avait été recruté à l'issue du conflit de 1939-1945 en Allemagne.

moindre risque se sont développés en raison de l'utilisation grandissante des moyens technologiques de communications. Aujourd'hui, les liaisons téléphoniques intercontinentales, et même infra-continentales, se font par l'intermédiaire de satellites, de câbles sous-marins ou de relais de transmissions facilement détournables. Les appareils de communications modernes se sont démocratisés, et la grande majorité de la population des Etats développés est aujourd'hui propriétaire de téléphones cellulaires. Les affaires concernant le terrorisme en Corse nous ont montré qu'en plus de pouvoir être interceptés et écoutés, les possesseurs de tels appareils pouvaient être situés géographiquement, « grâce » aux techniques de trigonométrie.

Les spécialistes du renseignement se sont donc constamment adaptés aux évolutions des mœurs. L'information se trouve à l'endroit où elle naît, où elle transite et où elle arrive à destination. Or la plupart des informations intéressantes transitent par l'intermédiaire des canaux rapides : le câble ou le satellite. Pourquoi rapide ? parce que les décideurs, politiques, militaires, économiques ou financiers, sont de plus en plus pressés. Ce sont eux qui façonnent notre monde. Ils détiennent le pouvoir. Tout l'intérêt des services de renseignement est justement focalisé sur ces personnes. Savoir ce qu'ils prévoient équivaut à savoir comment sera fait le monde de demain, et permettra donc une meilleure prévision des diverses stratégies de chacun.

Malgré les enthousiasmes conséquents à la facilitation de l'acquisition du renseignement, il ne faut cependant pas omettre de garder à l'esprit la fragilité de ce processus, surtout lorsqu'il se fait au détriment de moyens plus classiques, c'est à dire les moyens humains. Qu'advierait-il si – c'est un cas d'école – tous les moyens technologiques d'acquisition du renseignement tombaient en panne en même temps, ou étaient victimes de dérèglements d'origines diverses. En un mot, que feraient les agences de renseignements sans les moyens nécessaires à l'acquisition du renseignement ?

Plus globalement, la question que nous allons nous poser au cours de cet exposé est celle de savoir si les moyens techniques, les nouvelles technologies, doivent être considérées comme l'unique outil de travail des services de renseignement, ou de toute autre personne susceptible de rechercher à un moment ou à un autre une information. L'Homme a-t-il définitivement perdu sa place dans le cycle du renseignement ? Le monde du

renseignement va-t-il se diriger lentement mais sûrement vers la solution de la confiance absolue accordée aux technologies modernes ? Au-delà de ces aspects techniques, nos sociétés démocratiques peuvent-elles accepter que la vie privée de ses citoyens soit mise à jour de façon permanente, du fait de l'efficacité des moyens d'interception et des politiques d'acquisition tous azimut de l'information de certains Etats occidentaux ? Ne faut-il pas, non plus, participer à un contrôle accru des agences de renseignement qui pourraient être tentées par une utilisation démesurée des moyens techniques de surveillance ? En ce qui concerne les moyens humains, suffit-il d'augmenter les budgets de l'action clandestine sur le terrain ? Faut-il encourager nos responsables politiques et nos spécialistes du renseignement à reconsidérer le renseignement du nouveau siècle, et à mieux coordonner les activités des « métiers de seigneurs » ? La naissance d'une véritable culture du renseignement est-elle fondamentale ?

Autant de questions auxquelles nous tenterons d'apporter des éclaircissements en analysant, dans un premier temps, les limites rencontrées par le renseignement effectué par des moyens technologiques, puis dans un second mouvement, nous observerons le rôle prépondérant de la présence humaine dans le cycle du renseignement.

**PARTIE 1<sup>ERE</sup>**

-

**LES LIMITES A L'EFFICACITE DU  
« TOUT TECHNOLOGIQUE »**

L'avènement de moyens technologiquement développés dans le monde du renseignement a certainement constitué une révolution dans l'organisation et la façon de travailler des services spéciaux. Mais, ce qui dans un premier temps a pu apparaître comme une véritable bénédiction, est vite apparu comme générateur de soucis, notamment au niveau du traitement des informations reçues, mais aussi en raison des nombreux moyens de contournement opposables aux espions de nouvelle génération (Titre 1).

Les préoccupations ne se sont pas uniquement manifestées au plan technique. En effet, les risques d'atteintes aux libertés publiques, dans nos démocraties, ont été mis en relief très tôt. Ces libertés ont ainsi fait l'objet de nombreuses protections conventionnelles et législatives, et les services de renseignement sont, aujourd'hui, davantage contrôlés par des organismes extérieurs (Titre 2).

## **TITRE 1- LES DIFFICULTES LIEES A LA MASSE D'INFORMATIONS OBTENUES TECHNIQUEMENT**

Les progrès dans les différents domaines techniques ont permis de mettre au point des applications sophistiquées permettant de transmettre et de recevoir un certain nombre de données de toutes natures. Mais ces mêmes progrès ont également grandement facilité l'interception des flux d'informations (Chapitre 1). Cependant, si la théorie tend à nous démontrer à quel point il est facile, pour les services de renseignement, de surveiller, de voir et d'écouter tout ce qui se passe sur notre planète, la pratique n'est, quant à elle, pas aussi flamboyante, et nous montre les limites de ce processus du « tout technologique » (Chapitre2).

### **CHAPITRE 1- LA MULTIPLICATION DES RENSEIGNEMENTS D'ORIGINE TECHNIQUE**

Les services spéciaux disposent aujourd'hui de différents moyens de surveillance qui n'existaient pas à l'époque où l'espion humain « régnait » en maître sur les affaires de renseignement (Section 1). L'accroissement quantitatif de ces moyens, et l'importance que leur ont donné les différents gouvernements, ont eu pour conséquence la création d'agences d'un genre nouveau dans les communautés du renseignement, spécialisés dans la mise en œuvre des nouveaux moyens d'acquisition du renseignement (Section 2).

#### **Section 1- Des moyens discrets et variés**

Les moyens technologiques mis en œuvre par les services spéciaux ont permis d'acquérir une multitude de renseignements divers, tant dans le domaine du visible que de l'audible.

## §1- Les différents types de renseignement d'origine technique

Les types de renseignement électronique sont très variés et s'adaptent à la nature de l'émetteur. Il existe cependant une appellation commune : SIGINT (Signal Intelligence). Le SIGINT est considéré comme une des formes de renseignement les plus importantes car l'interception des différentes émissions peut fournir un nombre très important d'informations de nature diplomatique, économique, militaire mais aussi d'autres données inhérentes aux émissions de radars, de systèmes d'armes ou de vols spatiaux<sup>32</sup>. Deux sous-catégories de SIGINT peuvent être distinguées : le COMINT (Communication Intelligence) et le ELINT (Electronics Intelligence).

Le COMINT consiste en l'interception des communications de gouvernements, d'organisations ou groupuscules étrangers et de particuliers. Ne sont pas concernées ici les émissions télévisuelles et radiophoniques classiques. Ces communications peuvent prendre différentes formes telles que la voix, le morse (moins utilisé de nos jours), le télex ou la télécopie, et peuvent être protégées, c'est à dire cryptées, ou non. De plus, elles peuvent passer par des fréquences hertziennes, sous forme numérique ou encore être acheminées via des câbles sous-marins. Il faut cependant dire que la plupart des interceptions de ce type concernent les échanges entre les représentations diplomatiques et leur capitale. Cela étant, les exemples pourraient être multipliés car chaque communication peut comporter des éléments intéressants au regard de certains gouvernements, ce qui pose le problème de la surproduction d'informations comme nous le verrons plus loin dans l'exposé.

L'ELINT, quant à lui, consiste à intercepter les signaux ne constituant pas une communication et provenant de matériels ou d'éléments civils ou militaires, à l'exclusion de ceux provenant d'explosions nucléaires. Ainsi est-il possible de recueillir des informations concernant les fréquences utilisées, la longueur du signal, et d'autres informations spécifiques et par conséquent de mener une véritable guerre électronique en recueillant des informations sur les positions ennemies, notamment en détectant, identifiant et en localisant les différentes sources émettrices. Il existe une sous-catégorie de l'ELINT, dénommée FISINT (Foreign Instrumentation Signals Intelligence). Il s'agit ici d'intercepter les

---

<sup>32</sup> RICHELSON (J.), *The U.S. Intelligence community*, Westview Press, San Francisco, Third Edition, 1995, p. 171.

émissions électromagnétiques associées à des tests ou à des déploiements d'appareils spatiaux, aériens ou sous-marins. Le test d'un missile fera l'objet d'un recueil d'informations de type télémétriques. Les renseignements tirés de ce recueil deviendront TELINT (Telemetry Intelligence), nouvelle sous-catégorie du FISINT.

Une autre catégorie importante de renseignement existe : le MASINT (Measurement and Signature Intelligence). La méthode d'acquisition est différente dans ce cas. En effet, le but de cette action n'est pas d'intercepter les émissions électroniques d'une source mais d'envoyer des signaux électroniques afin qu'ils heurtent l'objet suivi et réfléchissent ensuite les ondes, dans le but de communiquer un certain nombre de données quant à la vitesse et à la trajectoire. De nombreux dérivés du MASINT sont mis en œuvre : l'ACINT (renseignement acoustique), le LASINT (Laser Intelligence), l'OPINT (Optical Intelligence) ou encore le NUCINT (Nuclear Intelligence).

L'IMINT (Imagery Intelligence) est quant à lui devenu un type de renseignement hautement technique depuis l'apparition des satellites d'observation terrestre. Il s'agit du renseignement mettant en œuvre l'acquisition et le traitement d'images optiques ou électroniques. Il comprend, lui aussi, un certain nombre de sous-catégories : le VISINT (Visual Intelligence), les images visuelles ; le PHOTINT, les photographies ; le VIDINT, les images vidéos et l'OPTINT (Optronics Intelligence), les images thermiques ou infrarouges.

Toutes ces catégories d'intelligence mettent en œuvre des moyens techniques très sophistiqués, et ces derniers ont tendance à être de plus en plus employés depuis les airs et l'espace.

## **§2- Les moyens de l'acquisition**

La volonté de connaître un maximum d'informations doit s'accomplir en parallèle avec la nécessité de discrétion. Or les technologies apparues au cours du XX<sup>ème</sup> siècle ont permis de se faire moins voyant. Les ballons, puis les avions pilotés, ont ainsi permis de survoler le territoire adverse et d'y observer les différentes activités<sup>33</sup>. Mais aujourd'hui, il

---

<sup>33</sup> L'armée de l'air française possède toujours des moyens de renseignement aériens et pilotés utilisés dans le cadre, entre autres, de deux escadrons de reconnaissance aérienne, les ER 1/33 *Belfort* et 2/33 *Savoie*: avions

est plutôt question de mettre en œuvre des moyens guidés à distance et sans présence humaine à leur bord : les drones et les satellites.

#### A- Les drones

L'appellation d'origine de cet appareil est le « *Unmanned Aerial Vehicule* », c'est à dire véhicule sans pilote. L'avantage de ces petits avions de reconnaissance est remarquable : ils permettent le survol d'une zone quelconque<sup>34</sup>, la prise de clichés photographiques ou de séquences vidéo, sans faire appel à un pilote à leur bord puisqu'ils sont téléguidés à distance depuis une station de guidage, mobile ou statique, située au sol. Leurs missions sont variables. Ils permettent la reconnaissance aérienne, la surveillance du champ de bataille, la surveillance des frontières<sup>35</sup> ou encore la guerre électronique.

A l'origine, les drones étaient conçus comme des petits avions de modélisme améliorés. Transportant tout d'abord un simple appareil photo, ils sont devenus, avec le temps, des concentrés de technologies. Leur modernisation s'est effectuée avec la possibilité de lire les données recueillies en temps réel, de jour ou de nuit, et quelles que soient les conditions météorologiques. Ceci a été possible avec l'amélioration des moyens de communication et la faculté d'y installer des caméras de télévision. Ils ont ensuite été renforcés par des instruments infrarouges, thermiques, des désignateurs de but laser et des moyens de renseignement SIGINT.

Nous l'avons vu, le drone permet d'effectuer des missions dangereuses sans mettre en danger la vie de pilotes. Mais il faut également constater d'autres avantages. L'utilisation d'un avion de combat piloté pour une mission de renseignement amène, selon l'ancien contrôleur des armées, François Cailleateau, « *des contraintes non négligeables au détriment d'une meilleure productivité. Son poids, celui de son siège éjectable et de son alimentation en oxygène, multipliés par deux, de plus en plus souvent, pour les besoins d'une exploitation*

---

Mirage IV et Mirage F1 de reconnaissance, DC8 Sarigue et Gabriel pour l'interception électronique et hélicoptères Puma spécialisés dans l'intelligence électronique.

<sup>34</sup> Ils sont généralement utilisés lors de conflits de type militaires.

<sup>35</sup> Les Israéliens font un usage très intensif des drones pour la surveillance de leurs frontières avec les pays arabes, ainsi que l'observation des camps d'entraînement des membres du Hezbollah.

*rationnelle du système de combat, limitent les possibilités d'emport ou de portée* »<sup>36</sup>. Or l'un des avantages du drone consiste en sa grande distance d'engagement pouvant dépasser les 5000 km et, élément autrement intéressant, il ne requiert aucune piste d'envol et d'atterrissage. De plus, dans un futur très proche, les drones seront dotés de fuselages furtifs, réduisant ainsi au maximum leur signature radar<sup>37</sup>.

Depuis leur utilisation intensive lors des récents conflits, notamment en ex-Yougoslavie, un débat est apparu quant à l'avenir du renseignement aérien piloté. En effet, les Etats-Unis ont été les premiers à clairement faire un pas décisif dans le changement de leur politique de renseignement militaire. Ainsi en 1995, l'US Air Force a-t-elle décidé de retirer du service les derniers Mc Donnell Douglas *RF-4C Phantom*, avions spécialisés dans le renseignement aérien piloté. Ces avions ont rapidement été remplacés par la 11<sup>ème</sup> escadre de reconnaissance basée à Nellis, dotée exclusivement de drones. Mais certains auteurs estiment qu'il faut davantage opérer une redistribution des rôles de chaque moyen, et non pas un remplacement définitif.

Ainsi Patrick Erhardt écrit-il : « *qu'on le veuille ou non, un [...] œil robot (ou son opérateur au sol), aussi perfectionné soit-il, n'aura jamais les réflexes intelligents dont peut faire preuve un observateur embarqué à bord d'un aéronef. Certes, l'œil robot peut mieux voir que l'œil humain mais son action s'inscrit dans un espace d'évolution réduit et relativement conditionné par son plan de vol, alors que l'œil humain prend en compte une multitude d'indices pour faire évoluer le cours de ses recherches, tels que par exemple un nuage de poussière soulevé à l'horizon, un panache de fumée, voire un simple coup d'éclat de soleil sur le pare-brise d'un véhicule [...]* »<sup>38</sup>. Ceci peut sans doute expliquer la politique française de maintien de l'élément humain dans la reconnaissance militaire. Ainsi la France est-elle devenue une spécialiste dans le domaine de la veille radar avancée depuis la conception d'un système hélicoptère opérationnel appelé *Horizon*. Celui-ci, monté sous un hélicoptère de type *Cougar*, permet de détecter tout objet mobile se déplaçant à une vitesse

---

<sup>36</sup> CAILLETEAU (F.), *Faut-il un pilote dans l'avion ?*, Bulletin de Documentation de l'armée de l'air, n°501, novembre-décembre 1995, p.15.

<sup>37</sup> Technique agissant sur la forme et la composition des matériaux.

<sup>38</sup> ERHARDT (P.), *Le renseignement aérien piloté a-t-il encore un avenir ?*, Enjeux Atlantiques, n°15, juin 1997.

supérieure à 6km/h, avec une portée de 200 km en profondeur, quelles que soient les conditions météorologiques.

Toujours est-il qu'en dépit de ces débats au sujet de l'automatisation des systèmes de reconnaissance, il est un fait que les services de renseignement désirent non seulement éviter les pertes humaines, mais aussi accroître leur discrétion en utilisant au mieux les nouvelles technologies de l'espace.

## B- Les satellites

Voir sans être vu, écouter sans être entendu. Telle pourrait être la devise, et le désir, des spécialistes du renseignement. Ce désir a pourtant été satisfait depuis que l'Homme a décidé de faire évoluer des satellites en orbite terrestre. Leur déploiement permet, entre autres possibilités, de recueillir une masse considérable d'informations sur l'état de la planète, et de l'espace, sur l'état des forces des différents adversaires, sur les télécommunications transitant par d'autres satellites. En somme, il est possible grâce aux satellites de diminuer les risques d'obtenir des informations, d'éviter ainsi les pertes humaines et la publicité des actions de collecte de renseignements, comme ce fut le cas avec l'opération *Overflight*, dans laquelle un avion-espion américain, un U-2, avait été abattu au-dessus du territoire soviétique, le 1<sup>er</sup> mai 1960<sup>39</sup>.

Les satellites ont plusieurs avantages. Ils sont, à ce jour<sup>40</sup>, invulnérables (même s'ils ne sont pas à l'abri d'une collision avec un déchet spatial). Ils peuvent, pour les plus modernes d'entre eux, effectuer des missions, quelles que soient les conditions météorologiques. Enfin, ils échappent à toute législation internationale et nationale, interdisant le survol spatial d'un territoire sans autorisation préalable. Autant d'atouts que les services de renseignement ne peuvent négliger. Les soviétiques et les américains l'ont compris très vite. Pionniers dans le domaine spatial, ces derniers ont, dès les années 50 décidé de consacrer un budget non négligeable à la recherche spatiale. C'est ainsi que

---

<sup>39</sup> L'avion, et son pilote Gary Powers, avait décollé d'une base au Pakistan et avait pour mission de plusieurs sites stratégiques en URSS. Lire à ce sujet l'article suivant : LE GENDRE (B.), *Opération «Overflight»*, Le Monde, 2 mai 2000, p.14.

<sup>40</sup> Les scientifiques de nombreux pays essaient de mettre au point des techniques susceptibles d'atteindre, depuis le sol terrien ou l'espace, les satellites « gênants ». On les nomme ASAT (Armes anti-satellites). Elles peuvent être constituées de satellites tueurs, de missiles lancés par avion et de tirs lasers.

depuis 1958, ces deux pays ont lancé quelque trois mille satellites militaires en orbite dont un millier consacré à l'observation terrestre.

Le principal inconvénient de ces appareils est leur coût. Non seulement il faut les concevoir, ce qui implique des recherches importantes, des infrastructures modernes et des techniciens spécialisés. Mais il est également nécessaire de pouvoir les envoyer dans l'espace de manière indépendante, et donc de posséder ses propres fusées de lancement. Peu de nations en sont actuellement capables, même si leur nombre tend à augmenter. Des pays tels que la Chine, le Japon, l'Inde, le Pakistan, Israël, la Corée du Nord et d'autres encore ont manifesté le souhait de rejoindre le club des Etats maîtrisant les techniques spatiales.

Les satellites utilisent des orbites différentes selon la nature de leurs missions<sup>41</sup> :

- **Orbites hautes** (36.000 km d'altitude): utilisées par les satellites géostationnaires. Il s'agit de satellites d'alerte lointaine et de renseignement électronique (COMINT) de type MAGNUM et VORTEX.
- **Orbites semi-synchrones** (20.000 km d'altitude): utilisées par les satellites de surveillance des explosions nucléaires.
- **Orbites basses** (entre 200 et 1500 km d'altitude): utilisées par les satellites de reconnaissance optique (IMINT).
- **Orbites elliptique** ( variation entre 600 et 40.000 km d'altitude) : utilisées par les satellites d'alerte lointaine russes.

Nous l'avons constaté précédemment, il existe plusieurs types de satellites. Ainsi, certains ont-ils les facultés de recueillir des informations de type image, et d'autres, de type électronique. Pour les premiers, l'intérêt a été de développer des matériels d'observation à haute résolution par des moyens optique, électro-optique, infrarouge ou radar (capables de capter des images de quelques centimètres de résolution, ce qui revient à « défricher » l'équivalent d'une plaque d'immatriculation) et manoeuvrables depuis la Terre. Ceux-ci transmettent leurs images selon deux modes : par la transmission électronique, quasiment en temps réel, ou par la récupération de cartouches de films en mer ou dans les airs. Les seconds sont, quant à eux, capables d'intercepter les communications d'autres satellites et

---

<sup>41</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, p. 435.

des émissions venant de la Terre. Ainsi le satellite américain d'écoutes, MERCURY, possède une antenne dont le diamètre est égal à la longueur d'un terrain de football<sup>42</sup>.

La France a décidé, depuis quelques années, de se doter de satellites IMINT et SIGINT. Ainsi, le 7 juillet 1995, le premier satellite d'observation militaire français<sup>43</sup> a été lancé depuis la base de Kourou, en Guyane, afin d'être placé en orbite basse à 700km: HELIOS 1A. D'autres ont été lancés et ont fait leurs preuves dans le conflit yougoslave. Cela étant, la France a également émis le souhait de se doter de systèmes spatiaux d'écoute électronique. Elle a, dans ce but, mis en orbite des micro-satellites capables d'enregistrer et cataloguer les émissions électromagnétiques terrestres à hautes fréquences: CERISE et CLEMENTINE<sup>44</sup>.

Les technologies nouvelles au service des agences de renseignement se sont donc considérablement développées ces dernières décennies. Ceci a eu pour conséquence la création de nouvelles agences spécialisées dans la collecte d'informations par des moyens techniques sophistiqués, et l'apparition d'un nouveau type de personnel au sein des services spéciaux.

## **Section 2- Les agences de renseignement technique**

Le développement des agences techniques a montré les développements, au cours des dernières décennies, en matière de progrès de l'espionnage technique. Nous avons choisi de sélectionner les principales agences connues dans le monde.

### **§1- Les Etats-Unis d'Amérique**

Les américains sont aujourd'hui les plus grands utilisateurs de matériels techniques dans la recherche du renseignement. Pour cela, ils disposent de moyens très développés en raison des budgets colossaux attribués chaque année à leur communauté du renseignement.

---

<sup>42</sup> Environ 100 mètres. In Le Nouvel Observateur, *Comment l'Amérique nous espionne*, 10-09-1998, n°1779, p.16.

<sup>43</sup> Construit en partenariat avec l'Italie et l'Espagne qui bénéficient de renseignement au *pro rata* de leur participation dans le budget du programme HELIOS.

<sup>44</sup> X, *Hélios: le premier satellite militaire français*, Bulletin de documentation de l'Armée de l'air, n°501, novembre-décembre 1995, p.100.

Ils bénéficient à cet effet de plusieurs agences spécialisées dans la recherche technique d'informations, contrairement à la plupart des autres pays développés qui, eux, n'en possèdent qu'une seule, voire aucune. La première de ces agences est la NSA (National Security Agency). Selon certains spécialistes, elle serait même plus importante que la fameuse CIA (Central Intelligence Agency) qui est plus attachée à l'acquisition de renseignements d'origine humaine.

#### A- La NSA

Les missions de cette agence sont variées. Son occupation la plus connue est celle de l'espionnage technique, c'est à dire tout ce qui concerne le SIGINT (Signal Intelligence), soit l'interception de tous les signaux de toutes natures émis dans l'atmosphère terrestre par des puissances ou organisations étrangères. A ce titre, elle est aussi devenue une spécialiste des moyens de communications, d'informatique et d'acheminement des données dans le monde. La NSA est également l'établissement des Etats-Unis chargé des affaires de cryptologie. Elle doit sans cesse inventer de nouveaux codes pour les communications gouvernementales ou militaires américaines, et essayer de « casser » ceux qu'elle peut rencontrer lors de ses missions d'interceptions électroniques. De plus, cette agence est une des principales composantes américaines en matière de recherches et d'analyse des langues étrangères.

La création de cette agence date d'une directive présidentielle de Harry Truman émise en 1952<sup>45</sup>. Celle-ci désignait le ministre de la Défense comme responsable exécutif des interceptions de signaux ainsi que de la sécurité des transmissions gouvernementales. Elle est aujourd'hui sujette aux termes de la Directive sur le renseignement du Conseil National de Sécurité n°6<sup>46</sup> et du *National Security Act* de 1947. Elle constitue une organisation du ministère de la Défense américain et est subordonnée au ministre de la Défense.

La NSA est organisée en plusieurs directions spécialisées : les opérations, la sécurité des systèmes d'information, la recherche en technologies nouvelles, la formation et

---

<sup>45</sup> La NSA succède ainsi à l'AFSA (Armed Forces Security Agency).

<sup>46</sup> National Security Council Intelligence Directive.

l'entraînement, etc. La direction chargée des interceptions est divisée en plusieurs entités. Le groupe A est chargé du secteur russe et de l'Europe de l'est ; le groupe B focalise ses actions sur la Chine, la Corée, le Vietnam et l'Asie en général ; enfin le groupe G est chargé d'écouter le reste du monde, tant les nations du tiers monde que les alliés. Son budget n'est pas souvent publié mais les chiffres parfois révélés sont impressionnants. A elle seule, la NSA fonctionnerait grâce à un budget avoisinant les 4 milliards de dollars (environ 25 milliards de francs). Ses effectifs sont également peu connus mais les estimations laissent à penser que les civils employés à son quartier général, à Fort Meade au Maryland, seraient environ 20.000<sup>47</sup>, en plus des militaires rattachées à l'agence.

Les installations de la NSA sont très nombreuses. Fort Meade est une véritable ville dont la superficie approche les deux millions de mètres carrés, et dont l'accès est strictement réservé aux agents travaillant pour la NSA. Ils bénéficient de leurs propres magasins, de leurs installations sportives, de leurs cinémas et autres locaux de divertissement. De plus, la direction les encourage vivement à se marier entre eux afin de réduire les risques d'infiltrations. Ce sont toutefois leurs stations d'écoute à travers le monde qui montrent la puissance de cette agence : aux Etats-Unis (Yakima, WA ; Buckley, CO ; etc.), en Allemagne (Bad Aibling), au Japon (Misawa), en Australie (Pine Gap) et au Royaume-Uni (Menwith Hill) et bien d'autres encore.

## B- Le NRO

Le National Reconnaissance Office est l'administration du ministère de la Défense américain chargée de recueillir les informations d'origine image par le biais de satellites d'observation. Malgré sa grande discrétion à l'égard du contribuable américain<sup>48</sup>, le NRO dispose d'un budget annuel colossal : 8 milliards de dollars (environ 50 milliards de francs). Il est placé sous les ordres du responsable de l'Armée de l'Air américaine pour les systèmes spatiaux.

---

<sup>47</sup> La NSA est un des premiers employeurs de l'Etat du Maryland. Les civils sont en majorité des ingénieurs, des physiciens, des mathématiciens, des linguistes et des spécialistes de l'informatique.

<sup>48</sup> Son existence n'a été reconnue officiellement qu'en 1992, alors qu'elle a été créée en 1961.

L'agence dispose de deux installations majeures. L'une élabore et conçoit les satellites, L'*Air Force's Special PROJECTS Office*, située à El Segundo en Californie. L'autre, le *Consolidated Space Operation Center*, est chargée du contrôle de tous les satellites espions, et se trouve à Colorado Springs depuis 1992. Le NRO travaille en étroite collaboration avec la NIMA (National Imagery and Mapping Agency). Créée en 1996, celle-ci est chargée de coordonner et d'exploiter les informations obtenues par le biais des observations satellites, en éditant des cartes et des séquences vidéo des secteurs photographiés.

## **§2- La Fédération de Russie**

L'agence chargée de la collecte technique est la FAPSI : l'Agence Fédérale pour les Communications Gouvernementales et l'Information. Elle est considérée comme étant l'homologue de la NSA américaine. Elle a été créée par un décret présidentiel, du 19 février 1993. Ses fonctions étaient autrefois remplies par la 8<sup>ème</sup> Direction Principale et la 16<sup>ème</sup> Direction du KGB, le Service des Interceptions Radio et la Direction des Communications gouvernementales de l'URSS. Ses missions sont d'assurer la sécurité des systèmes d'information et de communications (notamment assurer la continuité des transmissions entre le Président et les forces nucléaires stratégiques), développer les outils technologiques de communications de l'administration et des forces armées, aussi bien en temps de guerre qu'en temps de paix. Mais la FAPSI est également chargée d'effectuer des missions d'écoutes et d'interception, parfois en collaboration avec le GRU, le service de renseignement militaire russe.

L'agence comprend une 1<sup>ère</sup> Direction Principale coiffant un certain nombre d'autres Directions et services : la Direction des opérations ; la Direction Principale des Communications gouvernementales : celle-ci est chargée de maintenir opérationnels les canaux de transmissions entre le Président et les différents services de sécurité ; le Centre technique et scientifique : il s'occupe de la conception de matériel informatique et de

logiciels destinés à assurer la protection des données. Un de ses logiciels est le VERBA qui est un système de cryptographie des informations commerciales<sup>49</sup>.

Elle est essentiellement composée de spécialistes (mathématiciens, physiciens, ingénieurs en électronique formés à l'Institut militaire des communications gouvernementales d'Orel et à l'Institut de cryptographie des communications et de l'information dépendant du FSB (service de contre-espionnage russe). Ses effectifs sont estimés à plusieurs dizaines de milliers. Mais des projets prévoient une réduction de 40%, d'ici à 2001, de ses effectifs civils et militaires. En dépit de cette réduction de personnel, une augmentation de budget est prévue : il passerait de 3 000 milliards de roubles en 1997 à 11 000 milliards de roubles à l'horizon 2001. Cette tendance explique sans doute une volonté de moderniser les équipements et les infrastructures.

Une des fonctions majeures de la FAPSI dans le domaine du renseignement est la collecte d'informations de nature politique, économique, militaire, scientifique et technologique transmises par des signaux hertziens, satellites ou autres. Ces données sont collectées par le biais d'une surveillance électronique permanente.

La FAPSI dispose d'un vaste réseau d'interception et de communications HF et satellite éparpillés sur le territoire russe et à l'étranger. En Russie, il existe des stations d'écoute au Laboratoire de recherche de renseignement électronique de Kuntsevo, au Service du chiffre du GRU à Komsomolskiy Prospekt à Moscou, au Centre de conduite du renseignement électronique du GRU à Klimovsk, au Centre de conduite du renseignement électronique naval à Puchkovo et à la station de réception du renseignement électronique cosmique du GRU à Vatutinki. A l'étranger, il existe encore des stations d'écoute dans les pays baltes, chargées de surveiller les pays scandinaves, la mer Baltique et plus généralement la partie nord de l'OTAN. Mais les plus importantes stations sont situées ailleurs : Lourdes (Cuba) ; le complexe électronique d'Aden et de l'île de Socotra au Yémen ; Cam Ranh Bay (Vietnam) : un accord avec les vietnamiens autorise l'exploitation de ce centre jusqu'en 2004.

---

<sup>49</sup> L'agence entretient également de nombreux contacts avec des organismes scientifiques tels que le NTT (Centre des sciences et des technologies) ou le TsITiS (Institut central pour l'information et les communications).

Une autre activité de la FAPSI dans le domaine du renseignement, à l'instar de la NSA, concerne la cryptologie. Bien qu'officiellement l'agence ne soit pas autorisée à mener des interceptions de conversations téléphoniques internes au pays, elle contrôle, entre autres, les transactions financières effectuées ainsi que les communications de nature électronique telles celles effectuées via internet.

### **§3- Le Royaume-Uni**

Le Government Communications Headquarters (GCHQ) est l'organisme chargé des interceptions. Il se trouve sous la responsabilité du Secrétaire d'Etat aux Affaires étrangères, et fournit le gouvernement britannique en renseignement de type SIGINT. Issu du service cryptologique de la Navy et de l'Armée (respectivement Room 40 et MI-8), le Government Code and Cypher School deviendra définitivement GCHQ en 1942. Officiellement, sa mission est la «*réception et l'analyse des transmissions étrangères et autres transmissions électroniques dans le but d'acquérir des renseignements*»<sup>50</sup>, menée à bien grâce à ses effectifs estimés à environ 15.000 agents.

Le rôle du GCHQ est de planifier et contrôler la coordination et l'exploitation des recherches de type SIGINT engagées dans le monde. Composée de six directions, cette agence tire la majeure partie de ses informations brutes de celle spécialisée dans les Opérations et la Collection qui se charge d'écouter les pays de l'ancien bloc soviétique (Special SIGINT), les autres territoires du globe (General SIGINT), de décrypter les éventuels messages codés (Cryptoanalysis) et de maintenir une coopération avec d'autres nations alliées telles que les Etats-Unis, le Canada, l'Australie ou la Nouvelle Zélande.

Son efficacité est aussi due à un réseau de stations d'écoutes éparpillées dans le monde. Quelques-une se situent au Royaume Uni (Morwenstow, Menwith Hill, Bletchey Park), en Allemagne (Teufelsberg, Dannenberg), en Australie (Darwin) et à Chypre (Pergamos).

---

<sup>50</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, p.232.

#### §4- La France

La France ne dispose pas vraiment d'agence de grande envergure spécialisée dans le renseignement technique. Ce sont en fait les deux agences chargées du renseignement extérieur qui se chargent de la collecte d'informations par les moyens technologiques divers : la DGSE (Direction Générale de la Sécurité Extérieure) et la DRM (Direction du Renseignement militaire).

La première travaille avec le GIC (Groupement des Contrôles radioélectriques). Son quartier général est situé à Domme dans la Dordogne, et centralise les résultats des stations d'écoutes situées en France et dans le monde, notamment sur l'île de Saint Barthélemy dans les Antilles, à Djibouti, à Mayotte et à La Réunion. Officiellement, la France ne dispose donc que peu de stations par rapport aux autres pays développés. Mais elle a récemment rattrapé son retard en matière d'observation spatiale grâce à la création de la DRM en 1992<sup>51</sup>. Celle-ci est en effet responsable de l'exploitation des satellites espions français mis en orbite avec le développement du programme Hélios 1 ET 2, ainsi que de l'utilisation accrue des drones, lors des divers conflits militaires engageant le pays. La DRM dispose des moyens des trois armées : une Brigade de l'armée de Terre dont l'activité est dédiée au renseignement technique : la BRGE (Brigade de Renseignement et de Guerre Electronique). Créée en 1993, celle-ci comprend des moyens de recherche du renseignement d'origine humaine, le 13<sup>ème</sup> RDP de Dieuze, mais surtout électromagnétique (44<sup>ème</sup> RT de Mutzig, 54<sup>ème</sup> RT de Haguenau) et image (7<sup>ème</sup> RA de Nevers). L'armée de l'air dispose aussi d'un escadron de renseignement (54<sup>ème</sup> ERA) et la marine met à la disposition de la DRM quelques navires de recueil SIGINT dont le *Monge* et le *Berry*.

Il ne s'agit pour le moment pas d'atteindre le niveau américain ou russe en matière d'acquisition technologique, mais il semble malgré tout que la France devrait se doter d'une agence unique et spécialisée dans les domaines de l'acquisition du renseignement d'origine technique, à l'instar des nations précédemment citées.

---

<sup>51</sup> Création due à de nombreuses défaillances françaises en matière de renseignement militaire remarquées pendant le conflit du Golfe.

## **CHAPITRE 2- LES DEFAILLANCES INHERENTES A LA RECHERCHE ET A L'EXPLOITATION DU RENSEIGNEMENT D'ORIGINE TECHNIQUE**

Les moyens techniques ont certainement permis de faciliter le travail des services de renseignement, mais il existe un certain nombre de problèmes liés à leur développement, tant au niveau des nombreux moyens de dissimulation existant (Section 1) qu'au niveau de l'exploitation des informations reçues qui, en raison de leur volume sans cesse croissant, deviennent ingérables (Section 2).

### **Section 1- Les moyens de dissimulation de l'information**

Les principaux moyens de dissimulation connus sont aujourd'hui le camouflage et la cryptographie.

#### **§1- Le camouflage**

La première réaction naturelle de l'Homme lorsqu'il se trouve dans une situation plus ou moins dangereuse est de se cacher. Le processus est identique quand il s'agit de protéger un objet du regard trop curieux d'un autre. Ce principe a rapidement été mis en application par les militaires, en particulier depuis les progrès effectués dans le domaine de l'observation aérienne. L'avènement des satellites a rendu la nécessité du camouflage permanent inéluctable. Il est certes possible de suivre la trajectoire d'un satellite et de savoir à quel moment il se trouve au-dessus d'un territoire, mais sa présence ininterrompue dans l'espace ne permet de dire exactement quand il va photographier le terrain, ni avec quels types de capteurs, optiques, radars ou infrarouges. Il a donc fallu adapter les moyens de camouflage. Il en existe plusieurs types<sup>52</sup> :

- **Le camouflage optique** : moyen le plus répandu et le plus ancien. Efficace contre les observations agissant dans le spectre visible, il peut utiliser des filets ou des couleurs permettant la confusion avec le terrain et les obstacles physiques (création de bâtiments sous-terrain).

---

<sup>52</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, pp.73-75.

- **Le camouflage infrarouge** : les moyens d'observation permettent de distinguer un objet artificiel ou naturel selon son degré de réflexion infrarouge (IR). Il a été constaté que les peintures classiques ne reflétaient pas suffisamment l'IR, contrairement à la chlorophylle des plantes, entraînant ainsi la détection immédiate d'un objet artificiel dans un environnement naturel. Des peintures et des filets agissant comme la chlorophylle ont donc été conçus à des fins de camouflage.
- **Le camouflage thermique** : il permet de réduire et de disperser l'émission de chaleur provenant de chaque objet. En effet, chaque objet, selon sa couleur, sa superficie, sa chaleur émet des rayonnements thermiques particuliers facilement détectables, de jour comme de nuit. Les moyens de camouflage se sont adaptés à cette difficulté.
- **Le camouflage radar** : ce moyen cherche à réduire la réflexion des ondes radars par un objet. Il s'est fait connaître pendant la guerre du Golfe avec les avions furtifs F-117 dont la forme et l'alliage avaient été conçues pour absorber le plus possible les signaux radars ennemis. Le but ultime étant soit de renvoyer très peu, ou pas du tout, d'ondes à la source, soit de les capter et de les transformer en ondes différentes.
- **Le camouflage sonore** : les sous-marins sont des exemples parfaits de ce type de camouflage car leur utilité se fonde exclusivement sur leur capacité de discrétion totale. Mais cette logique existe aussi en surface. Toutes les émissions sonores sont dangereuses. Les recherches portent donc de plus en plus sur leur réduction, à tous les niveaux de l'équipement militaire, ou autre (générateur électrique, armes, bavardages, etc.).

Un autre moyen permet d'induire l'adversaire en erreur : la déception. Elle consiste à simuler une activité en faisant passer une activité anormale pour une activité normale et vice versa. Une autre technique consiste à imiter la signature d'installations en plaçant des objets fictifs sur le terrain : des leurre. Ceux-ci peuvent reproduire des signaux ressemblant à des ponts, des stations radars, des colonnes de véhicules ou tout autre installation sensible.

La multiplication des transmissions de données, constatée depuis la modernisation des moyens de communication, a nécessité le besoin de se protéger contre toute éventualité de surveillance de ces échanges, notamment grâce aux moyens de cryptographie.

## §2- La cryptographie

La cryptographie, considérée comme étant un moyen “à la frontière des libertés”<sup>53</sup>, consiste à développer et mettre en œuvre des méthodes de chiffrement, pour un message ou un fichier informatique, dans le but de rendre le contenu incompréhensible à toute personne non autorisée à y avoir accès. Pour cela, des techniques diverses sont utilisées et reposent, en général, sur des ensembles mathématiques très complexes. Plus les techniques sont complexes, plus elles mettront de temps à être déchiffrées. Longtemps, les systèmes les plus utilisés en cryptographie ont été le codage et la substitution, ou bien la combinaison de ces techniques<sup>54</sup>.

- **Le codage** : il nécessite d'établir préalablement une liste exhaustive de mots accompagnés de leur équivalent codé. Les forces armées utilisent des codes tactiques dans lesquels chaque opérateur dispose d'un catalogue, à partir duquel il compose un trigramme, soit un ensemble de trois lettres. Le risque réside dans le fait de se faire capturer avec la traduction des codes, autorisant ainsi l'ennemi à intoxiquer le destinataire du message.

- **La substitution** : il s'agit de remplacer une lettre ou un chiffre par un autre. Par exemple, lorsqu'un message contient un «A», le message substitué contient un «Z». Cette substitution peut prendre des aspects différents et plus complexes que dans l'exemple précité.

Aujourd'hui, la cryptographie ne se fait plus de façon rudimentaire, mais par l'intermédiaire de moyens électroniques et de supercalculateurs. Une des principales conséquences de l'apparition de ces appareils de chiffrement a été la possibilité accrue de multiplier les types de cryptologie, et d'accroître ainsi la difficulté de déchiffrer les codes. Certes, un chiffrement en 40 bits (équivalent de  $10^{12}$  possibilités) est « cassé » en quelques secondes. Des codes de 56 bits (équivalent de  $7 \times 10^{16}$  possibilités) sont déchiffrés en 56 heures, à condition de mobiliser un nombre important de spécialistes, et d'ordinateurs. Ce

---

<sup>53</sup> GUISEL (J.), *Guerre dans le cyberspace- Services secrets et Internet*, La Découverte, Enquêtes, 1995, p.39.

<sup>54</sup> Voir pour plus de précision l'ouvrage de DESMARETZ (G.), *Le grand livre de l'espionnage*, Editions Chiron, Paris, 1999, pp.219-236.

sont finalement des temps assez faibles, et cela ne pose que peu de problèmes à des informaticiens chevronnés.

Il existe toutefois des chiffrements beaucoup plus puissants. Certains atteignent 56.000 voire 1 million de bits, ce qui est gigantesque, et finalement pas nécessaire puisqu'on estime que des codes de 128 ou 256 bits, au maximum, sont suffisamment efficaces contre les tentatives de déchiffrement. Là réside tout le problème pour les services de renseignement. A quoi bon posséder tout l'éventail technologique d'interception si d'autres technologies arrivent à brouiller les données, à moins d'essayer sans cesse de casser les codes rencontrés. Un autre obstacle s'ajoute à cela. Des logiciels de cryptologie sont désormais disponibles dans le public et notamment sur Internet (le fameux PGP, Pretty Good Privacy par exemple). La plupart des gouvernements se montrent hostiles face à l'expansion de ces logiciels. Il n'est pas facile de trouver l'équilibre entre la nécessité d'assurer un minimum de surveillance et l'obligation d'assurer à chaque citoyen la protection de son espace privé. Le gouvernement français a opté pour la protection de la confidentialité des communications en autorisant un codage à 128 bits<sup>55</sup>. Mais il n'est pas insensé de penser que les services de sécurité français sont capables de déchiffrer ces codes.

La plupart des pays financent des quantités de projets de recherche consacrées à la cryptographie, ce qui ne va pas faciliter la tâche des services spécialisés, démontrant par là que les limites des nouvelles technologies dans la quête du renseignement. Ceci est également vrai quant au traitement des informations interceptées, car leur très grande quantité souffre d'un manque de plus en plus évident d'exploitation et d'analyse.

---

<sup>55</sup> La science du cryptage a longtemps été réservée aux domaines militaires, diplomatiques et gouvernementaux. Mais accepter la « démocratisation » de la cryptologie donne l'occasion à des groupuscules mafieux ou autrement dangereux de communiquer sans crainte.

## Section 2- Le manque d'exploitation et de valorisation des données

### §1- Le manque d'exploitation des informations

Les américains sont très clairs vis à vis de leur politique de renseignement. Zbigniew Brzezinski, ancien conseiller pour la Sécurité nationale du président Carter, précise que les Etats-Unis ont «*fait le choix de tout savoir*»<sup>56</sup>. Cet objectif très ambitieux semblerait difficile à atteindre s'il n'existait pas toute la panoplie de moyens que nous avons étudié plus tôt. Les ordinateurs ont la possibilité de stocker une masse énorme d'informations. La NSA et les services spéciaux sont bien sûr équipés avec ce genre de matériel. Mais ces informations ne seront pas d'une grande utilité si personne ne peut les lire et en faire un usage efficace. Or là réside un des problèmes majeurs des services secrets. Trop d'informations tuent le renseignement. C'est pour cela que l'exploitation et l'analyse des informations doit devenir une priorité majeure du renseignement futur.

L'exploitation constitue l'étape dans laquelle un spécialiste traite un certain nombre d'informations provenant de tous les niveaux (humains, techniques, etc.). Ces informations sont variées. Elles peuvent provenir de représentations officielles telles que les ambassades ou les consulats, de documentations ouverte, d'interceptions électroniques, d'opérations clandestines à l'étranger, ou d'autres encore. Lorsque ces documents ont été traités, le spécialiste les trie, les confronte avec les connaissances qu'il peut avoir du problème<sup>57</sup>, les évalue, les recoupe avec des informations obtenues dans le passé et inscrites dans les différents fichiers, sélectionne les renseignements jugés intéressants et les met en forme afin de les diffuser aux commanditaires. Il s'agit donc d'un travail de synthèse indispensable face à la masse d'éléments recueillis chaque jour.

Mais l'exploitation n'est pas complète si les renseignements qu'elle engendre ne font pas l'objet d'analyses. Or la conséquence directe d'une défaillance dans l'exploitation est le manque d'analyses des informations. L'analyse représente le moment, au cours de l'exploitation de l'information, pendant lequel cette dernière est soumise à un examen rationnel et complet afin d'en identifier les données concluantes, pour un problème donné.

---

<sup>56</sup> In Le Nouvel Observateur, *Comment l'Amérique nous espionne*, 10-09-1998, n°1779, p.26.

<sup>57</sup> Ces spécialistes s'occupent en général de thèmes pour lesquels ils ont une connaissance approfondie.

Pour cela, les spécialistes font appel à la taxonomie des problèmes analytiques, c'est à dire « *la description des problèmes et les caractéristiques génériques des solutions recherchées* »<sup>58</sup>. Cette technique permet donc de sélectionner les personnes capables de traiter au mieux un problème en fonction de celui-ci, et de définir correctement les tâches qu'elles devront accomplir. Cependant des progrès sont à effectuer en matière d'analyse et d'exploitation.

Ce travail nécessite, en effet, le recrutement important de nombreux analystes venant d'horizons divers<sup>59</sup>, ceux-ci s'avérant être, pour l'heure, trop peu nombreux dans notre nouvelle ère de l'information. Il existe certes des moyens automatisés de traitement de l'information. Ce sont des logiciels capables d'explorer les banques de données informatiques afin d'en tirer les informations pertinentes<sup>60</sup>. Bien qu'étant d'une très grande utilité, notamment face à l'afflux massif de données sur Internet, ces moyens sont limités car ils ne font pas appel à la forme humaine d'intelligence mais à une forme mécanique d'intelligence. Or l'analyse doit faire intervenir une part de subjectivité, ce que la machine ne peut pas effectuer. En effet, l'analyse consiste, en plus de la compréhension en temps réel des évènements, à tenter de prévoir l'avenir. Il ne s'agit pas ici de faire de la voyance mais de la prospective, à l'instar de ce que font les milieux de la finance et de l'économie avec la notion de « risque-pays »<sup>61</sup>. Une bonne analyse ne peut que dire avec précision en quoi consisteront les actions d'un Etat, d'une organisation ou d'une armée incontrôlée. Cela nécessite une connaissance très complète d'un environnement, notamment par le biais d'éléments culturels et psychologiques, ce qui a, semble-t-il, fait défaut lors du conflit du Kosovo. En somme, le travail des exploitants et analystes doit contribuer à donner de la valeur à l'information, et donc au renseignement.

## **§2- La valeur à donner au renseignement**

L'évaluation d'une information représente une tâche complexe que l'analyste doit pratiquer systématiquement, avant même de tenir compte de celle-ci. Les éléments qu'il reçoit continuellement proviennent de plus en plus de sources techniques. Les interceptions réalisées par les nombreuses stations d'écoutes sont transmises en bloc à des centres de

---

<sup>58</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, p.29.

<sup>59</sup> Notamment des universitaires : sociologues, économistes, juristes, géographes, etc.

<sup>60</sup> Ils sont connus sous diverses appellations : Tai ga, Noémic, Spirit, Semiomap, Périclès, etc.

<sup>61</sup> KLEN (M.), *La nouvelle bataille du renseignement*, Défense Nationale, juin 1993, p.52.

traitement. Or parmi ces interceptions, certaines contiennent des erreurs volontairement transmises. Sachant que les ordinateurs des réseaux d'écoutes de certains Etats enregistrent des conversations en fonction des mots employés, il est facile de prononcer d'autres mots, anodins, et définis à l'avance. De même, il est facile de noyer tout un réseau de surveillance en utilisant systématiquement des mots particuliers susceptibles d'entraîner l'enregistrement de la conversation ou de l'échange par fax ou courrier électronique. Ainsi, la technologie ne peut pas faire grand chose face à ce nouveau problème. L'analyste recevant la transcription d'un échange vocal ou autre devra donc doubler le volume de son travail : vérifier la crédibilité de l'information et, ensuite, la traiter.

La vérification d'une information consiste en son évaluation. Selon Brigitte Henri, « pour l'agent de renseignement, la valeur des informations qu'il recueille est déterminante. A partir du moment où il décide de les transmettre, c'est qu'il leur accorde un intérêt suffisant. Cela signifie donc que l'informateur est fiable et que les recoupements effectués rendent ses informations crédibles. L'agent de renseignement attribue une valeur au renseignement qu'il transmet, une sorte de « cotation » : source digne de foi, source non recoupée, renseignement confidentiel, secret... »<sup>62</sup>. Pendant longtemps, l'évaluation n'avait porté que sur des sources humaines. Mais les nombreux moyens de contourner les techniques mises au service de l'espionnage ont également amené à évaluer les sources techniques.

Il s'agit dans un premier temps d'effectuer une qualification de la source. Le barème va de « Fiable » à « Peu sûre » ou « Fiabilité non évaluable ». Puis on tâche de qualifier le contenu de l'information apportée : « Confirmé » pour le meilleur des cas ou « Improbable » et « Exactitude non évaluable » pour le moins bon. Lorsque ces qualifications sont faites, on établit une « matrice d'évaluation empirique », consistant en un tableau permettant de déterminer en fonction de la source et du contenu, si une information deviendra renseignement, et à quel niveau la classification devra être opérée. L'art de bien évaluer fait appel à l'équilibre entre la justesse et la précision de l'information. Beaucoup de conclusions peuvent s'avérer exactes dans toutes les situations, ne présentant ainsi pas d'intérêt véritable pour le commanditaire du renseignement. Mais des conclusions

---

<sup>62</sup> HENRI (B.), *Le renseignement – Un enjeu de pouvoir*, Economica, Paris, 1998, p.48.

davantage « risquées », malgré leur part d'incertitude, sont susceptibles d'apporter un meilleur éclairage de la situation présente ou à venir.

Les faiblesses constatées dans l'exploitation et la valorisation du renseignement se sont concrétisées par quelques défaillances marquantes ayant permis de démontrer les faiblesses des Goliaths de l'espionnage.

### **Section 3- Les ratés des puissances centrales occidentales**

Les échecs dans le monde de l'espionnage sont généralement plus connus que les réussites. Les américains, malgré leurs moyens, n'avaient ainsi pas réussi à connaître exactement le moment de l'invasion de l'Afghanistan par les soviétiques. Depuis les exemples se sont multipliés, et leur médiatisation n'a fait qu'accroître les interrogations sur l'importance accordée au renseignement technique.

#### **§1- Les essais nucléaires indiens**

Quelques régions du monde sont considérées comme des poudrières. Ainsi en est-il des Balkans, mais aussi, et surtout, de l'Asie. La Chine, ayant vocation à devenir une puissance régionale, voire mondiale, est entourée de voisins dont les intentions sont assez proches. L'Inde, le Pakistan et la Corée du Nord posent un certain nombre de problèmes aux puissances de renseignement occidentales, en raison de leur volonté de se doter d'armements sophistiqués et destructeurs. La non-prolifération est un sujet majeur d'inquiétude pour le futur. Or le « club » fermé des nations nucléaires ne souhaite pas voir émerger d'autres membres en son sein, sous peine de voir s'effondrer le principe de dissuasion mutuelle. Pourtant, des essais nucléaires ont été effectués par les indiens en mai 1998, dans la région de Pokharan, au sud-ouest de New Delhi. Les indiens avaient déjà effectué des essais nucléaires dans le passé, en 1974 (Ils disposeraient d'une soixantaine de têtes nucléaires pouvant être envoyés à près de 2500 km<sup>63</sup>). Mais cette fois-ci, les services de renseignement occidentaux ont été pris par surprise, soulevant des tempêtes de protestations, notamment aux Etats-Unis.

---

<sup>63</sup> Arms Control Association in TIME Magazine, 25 mai 1998, p.26.

En effet, avec, d'une part, leurs satellites *Keyhole-12* (de type IMINT, comparables au satellite *Hubble*<sup>64</sup>), d'une valeur d'un milliard de dollars chacun, capables de photographier des objets terriens très petits, et d'autre part, leurs satellites *Lacrosse*, tout aussi chers, dotés de caméras radar capables de s'affranchir des pires conditions météorologiques terrestres (ce qui est le cas dans la région de Pokharan), les américains n'ont pas réussi à prévoir la série de tests avant l'heure. En temps de crise, ces satellites sont rapidement positionnables à la verticale de la zone concernée, et permettent la prise de clichés et leur traitement en quelques heures, tout au plus.

Cela étant, si aucun responsable du renseignement ne commande ces photos, l'information ne pourra pas être obtenue. Or il semble qu'à cette époque, les décideurs politiques américains ne concevaient pas une probable série de tests en Inde. Les prises de vue satellite ne s'effectuaient donc qu'une fois toutes les 24 heures. De plus, les scientifiques indiens, connaissant les temps de passage des satellites à leur verticale, avaient pris le soin de camoufler les préparatifs par des manœuvres anodines. Les indiens avaient aussi procédé à une synchronisation de leurs essais afin que les centres de détection sismique n'enregistrent qu'une seule détonation<sup>65</sup>. Après enquête, il est apparu qu'une photo avait été prise six heures avant l'explosion et révélait de manière très claire des preuves de préparatifs inhabituels, ce qui a démontré un manque de rapidité du traitement des renseignements d'origine image et de leur diffusion aux politiques. Ces derniers, avertis à temps, auraient sans doute exercé des pressions sur le gouvernement indien pour stopper leur cycle d'essais, évitant ainsi une probable course aux armes nucléaires dans cette région.

Un autre pays, voisin de la République Populaire de Chine, a également posé quelques problèmes : la Corée du Nord.

## **§2- La fusée nord-coréenne**

Les relations entre la Corée du Nord et les pays occidentaux ont été, et sont toujours, régulièrement marquées par des tensions plus ou moins graves. Considéré comme le dernier

---

<sup>64</sup> Satellite chargé de percer les mystères de l'Univers en photographiant les constellations stellaires.

<sup>65</sup> LABBE (M-H.), *Les essais nucléaires et la non-prolifération*, Politique étrangère, Automne 1998, p.535.

pays stalinien de la planète par les observateurs internationaux, le pays a reçu l'appellation de « *rogue state* » (Etat voyou) par les responsables américains. Touché gravement par la famine, le pays n'hésite pourtant pas à investir énormément de fonds dans la recherche militaire, en particulier dans le domaine nucléaire, posant ainsi quelques problèmes stratégiques. Les américains, soucieux de la sécurité internationale en Asie du sud-est, mobilisent des moyens importants de surveillance à l'encontre de la Corée. Les USA considèrent que si ces les coréens ont les moyens de maîtriser l'énergie nucléaire, ils essaieront, tôt ou tard, de fabriquer des vecteurs susceptibles de transporter des têtes nucléaires, et d'atteindre d'autres pays comme, par exemple, la Corée du sud, le Japon ou les Etats-Unis.

Dans ces circonstances, le régime de Pyongyang a procédé, le 31 août 1998, au lancement d'une fusée de trois étages, « *Taepo Dong 1* », depuis la base de Musudin-ri Hwadae dans la province de Hamgyoung, capable d'atteindre une cible à deux mille kilomètres, et ayant survolé le Japon. Les coréens ont, dès après le lancement, indiqué que la fusée avait placé, avec succès, un petit satellite en orbite, déclaration infirmée par le Commandement spatial américain. Mais quelques semaines après, le ministre de la Défense sud-coréen déclara qu'il ne s'agissait pas d'une fusée et d'un satellite, mais d'un missile balistique pouvant transporter une tête nucléaire. Selon l'édition électronique de CNN du 31 août 1998<sup>66</sup>, ce test ne constituait nullement une surprise pour les japonais. Il est vrai que les américains, en raison de la surveillance effectuée en permanence par l'intermédiaire des satellites IMINT et SIGINT et d'un navire d'écoute, le « *Observation Island* », naviguant sur zone, pouvaient difficilement ignorer ce qui se passait en Corée. Il est pourtant difficile de croire que les américains aient décidé de laisser faire le lancement, car le missile aurait pu être chargé et toucher un pays allié. Le fait qu'il ait survolé le Japon montre bien les défaillances de tout l'arsenal technologique américain. Selon le sénateur Byrd de l'Etat d'Alaska, le missile serait retombé non loin des côtes de son Etat<sup>67</sup>, prouvant clairement que si les analystes américains avaient eu connaissance du test, ils auraient engagé des mesures défensives de type anti-missile.

---

<sup>66</sup> [www.cnn.com](http://www.cnn.com)

<sup>67</sup> [www.kimsoft.com/1997/byrd.htm](http://www.kimsoft.com/1997/byrd.htm)

Cela étant, la Corée du Nord est un obstacle important pour les services occidentaux et américains. Selon un ancien ambassadeur américain en Corée du Sud, Donald Gregg : *« j'ai passé trente ans de ma vie à travailler avec la CIA et j'avais pour habitude de dire que l'espionnage de la Corée du Nord constituait un des principaux échecs de la communauté américaine du renseignement. C'est une cible très difficile à toucher. Nous avons des satellites très performants, qui nous envoient des photos très précises du pays, mais cela ne nous permet pourtant pas de savoir ce qui se passe dans la tête des gens, en particulier des dirigeants et des militaires, que nous n'avons pas la possibilité d'approcher, rendant impossible de connaître leurs intentions, ne serait-ce que superficiellement »*<sup>68</sup>. Cette déclaration nous amène à constater qu'un autre système américain, dévoilé récemment, en dépit de sa grande ambition en matière d'espionnage, risque de devenir un échec majeur, ainsi qu'un gouffre financier. Il s'agit du réseau « Echelon ».

### **§3- Echelon ou l'échec annoncé d'un programme trop ambitieux**

De quoi s'agit-il ? Echelon est un immense réseau d'ordinateurs qui sélectionnent automatiquement des adresses électroniques ou des numéros de téléphone, grâce à un certain nombre d'interceptions d'échanges téléphoniques, fax ou via Internet, effectuées à travers le monde par le biais de moyens électroniques de type SIGINT. Les mots clés, et tous les autres éléments aidant à trier les interceptions, sont catalogués dans ce qu'on appelle les dictionnaires ECHELON. La partie la plus impressionnante de ce programme est sans doute la masse de moyens mis en œuvre pour écouter le monde. Créé par les américains pendant la guerre froide pour identifier les communications en Union Soviétique, ce système est aujourd'hui actionné par d'autres pays anglo-saxons tels que le Royaume-Uni, l'Australie, le Canada et la Nouvelle Zélande. De nombreuses stations d'écoute sont réparties dans ces pays et l'ensemble de leur production est envoyée au quartier général de la NSA à Fort Meade (en Virginie) aux USA. Mais les critiques venant d'anciens agents de la NSA se font de moins en moins rares.

Selon eux, la NSA ne possède pas les logiciels capables de traiter correctement et efficacement la totalité des interceptions effectuées, même si une partie minime d'entre elles

---

<sup>68</sup> [www.commongroundradio.org/transcpt/98/9848.html](http://www.commongroundradio.org/transcpt/98/9848.html)

est sélectionnée. Ils ajoutent que « *si le système était si performant que nous voulons bien le croire, les terroristes internationaux tels qu'Oussama Bin Laden ne seraient plus capables de se faufiler entre les mailles du filet technologique* »<sup>69</sup>. (Les conséquences tragiques de cette lacune nous sont apparues lors des attentats du 11 septembre 2001 aux Etats-Unis. Cette date restera sans doute connue comme le plus grand échec de la communauté américaine du renseignement)<sup>70</sup>. De même, certains élus américains commencent également à s'interroger sur la raison d'être de ce réseau. Dans son article, Seymour Hersh<sup>71</sup> dit à ce sujet que « *Echelon, à défaut d'être un des plus grand secret de la NSA, loin de là, est davantage considéré comme un trou noir fiscal par les commissions parlementaires et sénatoriales américaines pour les questions de renseignement* ». Comme nous l'avons observé plus tôt, il existe des possibilités de contourner ce type d'espionnage, notamment en le noyant par des mots connus comme étant sensibles, et en adaptant son vocabulaire avec des mots plus anodins. En somme, l'échec du réseau tire sans doute son origine dans sa révélation au grand public<sup>72</sup>. Car en ayant connaissance du principe de fonctionnement de ce système, il nous est facile de le contourner. Les individus à l'encontre de qui ce réseau est orienté, c'est à dire les terroristes, les industriels ou les gouvernements, ont ainsi la faculté de détourner l'attention des ordinateurs de la NSA, démultipliant le travail des analystes, et rendant, par conséquent, « l'hydre mondiale »<sup>73</sup> inefficace.

Nous avons vu que l'avènement des technologie sophistiquées dans le monde de l'espionnage n'a pas eu que des avantages, et suscite aujourd'hui des interrogations, davantage quant à leur mode d'emploi que vis à vis de leur existence même. Ainsi, des interrogations sont apparues sur le plan juridique, notamment en raison des ombreuses libertés publiques mises en cause.

---

<sup>69</sup> HERSH (S.), *The Intelligence Gap*, The New Yorker, 6 décembre 1999, pp.58-76.

<sup>70</sup> Mise à jour de notre mémoire (février 2002).

<sup>71</sup> *Idem*.

<sup>72</sup> Les services spéciaux des pays non membres du système Echelon en avaient connaissance depuis plus longtemps.

<sup>73</sup> Le Canard Enchaîné, n°4140, 1<sup>er</sup> mars 2000, p.1.

## **TITRE 2- LA QUESTION DES ATTEINTES AUX LIBERTES PUBLIQUES DANS LES DEMOCRATIES**

Certains auteurs ont très tôt compris les enjeux et les risques de dérapages d'une société de l'information dans laquelle la vie privée et l'intégrité des communications seraient rangées dans les archives de l'Histoire de l'Humanité. Ainsi George Orwell dans *1984* et Aldous Huxley dans *Le meilleur des mondes*, et le film américain *Ennemi d'Etat*, narraient à quel point certains Etats, et leurs services de renseignement, ont le pouvoir de s'immiscer dans les affaires privées des individus, grâce aujourd'hui à des moyens technologiques puissants. Cependant, si les libertés publiques ont tendance à être menacées davantage de jour en jour (Chapitre 1), les Etats d'essence démocratique tentent de mettre un frein à la surveillance toute azimut en instaurant un minimum de contrôles des activités de renseignement (Chapitre 2).

### **CHAPITRE 1- LA NATURE DES LIBERTES MENACEES**

Nous l'avons vu, les nouvelles technologies permettent non seulement de communiquer d'avantage et plus facilement, démultipliant ainsi les flux d'informations circulant dans le monde. En même temps, les moyens d'interception ont connu des améliorations et permettent désormais d'espionner tous les échanges effectués à partir d'un téléphone, fax, télex ou Internet. Cela ne va pas sans poser un certain nombre de problèmes juridiques, tant au niveau des atteintes à la personnalité (Section 1), des questions relatives aux données nominatives (Section 2) et des intrusions dans les systèmes informatiques (Section 3).

#### **Section 1- Les atteintes à la personnalité**

Les possibilités d'atteintes à la personnalité se sont multipliées à mesure que les techniques d'interception se sont modernisées. Un certain nombre de textes juridiques se sont interposés et rendent plus difficile, ou plutôt moins anarchique, les activités d'espionnage effectuées à l'encontre de la population civile.

## §1- Le droit à l'image et à la voix

Les atteintes à la vie privée ne sont pas évidentes à prouver, puisqu'en matière d'espionnage, il est difficile d'établir si nous faisons l'objet de curiosités répréhensibles. Nous allons toutefois considérer les cas dans lesquels il y a bien une intrusion dans la vie privée, et notamment en ce qui concerne notre image et nos communications. Les atteintes aux communications ont depuis longtemps fait l'objet d'études et de législations. Ainsi, en 1865, la première Convention internationale sur les Télégraphes contenait des dispositions concernant la liberté de communication et ses limitations. Son article 4 reconnaît « *le droit pour toute personne de correspondre par le biais des télégraphes* » et l'article 5 traite pour sa part de la garantie du secret des correspondances malgré l'existence de l'article 19 qui autorise les Parties Contractantes à interrompre les transmissions privées susceptibles de porter atteinte à la sécurité de l'Etat. Il a, en effet, toujours été difficile d'établir une frontière « acceptable » entre le domaine privé et la sécurité du pays, ce qui n'a cependant pas empêché les Etats démocratiques à prendre des mesures favorables à la protection de la vie privée.

En France, il existe un certain nombre de dispositions légales, parmi lesquelles la loi du 10 juillet 1991 introduisant dans son article premier, le principe du secret des « *correspondances émises par la voie des télécommunications* », et protégeant les citoyens des interceptions, ou des prises non autorisées de photographies ou de séquences vidéo. Ainsi l'art. 226-2 du Nouveau Code Pénal (NCP) s'applique-t-il aux documents visés par l'art. 226-1. Ces articles se caractérisent par deux conditions. Il doit s'agir :

- Soit de paroles prononcées à titre privé ou confidentiel, qui ont été captées, enregistrées ou transmises par un procédé quelconque. Il n'est plus exigé, comme dans l'art. 368 de l'ancien Code Pénal, qu'elles aient été prononcées dans un lieu privé; il suffit qu'elles aient été prononcées, même dans un lieu public, à titre privé ou confidentiel. Il peut donc s'agir aussi bien de paroles échangées dans la rue, à un domicile, au bureau, qu'au téléphone ou que sur Internet. Tous les cas de figure d'interceptions ont été pris en compte ici.

- Soit de l'image d'une personne se trouvant dans un lieu privé, qui a été fixée, enregistrée ou transmise par un procédé quelconque. La remarque relative aux paroles est identique quant à la question de l'image : cette dernière peut avoir été prise dans tout lieu privé, y compris un service Internet qui aurait un caractère privé.

L'article 226-1 NCP ajoute que ces documents doivent être obtenus « *volontairement* », dans le but de « *porter atteinte à l'intimité de la vie privée* ». Le comportement sanctionné est le fait de « *conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser* » ces documents.

En outre, le secret des correspondances est également protégé par les dispositions pénales de l'article 226-15 NCP. Cet article permet de poursuivre pénalement toute diffusion de correspondances, quelle soit leur nature : lettres, communications téléphoniques ou communications transmises par Internet<sup>74</sup>, intégrant ainsi le rôle croissant de ce vecteur de communication. En effet, l'alinéa 2 incrimine « *le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* ».

La question de la protection de la vie privée est également prise en compte par la Convention Européenne des Droits de l'Homme (CEDH). Celle-ci ne comporte pas vraiment de précisions relatives au droit au respect de la vie privée et familiale, du domicile et de la correspondance contenu dans l'article 8. Mais des interprétations de la Commission et de la Cour européenne des Droits de l'Homme ont permis de dégager davantage de principes dans ce domaine sensible. La Cour a indiqué qu'il ne pouvait y avoir ingérence d'un Etat dans l'exercice de ce droit, à l'exception de certaines circonstances particulières notamment lorsque l'ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la réalisation d'un nombre limité d'objectifs tels que la sûreté publique et la protection de la santé ou de la morale. Cependant, plusieurs

---

<sup>74</sup> Exemple : en septembre 1997, les messages émis sur un récepteur de poche du service de sécurité du Président des Etats-Unis s'affichaient automatiquement sur un site internet.

affaires ont mis en exergue des violations de l'article 8 par les Etats, notamment la surveillance secrète des conversations téléphoniques (Huvig contre France, 1990<sup>75</sup>).

Malgré l'existence de ces textes, il n'est pas rare de constater des atteintes à la vie privée, comme ce fut le cas en France avec l'affaire des écoutes de la « cellule anti-terroriste de l'Elysée » pendant la présidence de Mr Mitterrand<sup>76</sup>.

## §2- Le cas des écoutes téléphoniques en France

La loi du 10 juillet 1991 règlemente les conditions dans lesquelles peuvent être effectuées des écoutes téléphoniques par l'administration et la justice. Sont ainsi encadrées :

- **Les écoutes administratives**, effectuées à titre préventif : elles peuvent être demandées par les ministères de l'Intérieur, de la Défense ou de l'Economie et des Finances pour des motifs précis tels les atteintes à la sécurité nationale, le terrorisme, le crime organisé, l'espionnage économique et scientifique ou la reconstitution de groupements dissous. Elles sont autorisées par le Premier ministre, pour une durée de quatre mois, renouvelables, et confiés au Groupement interministériel de contrôle (GIC).
- **Les écoutes judiciaires** : effectuées dans le cadre d'une enquête relative à une infraction déjà commise, elles sont ordonnées par un juge d'instruction sur commission rogatoire écrite. Elles sont ici effectuées par les services chargés de l'enquête, c'est à dire la Police ou la Gendarmerie.

En règle générale, les écoutes sont effectuées dans des cadres légaux. Une affaire a cependant fait apparaître, en France, les liens ambigus entre le pouvoir et les réseaux du renseignement : les « écoutes de l'Elysée ». Pendant près de trois ans, de 1983 à 1986, un certain nombre de personnes ont fait l'objet d'écoutes téléphoniques systématiques de la part de la cellule antiterroriste de l'Elysée. Le problème résidait dans le fait que ces écoutes

---

<sup>75</sup> Cette condamnation de la France eut pour effet d'encourager la France à changer son arsenal juridique en votant une loi, datée du 10 juillet 1991, gouvernant les interceptions de communications et cherchant à créer un meilleur équilibre entre les nécessités de la sécurité nationale et le respect de la vie privée.

<sup>76</sup> Cela étant, la réglementation n'empêche nullement les écoutes, dites sauvages, effectuées en dehors de tout cadre juridique.

étaient diligentées à l'encontre de personnes n'ayant aucun lien avec des affaires de terrorisme : des journalistes, des avocats, des hommes politiques, des écrivains, des comédiens et des hommes d'affaires. Les gendarmes composant cette cellule utilisaient, et détournaient, des lignes du GIC normalement attribuées aux différents ministères. Ils effectuaient des écoutes, les classaient et les répertoriaient dans des fichiers informatiques incontrôlés. De plus, ces écoutes ne respectaient pas la procédure concernant les écoutes administratives.

Paul Barril, ancien membre de cette cellule précise que « *ces écoutes avaient été diligentées pour la bonne cause. Pour lutter contre la grande criminalité, le terrorisme ou le trafic d'armes qui représentent un réel danger. Aucun citoyen ne peut trouver à redire à ces écoutes quand on sait qu'elles servent à assurer la défense du pays et de la collectivité [...]. Mais on s'est aperçu très vite que ces écoutes étaient quelque chose de fabuleux. Et comme la lutte antiterroriste intéresse moins les hommes politiques que les sondages, que s'est-il passé ? Certains ont compris que ces écoutes étaient beaucoup plus intéressantes pour servir dans des affaires privées, dans des affaires de politique. Finalement, au lieu de s'occuper des attentats, comme celui du restaurant Goldenberg par exemple, on s'est davantage intéressé à ce qu'allait écrire Le Monde ou Le Canard Enchaîné, et Jean-Edern Hallier est devenu une cible prioritaire parce qu'il écrivait ou qu'il était supposé écrire un livre sur François Mitterrand* »<sup>77</sup>.

La lumière faite sur cette affaire ne doit pas faire penser que les écoutes illégales et sauvages ont subitement été abandonnées. La multiplication des agences de renseignement privées, et la présence de nombreux matériels de surveillance sur le marché, ont certainement contribué à cet état de fait. Si la loi de 1991 ne permet pas d'empêcher, en pratique, les écoutes sauvages, elle a cependant permis de mieux encadrer tout le système de surveillance et de préservation de la sécurité nationale.

Nous l'avons vu dans les affaires des écoutes de l'Élysée que les transcriptions des écoutes donnaient lieu à des fichages informatiques des données reçues. Or il est clair que cette pratique, naissante dans les années 80, s'est considérablement développée de nos jours,

---

<sup>77</sup> Historia, Dossier : Les services secrets français en action, n°602, février 1997, p.72.

et donne lieu à la création de très nombreux fichiers capables de rassembler des masses de données nominatives. La loi est cependant intervenue afin d'en limiter la création et la diffusion.

## **Section 2 – Les questions relatives aux données nominatives**

### **§1- Définition**

Depuis l'apparition de l'informatique, il a été possible de stocker un certain nombre d'informations concernant les individus. Prenons un exemple. Il n'est pas rare de trouver dans nos boîtes aux lettres des courriers libellés à nos noms et adresses, et dont le contenu est très personnalisé, de sorte que nous puissions croire que nous en sommes l'unique destinataire. Or il n'en est rien. Les logiciels informatiques permettent aujourd'hui de créer des fichiers nominatifs contenant notre adresse. Dès lors, il est assez facile de pratiquer le « *mailing* », c'est à dire envoyer le même courrier à toutes les personnes inscrites dans ce fichier. Au fil des années, ces fichiers se sont étoffés d'autres informations nominatives plus personnelles. Il peut ainsi s'agir de la nature de nos loisirs, du nombre de personne vivant à l'adresse indiquée, de l'âge des enfants, ou tellement d'autres données encore.

De même, sur Internet, est-t-il aisé de communiquer des informations nominatives, recueillies de manière régulière en dehors d'Internet ou sur le réseau. Or celles-ci font l'objet d'une protection organisée par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et complétée par celle du 3 janvier 1979 sur les archives et modifiée par la loi du 11 mars 1988. Cette loi a été votée pour encadrer le développement de l'informatique afin que celle-ci ne porte atteinte, comme le précise son article premier, « *ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Afin de communiquer ces informations, il faut respecter certaines dispositions, sous peine d'être poursuivi pénalement.

Selon l'article 4 de cette loi de 1978, les données nominatives contenues dans les fichiers sont définies comme étant « *les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent* ».

## §2- La constitution de fichiers

La constitution de ces fichiers est devenue plus simple, et le danger de ces bases de données personnelles est plus grand qu'auparavant car elles sont désormais beaucoup plus facilement accessibles, et peuvent se recouper avec d'autres, ce qui permet de connaître tous les aspects de la vie privée d'une personne<sup>78</sup>. Il faut donc prêter attention au traitement de ces données. Selon la loi de 1978, le traitement se définit comme « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* ». Jusqu'à présent, il est possible de distinguer deux types de règles de constitution de fichiers: si le traitement est créé dans le cadre d'un établissement privé, on doit faire une déclaration préalable. S'il l'est dans le cadre d'un établissement public, la constitution du traitement nécessite un avis préalable de la Commission nationale sur l'Informatique et les Libertés (CNIL), auquel on ne peut passer outre que par décret (pris sur avis conforme du Conseil d'Etat)<sup>79</sup>.

En matière de traitement proposé sur Internet, la CNIL a eu l'occasion d'énoncer des règles qu'il convient de respecter pour obtenir un avis favorable. La CNIL était saisie de deux demandes de constitution d'annuaires sur Internet<sup>80</sup>. Celle-ci a rendu un avis favorable car le traitement avait, selon elle, une finalité légitime et pertinente (« *favoriser les communications et les échanges entre les chercheurs du monde entier* ») car il portait sur des informations limitées (le sexe, le nom, les prénoms, le lieu de travail et le service d'affectation, les numéros de téléphone, de télécopie et l'adresse de "courriers électroniques" professionnels), il exigeait l'accord des personnes recensées, accord pouvant

---

<sup>78</sup> Dossier : " Vie privée à vendre sur le réseau " Le Monde cahiers multimédia 15 &16 juin 1997.

<sup>79</sup> Excepté dans le cadre de normes simplifiées ou des fichiers de santé pour lesquels l'avis d'un comité spécialisé est nécessaire.

<sup>80</sup> Délibérations de la CNIL n°95-131 & 95-132 - 7 nov. 1995 : Centre national de calcul parallèle des sciences de la terre et Institut de physique nucléaire d'Orsay – Gazette du Palais 1996 n°26, 27 p.36.

être révoqué à tout moment et il devait faire apparaître un avis rappelant les droits, garanties et protections dont bénéficient les personnes recensées.

De plus l'article 31 de la loi de 1978 précise que la mise en mémoire des données nominatives «*qui directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs de la personne*» est interdite, sauf accord exprès de l'intéressé, ou bien que les utilisateurs de ces traitements soient des églises, des mouvements à caractère religieux, philosophique, politique ou syndical. L'article 226-19 NCP, à l'instar de la loi de 1978, sanctionne le fait de mettre ou de conserver en mémoire informatisée des données nominatives qui directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs de la personnes, ainsi que les informations nominatives concernant des infractions, des condamnations ou des mesures de sûreté.

Une des craintes soulevées en matière de création de fichiers contenant des données nominatives, est certainement la possibilité de recouper ces informations avec d'autres fichiers. Chaque fichier pris séparément pourrait ne pas constituer une infraction en soi, mais son rapprochement avec d'autres données pourrait laisser apparaître des renseignements beaucoup moins superficiels. Une des activités des services spéciaux est de recouper systématiquement les informations qu'ils acquièrent dans le but d'en tirer un renseignement valable. Ceci a été énormément facilité grâce aux moyens informatiques. Mais en mars 1974, le journal *Le Monde* révélait que le Ministère de l'Intérieur prévoyait de mettre en place une banque de données alimentée par des fichiers provenant de différents services de police<sup>81</sup>. Le tollé soulevé par cette annonce amena le Premier ministre, Pierre Mesmer, à en limiter l'envergure et à créer une commission «*Informatique et Liberté*» chargé de proposer une réglementation dans ce domaine. Quelques années après, fut mise en œuvre la CNIL, qui n'hésitera pas à aller contrôler les services de renseignement français, dont le contre-espionnage (DST) et le renseignement extérieur (DGSE).

---

<sup>81</sup> Projet SAFARI (Système Automatisé pour les fichiers Administratifs et le Répertoire des Individus).

L'importance des réactions suscitées face aux décisions de constituer des fichiers montre à quel point il est difficile de mettre en balance la protection de la vie privée et la sécurité nationale.

### **Section 3- Les intrusions dans les systèmes informatiques**

Le développement des réseaux informatiques tels qu'Internet, Intranet ou d'autres réseaux, ont permis de rendre les informations qu'ils contiennent à la fois plus faciles à communiquer mais aussi beaucoup plus faciles à détourner. Bien sûr, le réseau constitue un moyen unique pour l'échange de ces informations. Il faut cependant ne pas omettre le fait que certaines d'entre-elles ne sont destinées qu'à un usage purement privé. Cela pose donc le problème de l'utilisation des réseaux dans le dessein de pratiquer des attaques informatiques à l'encontre d'ordinateurs et de leur contenu.

#### **§1- Les pirates informatiques**

La démocratisation des ordinateurs a permis aux individus, autres que les scientifiques ou les militaires, de se consacrer à des nouveaux types de loisirs. Les jeux vidéo, la bureautique à domicile puis Internet aujourd'hui, sont devenus des occupations que les générations précédant les années quatre vingt ne connaissaient pas toujours très bien. Pourtant, les amateurs de cette nouvelle ère technologique devinrent rapidement très nombreux. Parmi eux, certains se rendirent compte qu'avec un ordinateur et une ligne téléphonique, il était plus ou moins aisé de partir à la rencontre d'autres ordinateurs connectés. L'industrie américaine du cinéma ne perdit pas de temps et produisit rapidement quelques films précurseurs dont certains, et notamment un, deviendront un modèle pour les jeunes informaticiens.

En effet, le film *Wargame* racontait l'histoire d'un adolescent, passionné d'informatique, ayant réussi à pénétrer les systèmes du Commandement de l'Armée de l'air américaine. Cette histoire, totalement réaliste, est le reflet des cauchemars des services de sécurité des armées du monde entier, car l'issue de cet exploit technique aurait pu être dramatique et engendrer une guerre nucléaire, uniquement en raison d'une défaillance informatique. Le constat était toutefois irrémédiable : le piratage informatique était né.

Depuis, le piratage s'est multiplié, faisant de ces « génies » du cyberspace des ennemis publics, des criminels du troisième millénaire. Les raisons de ce phénomène n'ont pas toujours été clarifiées. Mais il semble qu'en raison de leur jeune âge, ces experts ont plus souvent été attirés par le défi lancé à la société que par un but lucratif. Il faut cependant opérer une distinction entre ces « nouveaux guerriers »<sup>82</sup>, notamment entre les *Hackers* et les *Crackers*.

Les premiers sont considérés comme n'ayant aucune intention délictuelle ou criminelle. Leur activité repose sur le fait de s'introduire, par le biais d'une ligne téléphonique, dans un ordinateur distant. Comme nous l'avons observé, il s'agit ici d'un jeu (comme s'il s'agissait d'un jeu vidéo) ou d'un défi. Leur jeu n'est cependant pas ouvert au premier venu. Avant de percer les systèmes qui deviendront leurs victimes, à l'instar des casseurs de code dont nous avons parlé en matière de cryptographie, ils devront approcher leur cible et comprendre la logique de la protection informatique. Ce travail sera d'autant plus difficile que leur cible aura mis en œuvre des moyens défensifs. En effet, l'intérêt est très réduit de s'attaquer à un système sans défense. C'est ainsi que leurs principales victimes sont des puissantes sociétés commerciales, des organismes militaires ou des services de renseignement<sup>83</sup>. S'ils réussissent, leur action ne pourra que les hisser à un niveau supérieur dans la hiérarchie virtuelle des pirates informatiques, car ce qu'ils recherchent, au-delà de l'aspect ludique, est sans doute la reconnaissance de leurs pairs.

Les autres pirates informatiques, les *Crackers*, sont moins attirés par le caractère ludique de l'action. Ils ont détourné les techniques développées par les *Hackers* à des fins plus matérielles. Ceux d'entre eux considérés comme les « agressifs » agissent par vengeance personnelle ou professionnelle, notamment dans le cas de l'employé licencié laissant un virus ou une bombe logique dans la mémoire de l'ordinateur de son ancienne entreprise. Ils peuvent également agir dans des buts stratégiques, idéologiques, terroristes ou cupides comme le précise la classification établie par le Service central de sécurité des systèmes d'information (organisme gérant, en France, l'ensemble des dossiers d'agrément concernant la cryptologie et chargé de la sécurité de réseaux civils comme Internet<sup>84</sup>). Les

---

<sup>82</sup> GUISEL (J.), *Les nouveaux James Bond se branchent sur Internet*, Historia, n°602, Février 1997, p.66.

<sup>83</sup> Le ministère de la Défense américain admit avoir subi près de 200.000 attaques en 1995.

<sup>84</sup> GUISEL (J.), *Guerres dans le cyberspace*, La Découverte – Enquêtes, Paris, 1995, p.66-67.

services de renseignement ont vite compris l'intérêt de ces génies en herbe, notamment en ce qui concerne le « cracking » stratégique. Dans ce cas, les *Crackers* vont tenter de découvrir, dans les systèmes d'organismes gouvernementaux, ou autres, des renseignements de natures diverses : militaires, industriels ou diplomatique. Ils peuvent aussi essayer d'attenter au fonctionnement des systèmes d'information de ces Etats, comme ce fut constaté pendant le conflit du Kosovo. Des attaques provenant de Serbie avaient ainsi directement visé les systèmes informatiques des pays alliés. Pour déstabiliser ainsi les utilisateurs du réseau, ces pirates (ou corsaires, tout dépend du point de vue duquel nous nous plaçons) ont des techniques dérivées de deux principes : tout système comporte au moins une faille et quiconque y a accès peut les découvrir. A partir de ces affirmations il est possible de mettre en œuvre des actions connues sous le nom de déguisement, fouille, salami, cheval de Troie ou, crime parmi les crimes, le virus transportant une « bombe logique ».

Les exemples de recrutement de ces talents par les services spéciaux sont assez nombreux. Le service français de contre-espionnage, la DST, avait même créé un club destiné à attirer des pirates afin de mieux les contrôler et d'utiliser leurs compétences dans des missions « plus honorables »<sup>85</sup>. Pourtant dans ce domaine aussi la loi existe et la guerre que se livrent les services de police spécialisés (Police judiciaire contre service de renseignement) ne peut que contribuer à rendre moins évidente la pratique de ces illégalités.

## §2- Les protections contre les attaques informatiques

Le projet du Nouveau Code Pénal<sup>86</sup> avait prévu l'incrimination distincte d'un certain nombre d'attaques informatiques. Ainsi en était-il de :

- **L'accès frauduleux à un programme** : « *le fait de capter frauduleusement un programme, une donnée ou tout autre élément de traitement automatique d'informations est puni de trois ans d'emprisonnement et de 1 000 000 F d'amende* ».

---

<sup>85</sup> Le CCCF : Chaos Computer Club de France. Créé à l'image du CCC allemand soupçonné d'être manipulé par le KGB, le CCCF fut, au début des années 90 très médiatisé et attira rapidement les meilleurs pirates français.

<sup>86</sup> In projet de nouveau de code pénal n°215 J.O. du Sénat 15 février 1989.

- **L'espionnage informatique** : *« le fait, au mépris des droits d'autrui, d'utiliser, de communiquer ou de reproduire un programme, une donnée ou tout autre élément d'un système de traitement automatique d'informations est puni de trois ans d'emprisonnement et de 1 000 000 F d'amende ».*
  
- **Le sabotage informatique** : il se caractérise par l'utilisation d'une « bombe logique » et permet de détruire totalement ou de rendre inutilisable la mémoire d'un ordinateur, ou de fausser le traitement, en altérant une donnée ou un élément de programme : *« le fait, intentionnellement et au mépris des droits d'autrui, de détruire ou d'altérer tout ou partie d'un système de traitement automatique d'informations, ou d'en entraver ou fausser le fonctionnement, est puni de cinq ans d'emprisonnement et de 2 500 000 F d'amende ».*

Mais finalement, les parlementaires préférèrent conserver les dispositions de la loi Godfrain du 5 janvier 1988. Relative à la fraude informatique, cette loi avait donné naissance à un certain nombre d'articles du Code Pénal, encore en vigueur aujourd'hui, dans le NCP. Un de ces articles incrimine très clairement la notion d'infraction en matière informatique, l'article 323-1 : *« le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende ».* Ce n'est pas la prise de connaissance de l'information détournée que ce texte réprime, mais l'accès ou le maintien frauduleux dans le système automatisé. Ce texte concerne de ce fait un « système de traitement automatisé » et non pas un « système de traitement de l'information » comme ce fut prévu dans le projet de loi Godfrain. Mais les termes finalement choisis permettaient une interprétation plus large, c'est à dire capable de viser non seulement le simple ordinateur d'un particulier, mais aussi tout les réseaux existants ou futurs.

En outre, une fois le système automatisé atteint, le pirate tente en général d'accéder et d'altérer les données contenues dans le système et le système en tant que tel, infractions également sanctionnée par le Code Pénal. Ainsi l'article 323-1 sanctionne l'atteinte aux données en précisant que *« la suppression ou la modification de données contenues dans le*

*ystème* » est une circonstance aggravante de l'accès ou du maintien frauduleux dans un système de traitement automatisé de données. De plus, les législateurs ont décidé de faire de l'atteinte aux systèmes une infraction à part car il est tout à fait possible d'atteindre le système sans accéder aux données, et inversement. L'article 323-1 condamne, à ce titre, l'atteinte aux systèmes, également en tant que circonstance aggravante.

C'est ainsi que les articles provenant de la loi Godfrain de 1988, dans son ensemble, ont eu un effet dévastateur à l'encontre des pirates informatiques et de leurs groupes (NICK, Hardcore Hackers, Piratel, TeKila Underground etc.<sup>87</sup>). Mais au-delà de l'éviction de la scène des groupuscules de « cyber-rebelles », tous les textes que nous avons relevés dans cette partie, participent à une meilleure protection des libertés publiques qui semblent, chaque jour, être mises en danger à mesure que la technologie progresse. Pourtant le rôle des services de renseignement est d'accomplir, en toute discrétion, des actions de recherches d'informations, souvent au moyen de techniques sophistiquées, et donc au détriment d'une certaine idée de la liberté. La question se pose alors de savoir si nous voulons participer à un système de surveillance globalisé, sans égard à l'application des lois, à la manière des pays d'essence totalitaire, ou si, au contraire, il est possible de concilier la nécessité de garantir la sécurité d'une nation avec les exigences d'une société démocratique. Ceci ne devrait pas être impossible, notamment en instaurant un minimum de contrôle démocratique des activités de renseignement.

---

<sup>87</sup> GUISEL (J.), *Guerres dans le cyberspace*, La Découverte – Enquêtes, Paris, 1995, p.88.

## **CHAPITRE 2- L'ACCENTUATION DU CONTROLE DEMOCRATIQUE DES SERVICES SPECIAUX**

La question du contrôle démocratique des services de renseignement pose le problème de l'intégration de ces derniers dans la vie démocratique d'un Etat. Certains pourront arguer du fait que, par nature, un service dit secret doit rester secret, et qu'en conséquence il ne doit pas y avoir le moindre droit de regard, de la part du parlement ou de diverses commissions, à son égard. Ainsi clameraient-ils que « *les services secrets ne peuvent s'accommoder de la transparence démocratique* »<sup>88</sup>. Mais une telle affirmation n'est, selon nous, pas lucide.

En effet, il faut garder à l'esprit que les budgets des services de renseignements sont votés par les différents parlements, représentant le peuple. Or la sécurité d'un Etat équivaut à assurer la sécurité de ses citoyens. Ces derniers ont donc le droit d'exercer, à travers l'action de leurs représentants, un contrôle sur les activités de renseignement comme sur n'importe quel autre organe étatique. La démocratie est fondée sur la transparence, notamment celle de l'utilisation des deniers publics. Si l'utilisation des fonds spéciaux échappe effectivement au contrôle démocratique, ils ne constituent toutefois qu'une part infime des budgets octroyés aux services de renseignement. Certaines grandes nations démocratiques ont dores et déjà démontré qu'il était possible de contrôler les activités de ces services, sans pour autant porter atteinte à la sécurité du pays.

### **Section 1- L'étendue du contrôle dans les principales démocraties**

Le contrôle des activités d'espionnage dans les différents pays que nous allons traiter, a fait, en partie, l'objet d'un rapport de la Commission de la Défense nationale et des forces armées, tendant à la création d'une délégation parlementaire pour les affaires de renseignement<sup>89</sup>.

---

<sup>88</sup> BRUNOT ( P.), *Le contrôle parlementaire des politiques de renseignement*, Défense Nationale, février 1997, p.55.

<sup>89</sup> PAECHT (A.), *Rapport sur la proposition de loi tendant à la création d'une délégation parlementaire pour les affaires de renseignement*, n°1951, novembre 1999, 99p.

## §1- L'application d'un stricte contrôle aux Etats-Unis

Le rôle des services secrets américains a été essentiel pendant la guerre froide. Leurs actions ont permis de concentrer leurs efforts principalement vers l'Union Soviétique. Pourtant, la nécessité de préserver le secret de leurs activités n'a pas empêché les Etats-Unis de mettre en place le système de contrôle parlementaire des affaires de renseignement le plus contraignant au monde.

Les liens entre les services spéciaux et le parlement américain ont été institutionnalisés dès l'origine, mais il ne s'agissait pas encore d'un véritable contrôle parlementaire. C'est ainsi qu'en 1947, lors de la création de la Central Intelligence Agency (CIA), a été décidée la mise en place d'un conseiller législatif chargé d'instaurer des relations entre l'Agence et les représentants élus, en plus des quelques contacts établis entre le directeur de la CIA et certains membres du Congrès. Il existait en outre un certain nombre de commissions, aussi bien à la Chambre des représentants qu'au Sénat, compétentes dans ce domaine : celles de Finances et des Forces armées. A cette époque, les représentants américains ne jugeaient pas utile de s'immiscer, trop en profondeur, dans les affaires de la CIA. Certains événements majeurs vont cependant remettre en cause ces relations de bon voisinage.

En effet, la guerre du Vietnam, et les négociations soviéto-américaines concernant les installations anti-missiles, vont amener les élus à réclamer beaucoup plus d'informations aux services concernés, en raison, notamment, de leurs prérogatives en matière de politique étrangère. Le vote du budget (colossal) de l'ensemble de la communauté du renseignement par les représentants, dans le cadre du programme national de renseignement extérieur, mis en place par le Président Nixon, va également amener les élus américains à mieux connaître les activités des services bénéficiaires<sup>90</sup>. Les premières mesures législatives tendant à instituer un véritable contrôle datent de 1974, suite aux révélations des actions litigieuses de la CIA au Chili<sup>91</sup>. Ainsi l'Amendement Hughes-Ryan précisait que les actions clandestines

---

<sup>90</sup> Le budget annuel de la communauté américaine du renseignement avoisine, de nos jours, les 30 milliards de dollars, soit environ 200 milliards de francs français.

<sup>91</sup> Le Chili, pays d'Amérique du Sud, et donc considéré comme chasse gardée des Etats-Unis, avait fait l'objet à l'époque de pénétrations de l'appareil d'Etat par des éléments communistes, ce que les américains n'ont pas accepté.

de la CIA, afin d'être autorisées, devaient être jugées indispensables pour la sécurité du pays par le Président, ce dernier devant, pour sa part, en informer les Commissions du Congrès traitant des affaires de renseignement. C'est ensuite en Février 1976 qu'est publié l'*Executive Order* n°11905. Il s'agit du premier décret encadrant les activités de renseignement et imposant un certain nombre de limites. Cette même année est créée la *Senate Select Committee on Intelligence* (SSCI) commission spéciale permanente du Sénat. En 1977, la chambre des Représentants crée à son tour une commission spéciale, le *House Permanent Select Committee on Intelligence* (HPSCI). Avalisées par une loi sur le contrôle du renseignement de 1980<sup>92</sup>, ces deux commissions sont à l'heure actuelle les principaux organismes chargés des autorisations et de la supervision des activités des services spéciaux<sup>93</sup>.

L'étendue des pouvoirs des deux principales commissions, la SSCI et le HPSCI, est identique. Elles ont le pouvoir de diligenter des enquêtes et de conduire des audits en rapport avec les actions de renseignement, et dont le déclenchement peut être dû à des éléments aussi divers que des révélations dans la presse, dans certains rapports du service interne de contrôle de la CIA ou provenant de confessions d'anciens agents. Les moyens mis à la disposition de ces commissions ne sont pas négligeables puisqu'elles ont accès à des informations très confidentielles et peuvent en faire un usage libre, sans toutefois risquer de porter atteinte à la sécurité du pays. La loi précitée de 1980 impose, en outre, aux services spéciaux de «*fournir toute information et/ou toute preuve matérielle concernant les activités de renseignement*»<sup>94</sup>. Le danger provient du fait que certaines informations peuvent avoir un caractère très sensible. Ceci a poussé à créer, au sein de ces commissions, des formations restreintes, composées de personnalités ayant déjà eu à traiter des affaires confidentielles. De même, les travaux effectués au sein de ces commissions sont entourés de strictes mesures de sécurité, et tout le personnel administratif travaillant dans ces organismes de contrôle est soumis aux enquêtes d'habilitation du service fédéral de sécurité, le Federal Bureau of Investigation (FBI).

---

<sup>92</sup> *Intelligence Oversight Act*.

<sup>93</sup> Deux autres commissions sont chargés du contrôle de ces activités : les commissions de la défense et des Affaires Judiciaires et des Affaires étrangères.

<sup>94</sup> PAECHT (A.), *op.cit*, p.22.

Une fois l'enquête achevée, les membres des commissions procèdent à un vote synthétisant la solution proposée en cas de litige, celle-ci étant préparée avec l'aval du Président de l'exécutif. Les commissions rédigent aussi régulièrement des rapports d'activités, ou même des projets de loi concernant les différents services composant la communauté du renseignement.

Nous avons vu à quel point les Etats-Unis possédaient des moyens importants en matière de contrôle des services secrets. Leur « petit-frère » d'outre-Atlantique possède également des moyens de contrôle en dépit d'une tradition de fermeture hermétique concernant les affaires d'espionnage<sup>95</sup>.

## §2- La révolution britannique

Cette fermeture se vérifie par la date, très tardive, consacrant les premiers pas vers le contrôle des services secrets. Ce fut cependant considéré comme une révolution. C'est, en effet en 1994 qu'une loi, l'*Intelligence Services Act*, a autorisé la création d'une commission sur le renseignement et la sécurité, l'*Intelligence and Security Committee* (ISC). Ses neuf membres, provenant des principaux partis politiques britanniques, et nommés par le Premier ministre, sont majoritairement issus de la Chambre des Communes (élus). Si cette commission est composée de parlementaires, elle n'est pourtant pas considérée comme étant une commission parlementaire classique car ses membres sont désignés par le pouvoir exécutif. Quelques opinions divergentes ont évoqué le fait qu'il ne pouvait s'agir d'une commission indépendante, respectant le principe de séparation des pouvoirs, puisque ses membres dépendaient de l'exécutif<sup>96</sup>. Il semble pourtant que les orientations prises aient été établies dans un souci de préservation totale du secret entourant les investigations, garantie présumée plus forte dans le cas présent de nomination des membres par le destinataire de toutes les informations recueillies secrètement, c'est à dire le Premier ministre.

Les travaux de cette commission sont assez limités puisqu'ils se limitent à examiner le budget, l'organisation et la ligne de conduite générale des différents services. Pour

---

<sup>95</sup> Les services de sécurité intérieure de renseignement extérieur et des écoutes, le MI5, le MI6 et le GCHQ, n'ont été reconnus officiellement qu'en 1989, 1992 et 1994.

<sup>96</sup> PAECHT (A.), *op.cit*, p. 35.

effectuer ce travail, les membres ont cependant accès à un certain nombre d'informations sensibles. Une classification particulière à l'ISC a été établie. Contrairement à la traditionnelle distinction entre information confidentielle ou non, il a été mis en place une distinction relative au caractère sensible ou non de l'information, évitant ainsi de passer par une procédure d'habilitation des parlementaires, et leur permettant donc d'avoir accès aux renseignements plus ou moins sensibles.

Si certains pays anglo-saxons ont, malgré les réticences de certains, décidé de la participation du parlement dans le contrôle des organismes de renseignement, d'autres, tels que le Canada, n'ont pas encore réussi à réellement impliquer le parlement dans le suivi des activités de renseignement.

### **§3- Le faible contrôle du Parlement au Canada**

Le système canadien de contrôle a été mis en place dans les années quatre vingt, suite à un certain nombre de zones d'ombre entourant les services spéciaux<sup>97</sup>. Il fut décidé la création de plusieurs commissions d'enquêtes relatives aux faits reprochés. L'une d'entre elles, la commission fédérale Mc Donald proposa, dans ses conclusions, la mise en place de contrôle des activités de renseignement à plusieurs niveaux : l'exécutif, le judiciaire, le parlementaire et un quatrième niveau indépendant. Parmi ces quatre propositions, seules trois ont été retenues, en excluant l'intervention du parlement.

Le système canadien est assez complexe puisque les deux principales agences de renseignement du pays sont contrôlées par deux organismes distincts (Il existe un troisième service secret, le renseignement militaire, mais celui-ci ne fait l'objet d'aucun contrôle). Le service des écoutes fait l'objet de rapports de la part d'un inspecteur général indépendant mais appartenant au ministère de l'Intérieur. Le service de sécurité intérieure est encadré par un contrôle judiciaire et externe, ce dernier étant effectué par le comité de surveillance des activités de renseignement de sécurité, le CSARS. Ce comité indépendant n'abrite aucun parlementaire actif et emploie plutôt des universitaires. Bien que n'étant pas de nature

---

<sup>97</sup> La Gendarmerie Royale fut mise en cause dans un cambriolage à Montréal en 1972.

parlementaire, ses membres ont accès à un certain nombre de documents confidentiels. Ceci leur permet de présenter annuellement un rapport devant le Parlement.

Ce dernier est relativement absent de la procédure de contrôle. Bien qu'il existe un comité sénatorial spécial créé en 1998, les liens entre les services spéciaux et les deux Chambres sont assez faibles. De plus, comme le précisent les conclusions du rapport Paecht<sup>98</sup>, parler d'un contrôle parlementaire serait excessif puisque les sénateurs membres du comité spécial ne sont pas élus mais désignés, et ils ne peuvent être révoqués avant leur départ en retraite, à 75 ans. « *Par conséquent, aucun représentant de la souveraineté nationale n'intervient dans le processus* »<sup>99</sup>.

Si les contrôles parlementaires existent, de façon plus ou moins étendue, dans ces grandes démocraties, qu'en est-il en France ?

## **Section 2 - Vers une accentuation des contrôles des activités de renseignement en France**

La France n'est pas totalement dépourvue d'organismes de contrôle des activités de renseignement, mais ce ne sont à l'heure actuelle que des commissions indépendantes et non parlementaires, et dont les prérogatives ne concernent pas les services spéciaux en tant que tels, mais une partie des activités de certains d'entre eux.

### **§1- Les commissions de contrôle relatives au renseignement technique**

#### **A- La CNIL**

La Commission nationale de l'informatique et des libertés, nous l'avons évoquée plus tôt, a été mise en place par une loi du 6 janvier 1978, afin de prévenir les risques de dérapages en matière de fichiers informatiques, notamment dans les services de sécurité, et donc aussi les services spéciaux. Ainsi cette loi autorise-t-elle les agents de la CNIL à

---

<sup>98</sup> PAECHT (A.), *op.cit*, p.41.

<sup>99</sup> *idem*.

effectuer un certain nombre de vérifications de fichiers. Pour cela, ils ont accès à toutes les informations nominatives stockées sur un support informatique, y compris les fichiers relevant des « *traitements intéressants la sûreté de l'Etat, la défense et la sécurité publique* »<sup>100</sup>. Notons qu'ils doivent tout de même faire l'objet d'une habilitation du Premier ministre dans le cas où ils auraient à prendre connaissance de données classifiées<sup>101</sup>. De plus, leur travail est assuré d'une grande indépendance vis à vis du pouvoir exécutif et des administrations puisque l'article 21 de la loi de 1978 dispose que les ministres et les autorités publiques « *ne peuvent s'opposer à l'action de la commission ou de ses membres pour quelque motif que ce soit* ». Bertrand Warusfel souligne qu'il s'agit là d'un dispositif remarquable « *dans la mesure où il donne à la CNIL une prérogative vis-à-vis du secret de défense que la pratique administrative et contentieuse refuse à tous les magistrats, tant de l'ordre judiciaire qu'administratif* »<sup>102</sup>. Grâce au précédent créé par cette commission, il a été possible de mettre en place, quelques années plus tard, une autre autorité administrative chargée de contrôler les interceptions de sécurité.

## B- La CNCIS

La Commission nationale de contrôle des interceptions de sécurité a vu le jour avec l'article 13 de la loi du 10 juillet 1991 protégeant le secret des communications. Elle est chargée de veiller à l'application de cette loi de 1991 par les services pratiquant les interceptions, notamment afin d'observer si celles-ci entrent dans le cadre de l'article 3 de la loi, c'est à dire si elles ont pour « *objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien des groupements dissous [...]* ». Les moyens de cette commission, composée uniquement de trois membres<sup>103</sup>, sont assez importants puisqu'ils peuvent obtenir du Premier ministre qu'il leur transmette très vite toute décision de mise en œuvre d'une écoute. Cependant, la CNCIS ne peut adresser au Premier ministre qu'une simple recommandation visant à interrompre l'interception si elle

---

<sup>100</sup> Article 6, loi du 6 janvier 1978.

<sup>101</sup> Décret du 28 décembre 1979, article 3.

<sup>102</sup> WARUSFEL (B.), *Contre-espionnage et protection du secret*, Lavauzelle, Panazol, 2000, p.381.

<sup>103</sup> Un président choisi par le Président de la République, et deux parlementaires, issus de chacune des Chambres, et choisis par les présidents de chacune d'entre elles.

pense qu'une des dispositions de la loi de 1991 n'est pas respectée, l'exécutif conservant le pouvoir de suivre ou non la recommandation.

L'importance de la CNCIS se retrouve également dans le contenu des rapports établis annuellement, et dans lesquels elle émet un certain nombre d'avis défavorables concernant certaines interceptions. Ces avis sont la plupart du temps suivis par le Premier ministre.

La présence de telles commissions de contrôle des activités de renseignement ne peut être que bénéfique pour un pays démocratique. Mais comme le faisait remarquer le chancelier du duché de Lancaster au Royaume-Uni, William Waldegrave, « *il n'est pas possible de qualifier le régime juridique français du contrôle de la politique du renseignement, car il n'existe pas. La France et les Etats-Unis se trouvent aux deux extrêmes de l'échelle* »<sup>104</sup>. Le constat est assez brutal, mais hormis les commissions que nous venons d'évoquer, il est vrai que le contrôle parlementaire des services secrets n'est pas encore né en France.

## **§2- L'inexistence d'un véritable contrôle parlementaire en France**

La France n'a, sans doute pour des raisons culturelles, jamais établi de véritable contrôle parlementaire relatif aux activités de ses services spéciaux. Il existe pourtant un mécanisme, constitutionnellement prévu, permettant de réunir chaque Assemblée en comité secret, permettant ainsi au Gouvernement d'informer le Parlement sur des questions sensibles. Ainsi en est-il avec l'article 33 de la Constitution de 1958 disposant que « *chaque Assemblée peut siéger en comité secret à la demande du Premier ministre ou d'un dixième de ses membres* »<sup>105</sup>. Mais il faut bien constater que cette procédure n'a été utilisée que très rarement<sup>106</sup>. Il n'est toutefois pas interdit aux parlementaires de poser des questions au

---

<sup>104</sup> BRUNOT ( P.), *Le contrôle parlementaire des politiques de renseignement*, Défense Nationale, février 1997, p.62.

<sup>105</sup> Les règlements intérieurs de l'Assemblée Nationale et du Sénat prévoient cette éventualité respectivement dans les articles 51 et 32.5.

<sup>106</sup> C'est en 1976, pour la dernière fois, qu'un parlementaire a évoqué la possibilité de convoquer l'Assemblée Nationale en comité secret.

Gouvernement lors des séances publiques. Cela étant, les ministres ont la possibilité d'éluder une question qu'ils jugent contraires à l'intérêt public<sup>107</sup>.

Au-delà de ces constats, il existe une réticence des responsables politiques à informer une assemblée parlementaire sur des questions relatives aux problèmes de sécurité, en raison, apparemment, du peu de confiance accordée à nos représentants en matière de divulgation de secrets. Pourtant, des pays comme les Etats-Unis n'ont pas hésité à ouvrir ces questions aux parlementaires, en prenant bien sûr la précaution de protéger les secrets susceptibles d'être dévoilés.

Il semble pourtant que les mentalités soient en train d'évoluer en France puisque, sous l'impulsion de certains députés, a été proposée la création de délégations parlementaires pour les affaires de renseignement<sup>108</sup>, présente dans chacune des deux assemblées. La commission de la Défense Nationale et des forces armées avait été pressentie pour avoir à connaître des questions de renseignement, mais le droit commun parlementaire ne permet pas aux représentants élus d'avoir accès à des informations classifiées. Le rapport PAECHT affirme que la seule solution, pour contrer ce problème, serait de créer une délégation, comme il en existe déjà un certain nombre, tant à l'Assemblée Nationale qu'au Sénat<sup>109</sup>.

Les effectifs de ces délégations autonomes seraient assez restreints en raison du caractère confidentiel de leurs travaux, à condition de « *prendre en compte l'équilibre politique général de l'assemblée concernée* »<sup>110</sup>. Leurs différentes tâches seraient de « *suivre les activités des services visés à l'article 13 de l'ordonnance n°59-147 du 7 janvier 1959 portant organisation générale de la défense, en examinant leur organisation et leurs missions générales, leurs compétences et leurs moyens, afin d'assurer, dans les conditions prévues au présent article, l'information de leur assemblée respective* »<sup>111</sup>. Toute la communauté française du renseignement est donc concernée par ce texte. Pour accomplir

---

<sup>107</sup> Article 139-3 du règlement de l'Assemblée Nationale ; article 75-2 du règlement du Sénat.

<sup>108</sup> PAECHT (A.), *Rapport sur la proposition de loi tendant à la création d'une délégation parlementaire pour les affaires de renseignement*, n°1951, novembre 1999, 99p.

<sup>109</sup> Délégations pour l'Union européenne, pour les problèmes démographiques, pour les droits des femmes, etc.

<sup>110</sup> PAECHT (A.), *op.cit.*, p.53.

<sup>111</sup> Proposition de loi pour la création de délégations parlementaires pour les affaires de renseignement, in Rapport PAECHT, p.70 : article premier, paragraphe n°IV.

leurs travaux dans les meilleures conditions, la proposition de loi prévoit que les membres des délégations pourront avoir accès à des informations classifiées, après avoir été habilités à qualité, c'est à dire qu'ils sont soumis, malgré leur statut de parlementaire, aux dispositions du code pénal inhérentes au secret de défense et au secret professionnel (articles 413-9 et 226-13 NCP). Rien ne précise toutefois la nature des informations sensibles auxquelles ils auront accès. Toujours est-il qu'un progrès important sera effectué lorsque cette proposition de loi sera concrétisée par un vote du Parlement.

Les limites à l'efficacité d'un système de renseignement, fondé principalement sur le recueil technique d'informations, s'avèrent de plus en plus manifestes. Un certain nombre de spécialistes des affaires de renseignement s'interrogent sur l'efficacité et la légitimité de ce type d'espionnage.

Les menaces ont changé de costumes depuis le jour où Leningrad est devenu Saint Petersburg et, de par leur caractère diffus, inquiètent toujours les centrales de renseignement. Mais hormis le fait que le renseignement technique apporte des informations souvent utiles, un facteur essentiel a été mis sur la touche depuis quelques années : l'Homme. Tant au niveau de l'approche qu'il a du renseignement, que de l'acquisition de ce dernier, l'Homme reste, à ce jour, un élément capital.

**PARTIE 2<sup>EME</sup>**

-

**LA NECESSAIRE PRESENCE DE L'HOMME  
DANS LE CYCLE DU RENSEIGNEMENT**

Ainsi que nous pourrions l'observer dans notre développement, de nombreux éléments laissent à penser que les services de renseignement, actuels et futurs, n'ont aucune raison d'abandonner leurs activités passées, au prétexte que la situation internationale n'est plus marquée par le probable déclenchement d'une guerre thermonucléaire entre le Pacte de Varsovie et les membres de l'OTAN. Si les fusées intercontinentales des puissances respectives ne sont plus, officiellement, pointées sur les capitales « ennemies », il n'en reste pas moins vrai que les tensions entre puissances sont encore vives. De même, la guerre froide a certainement contribué à occulter les nombreux autres affrontements existant.

Mais aujourd'hui, ces derniers ont soudainement fait surface, et posent des problèmes nouveaux. Il ne s'agit plus d'étudier une multitude de situations dans un type d'affrontement particulier et unique (crainte d'une attaque militaire soviétique en Europe de l'Ouest), mais de gérer la meilleure réponse à une multitude de crises possibles. Il ne nous sera pas utile de développer et acquérir une armada invincible d'outils technologiques si nous ne pouvons pas les orienter correctement vers les missions pour lesquelles ils peuvent être utiles. Dans ces conditions, il s'agit pour les décideurs politiques et les stratèges du renseignement, de mieux repenser leurs objectifs et leur façon de considérer le renseignement (Titre 1<sup>er</sup> ) car certaines des nouvelles menaces auxquelles nous devons faire face ne peuvent être combattues que par des moyens principalement humains. C'est en cela que nous devrions essayer de véritablement réhabiliter la recherche humaine des informations sur le terrain (Titre 2<sup>ème</sup> ), les moyens techniques ayant montré leurs limites.

## **TITRE 1<sup>ER</sup>. UNE MEILLEURE APPROCHE DES ACTIVITES DE RENSEIGNEMENT**

Le travail de renseignement ne se limite plus seulement à élaborer des moyens ultra sophistiqués d'acquisition du renseignement. Ces derniers ne se montreront pas très utiles si personne n'est en mesure d'élaborer une bonne politique coordonnée de recherche de l'information (Chapitre2). Il n'est en effet pas question de tout savoir en temps réel, mais de savoir à temps tout ce qui est réellement important. Pour cela, il est important de redéfinir les objectifs essentiels à la sécurité de l'Etat (Chapitre1).

### **CHAPITRE 1- LA REDEFINITION DES OBJECTIFS**

Les questions ont été nombreuses au lendemain de la chute du mur de Berlin. Certes, le « diable » combattu pendant tant d'années avait soudainement disparu. Mais les services de renseignement n'ont pas été dissous pour autant. Au contraire, certains d'entre eux voient leur budget croître d'année en année, et leurs responsables s'aperçoivent tous les jours davantage qu'ils manquent d'informations importantes concernant les nouvelles préoccupations de l'après-guerre froide (Section1). Afin d'assurer une meilleure efficacité dans leur quête du renseignement, les « combattants de l'ombre » devraient avoir pour autre objectif, essentiel, de construire une véritable culture du renseignement totalement décomplexée, à l'image de ce qui existe dans de nombreuses autres démocraties (Section2).

#### **Section 1- Les récents bouleversements géopolitiques**

Depuis quelques années, les principaux services de renseignement ont entrepris d'importantes restructurations. En effet, les observateurs de la scène internationale constatent globalement une multiplication, non pas des menaces, mais des risques susceptibles de toucher les Etats. La situation était finalement beaucoup plus limpide à l'époque où les russes et les occidentaux menaient, dans l'ombre, une guerre qui ne fut

jamais déclarée officiellement. Aujourd'hui, personne ne peut réellement affirmer avec précision où se situe le danger. Celui-ci s'est éparpillé, portant certainement en lui les traces du passé. Mais il a su s'adapter à notre époque.

### **§1- L'apparition d'une notion nouvelle : la guerre économique**

L'idéologie de l'économie de marché a eu raison de la guerre froide, et la logique de planification économique n'a pu se résoudre qu'à déposer les armes près des vestiges du colosse aux pieds d'argile, c'est à dire à terre. Pourtant la guerre n'est pas finie. Certes les militaires ont bien été obligés de repenser leur stratégie, ne sachant plus déterminer avec précision un adversaire. Mais ce sont d'autres guerriers des temps modernes qui sont apparus : les acteurs économiques. Paradoxalement, une véritable guerre économique globale a pris le relais, sans aucune déclaration préalable.

Comme dans toute guerre, les belligérants doivent s'informer. Pour cela, les entreprises ont engagé des stratégies diverses, mais dont la finalité reste la même : éliminer tous les obstacles susceptibles de freiner la progression. La notion d'intelligence économique est apparue récemment, même si les entreprises y ont toujours eu recours, sans parfois même le savoir. La différence est qu'aujourd'hui, on a fait de ce concept un véritable outil de guerre. Certains auteurs définissent ainsi ce concept : « *c'est un outil capable de détecter des menaces et des opportunités de toute nature dans un contexte de concurrence exacerbé* »<sup>112</sup>. Or pour détecter, il faut se renseigner. Mais parfois certaines entreprises se montrent très curieuses, et franchissent la ligne jaune de la légalité.

Un journaliste intitulait en 1993 son étude sur les méfaits de l'intelligence économique : « Le grand pillage de la France »<sup>113</sup>. Le titre ne peut laisser insensible car la France, comme beaucoup d'autres pays, est une des principales victimes du côté sombre de l'intelligence économique : l'espionnage économique et industriel. Les coûts en recherche et développement sont extrêmement élevés. En les économisant, une entreprise devient automatiquement plus compétitive que sa concurrence. Les soviétiques, à l'époque de la guerre froide (et certainement de nos jours encore), se sont souvent montrés gourmands en

---

<sup>112</sup> BESSON (B.), POSSIN (J.-C.), *Du renseignement à l'intelligence économique*, Dunod, Paris, 1996

<sup>113</sup> PONTAUT (J.-M.), *Le Point*, 6 novembre 1993

matière d'acquisition frauduleuse de secrets industriels. Ainsi dans les années 80 ont-ils acquis des renseignements technologiques dans le domaine de l'optronique (observation nocturne), des transmissions, des lasers (technologie des miroirs), des matériaux à base d'alliages de titane, et bien d'autres encore<sup>114</sup>. Cela dit, il ne faut pas seulement jeter la pierre aux soviétiques. Tous les pays ont été, et sont encore, impliqués dans des opérations d'espionnage industriel. La différence est que désormais ce ne sont plus exclusivement les services de renseignement qui ont la charge d'effectuer ce genre particulier de recherches. Nous assistons depuis peu à une privatisation de l'espionnage industriel. De même chaque grande entreprise possède son petit groupe de recherche de l'information ouverte. Toujours est-il que la place de l'Homme dans le monde du renseignement économique est prépondérante. Les entreprises ne sont pas toutes en mesure d'envoyer des satellites dans l'espace afin d'intercepter les communications de leurs concurrents. En outre, il existe une multitude d'informations ne pouvant être obtenues que par l'intermédiaire de l'Homme, notamment dans les expositions commerciales, les réunions regroupant un certain nombre de décideurs économiques, les entreprises mêmes ou encore par l'intermédiaire de stagiaires-espions dont les pays asiatiques sont devenus les premiers exportateurs au monde.

## **§2- Les risques émergents en matière de sécurité**

Malgré le fait que l'espionnage économique représente aujourd'hui la majorité des activités des services de renseignement, de nouveaux types de risques sont apparus. Ils sont de natures différentes, et engagent non seulement des Etats mais aussi, et chaque jour davantage, des éléments « privés », sans aucun lien apparent avec un quelconque Etat.

Pour les premiers, les exemples sont nombreux. Dès la fin de la guerre froide, une multitude de conflits firent leur apparition et engagèrent massivement les armées ainsi que les services de renseignements occidentaux. La guerre du Golfe, la guerre civile en Algérie, la guerre menée par les russes en Tchétchénie, la crise indo-pakistanaise, les conflits ethniques en Afrique et d'autres encore, sont des risques potentiels pour les puissances occidentales, sans doute pas pour l'intégrité de leur territoire, mais davantage en ce qui concerne leurs intérêts économiques. De plus, le continent européen a montré qu'il n'était

---

<sup>114</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, p.423

pas exempt de crises dignes d'une autre époque. Personne ne pouvait croire que des crimes contre l'Humanité pouvaient encore être perpétrés « à deux heures d'avion de Paris ». Pourtant, les faits ont prouvé le contraire. En outre, personne ne peut prédire, à l'heure actuelle, ce qu'advieront les différentes minorités en Europe : les bulgares, les roumains, les hongrois, etc. Mais d'autres inquiétudes sont apparues aux yeux des services de sécurité. Elles ne sont pas directement liées à des Etats, mais sont davantage le signe d'une manifestation anarchique au sein des relations internationales, échappant de plus en plus au contrôle des Etats, tout en mettant en cause leur sécurité.

En premier lieu, il est question de prolifération nucléaire. Cette crainte de voir des armements de destruction massive se développer dans le monde est un danger permanent. Elle peut être due à la perte de contrôle d'ogives<sup>115</sup> ou de composants nécessaires à l'élaboration d'une arme nucléaire, mais aussi à la migration de scientifiques, notamment russes, vers des Etats ou des groupuscules terroristes peu soucieux des conséquences catastrophiques qu'engendreraient leur utilisation. Il ne faut cependant pas omettre les risques concernant les armes de type chimique ou bactériologique. Facilement transportables et dissimulables, ces armes ont déjà été utilisées par des groupes terroristes. Le Japon en fut une des premières victimes<sup>116</sup>.

Le terrorisme est également devenu un fléau majeur pour les Etats (cet état de fait nous a été brutalement remis à l'esprit le 11 septembre 2001). Selon une classification des services de contre-espionnage français, il existerait quatre types de terrorisme<sup>117</sup> susceptibles de porter atteinte à la stabilité de l'Occident: le terrorisme interne d'essence nationaliste (breton, corse, basque); le terrorisme d'extrême droite dirigé contre certaines minorités ethniques (l'Allemagne est de nouveau victime d'attentats à l'encontre de minorités turques et juives); le terrorisme d'Etat provenant de pays connus pour leur politique de soutien aux groupuscules islamistes et le terrorisme lié à la question palestinienne. Les terroristes se sont également modernisés. Ils utilisent les techniques les plus pointues en matière de communication: téléphones satellitaires et Internet. De même,

---

<sup>115</sup> Il s'agirait plutôt de la perte d'ogives tactiques, moins encombrantes que les armes stratégiques.

<sup>116</sup> Attentat au gaz Sarin dans le métro de Tokyo.

<sup>117</sup> Classification reprise dans CAPPELLE (F.), *Le monde du renseignement de l'An 2000: restructuration des services et nouveaux enjeux*, Mémoire de DEA Défense Nationale et sécurité européenne, Université Lille II, 1998-1999, p.31.

ils n'éprouvent plus le besoin de revendiquer leurs méfaits, accroissant ainsi la crainte des populations et laissant aux services de sécurité des zones d'ombre plus importantes qu'autrefois. Cette évolution se traduit aussi dans les mafias.

Phénomène inquiétant depuis quelques décennies, les mafias se sont encore développées ces dernières années. Une des mafias les plus médiatisées, la sicilienne<sup>118</sup>, doit désormais partager le « marché » du crime organisé avec de nouveaux concurrents venus de l'ancienne Union soviétique, de l'Albanie, du Japon ou de la Chine. Le problème de ces groupements criminels vient du fait qu'ils tentent d'influencer et de pénétrer, de manière plus ou moins légale, les diverses institutions d'un pays, notamment au niveau financier, économique et parfois politique, comme ce fut le cas en Italie. Ces multinationales du crime bénéficient, en plus de réserves financières gigantesques, de la loi du silence d'une grande partie de la population (l'*omerta*), rendant difficile, voire impossible, leur déferrement devant les autorités judiciaires.

La lutte contre ces nouveaux fléaux ne peut pas se faire avec des moyens policiers classiques. Les services de renseignement le savent, et participent de plus en plus à la guerre discrète menée à l'encontre des organisations criminelles. Mais toutes les composantes de la société ne sont pas toujours sensibilisée par le danger que représentent ces « syndicats du crime » et le rôle essentiel du renseignement. Au delà de ces mafias, des groupuscules terroristes, des risques de prolifération, des actions d'espionnage venant de puissances étrangères, le problème majeur auquel se heurte les services de renseignement est certainement le désintérêt de la population, et des différents responsables politiques ou économiques, pour les affaires de renseignement, ceci étant particulièrement vrai en France. Il est donc nécessaire de construire une véritable culture du renseignement.

---

<sup>118</sup> En Sicile, la mafia se nomme *Cosa Nostra*. Mais il existe trois autres mafias en Italie : la *Camorra* en Campanie, la *Ndrangheta* en Calabre et la *Sacra Corona Unita* dans les Pouilles.

## **Section 2- La nécessaire construction d'une culture du renseignement**

### **§1- Une culture acquise dans de nombreux pays**

La culture du renseignement est une partie intégrante de notre esprit de Défense. Si le renseignement n'a plus d'objet strictement militaire, il en est de même pour les questions de Défense. Celles-ci sont devenues globales. Il n'est certes pas question d'abandonner les options relatives à la Défense de l'intégrité physique du territoire, mais les données ont évolué dans un sens plus économique que territorial.

Si les composantes d'une nation restent insensibles à l'esprit de Défense, il sera d'autant plus difficile de leur faire intégrer la notion de renseignement. Une trop grande majorité de français semble aujourd'hui réticente à cultiver cet esprit. Il n'est pourtant question que d'une manifestation de patriotisme et de civisme. Les pays anglo-saxons, entre autres, l'ont rapidement compris, et se sont vite décomplexés vis à vis des questions de Défense, et donc de renseignement. Il suffit de constater l'importance du budget américain consacrée à l' *intelligence community*, estimé à près de 30 milliards de dollars annuels, pour comprendre à quel point ils jugent cette activité essentielle. Bien sûr, les Etats-Unis tiennent le rôle d'hyper puissance au sein des relations internationales, et se doivent, à ce titre, d'être informés en permanence. Un pays dont le deuxième amendement de la Constitution accorde aux citoyens le « droit à détenir une arme » ne peut pas être hostile aux problèmes de Défense, même si elle se limite ici à la défense de la personne ou de la propriété. Cela étant, un tel budget ne peut être la conséquence que d'une longue maturation des esprits des responsables politiques, militaires et des représentants de la Fédération. Une des principales raisons de ce constat réside dans le fait que, dès le plus jeune âge, les américains sont confrontés aux questions de Défense.

Depuis leur intervention dans les conflits mondiaux et leur sortie d'un isolationnisme improductif, les Etats-Unis ont participé à la construction d'un ordre mondial, souvent décrié, mais dont les conséquences ont été la mise en place d'un véritable bouclier défensif de la zone occidentale face au bloc soviétique. Cela n'aurait toutefois pas été possible sans le soutien massif de la société civile américaine. En effet, les citoyens de ce pays reçoivent

très tôt une formation civique complète<sup>119</sup>, intégrant des matières relatives à la Défense. Il en est ainsi notamment avec le « Junior ROTC »<sup>120</sup>. Cet enseignement dispensé aux élèves du secondaire, dans les écoles acceptant ce programme, a été créé en 1916 et conçu pour « motiver les jeunes à devenir de meilleurs citoyens »<sup>121</sup>. Les sujets de cette formation sont très variés puisqu'ils évoquent tout aussi bien l'histoire de la Constitution américaine que l'histoire militaire ou la prévention anti-drogue. Le ministère de la Défense américain, le DOD<sup>122</sup>, prend en charge cet enseignement, notamment en le finançant. D'autres programmes scientifiques visant les élèves du secondaire sont préparés par le DOD dans le cadre de sa mission éducative : le « Naval Science Award », le « Junior Science and Humanities Symposia Program », etc. Il existe également un réseau d'écoles militaires privées du secondaire, les « Military Schools ». Des formations de ce genre sont également dispensées dans les universités publiques ou privées ainsi que dans les académies militaires des forces armées.

La culture du renseignement est également présente dans d'autres pays, notamment chez les deux « grands » défaits de la deuxième guerre mondiale, le Japon et l'Allemagne. Ruinés par le conflit, à l'instar de tous les acteurs du conflit, ces deux pays n'ont cependant pas eu le droit, durant un certain temps, de procéder à leur réarmement. Ils décidèrent alors de consacrer toute leur énergie à l'industrie et au commerce. En effet, le japonais, par exemple, est quelqu'un de curieux par nature, et parmi les nombreux clichés photographiques qu'il pourra prendre lors de ses nombreux voyages à l'étranger, certains pourront peut-être bénéficier à son employeur (en tout cas, ils ont une pensée qui va dans ce sens là). S'informer est un « devoir national » et l'acquisition de technologies à l'étranger est la conséquence de cette mentalité, ce qui ne leur a souvent conféré une réputation de tricheurs. En outre, il existe une véritable coopération entre acteurs économiques japonais, sous l'impulsion de leur ministère de l'Economie, entre autres. Ainsi, le fait de ne pas présenter une information intéressante peut être considéré comme une faute professionnelle, et un défaut de « patriotisme économique ».

---

<sup>119</sup> Tous les élèves américains, dès l'âge de 6 ans, récitent chaque matin le «pledge of allegiance» : «*je fais le serment de fidélité au drapeau des Etats-Unis et à la République qu'il représente, une nation sous la protection de Dieu, indivisible, offrant liberté et justice pour chacun* ».

<sup>120</sup> *Junior Reserve Officer Training Corps*.

<sup>121</sup> *National Defense Act* de 1916.

<sup>122</sup> Department Of Defense.

L'Allemagne est aussi un pays expérimenté en matière de renseignement économique. Nos voisins d'Outre-Rhin, en plus de leurs grandes connaissances techniques, ont depuis l'époque de Bismarck<sup>123</sup>, développé un système d'intelligence économique alimenté principalement en informations ouvertes, c'est à dire disponibles librement à celui qui veut bien se donner la peine d'être curieux. De plus, l'information obtenue est immédiatement traitée, classée dans des fichiers et des annuaires édités régulièrement, et mis à la disposition des entrepreneurs. Ainsi se tiennent-ils informés en temps réel sur l'évolution de leur concurrence, adaptant de ce fait leurs offres à la nouvelle demande. Ce système repose, en outre, sur tout un ensemble de capteurs sensibles au bon développement économique de leur pays, et ayant pignon sur rue dans le monde des affaires, c'est à dire les industriels et les financiers.

Il ne s'agit pas ici de renseignement de type politique, militaire ou diplomatique. Mais le Japon et l'Allemagne ont fait le choix de se concentrer sur le domaine économique. Leurs citoyens n'ont pas cette réticence française à l'égard des affaires de renseignement puisqu'ils savent qu'ils agissent pour un meilleur développement de leur pays. Cette culture du renseignement doit encore être développée en France

## **§2- Vers un changement de la mentalité française**

Le rapport PAECHT est très clair vis à vis de la défaillance culturelle française en matière de renseignement : *« Il n'existe pas aujourd'hui de véritable culture du renseignement en France, c'est à dire une démarche d'esprit globale et systématique incluant le renseignement dans la prise de décision politique »*<sup>124</sup>. D'autres études sur les services secrets français ont été très sévères à leur égard. Ainsi Douglas Porch<sup>125</sup> évoque-t-il une contradiction dans l'Histoire de France et les liens avec les services spéciaux. *« Compte tenu d'une histoire pleine de guerres, d'invasions, de responsabilités d'empire, on devrait logiquement conclure que, de tous les pays, la France est un de ceux où le renseignement a*

---

<sup>123</sup> Bismarck a décidé, au XIXème siècle de concurrencer la Grande Bretagne dans le domaine du commerce mondial.

<sup>124</sup> PAECHT (A.), *Rapport sur la proposition de loi tendant à la création d'une délégation parlementaire pour les affaires de renseignement*, n°1951, novembre 1999, p.11.

<sup>125</sup> Auteur américain considéré comme très sévère à l'égard de la communauté française du renseignement.

*joué un rôle central, décisif. Mais si ce rôle a bien été central, il a rarement été décisif* »<sup>126</sup>. Les raisons d'une telle défaillance se trouvent notamment dans le peu d'intérêt porté par les chercheurs français sur l'histoire du renseignement.

En effet, si les études sur les services spéciaux américains, soviétiques, allemands, britanniques ou israéliens sont assez nombreuses, elles ne sont que parcimonieuses en ce qui concerne les services français. Ces dernières années ont cependant montré un regain d'intérêt de la part des écrivains et journalistes français pour le monde de l'ombre<sup>127</sup>. De plus, les périodes évoquées sont en général antérieures à la seconde guerre mondiale, et ne présentent qu'un intérêt strictement historique. Il ne serait sans doute pas dommageable de démocratiser la littérature d'investigation, d'explication et de sensibilisation concernant le renseignement. Cette sensibilisation commence effectivement à être menée par les services de contre-espionnage français.

Cette démarche n'est pas nouvelle puisqu'en 1972, le directeur de la DST sur le départ, Jean Rochet, précisait : « *Je me suis beaucoup attaché à développer notre tâche de sensibilisation qui consiste, avec une inlassable persévérance, à informer, à mettre en garde tous ceux qui, dans leur domaine technique, scientifique, économique, administratif, militaire ou même politique, peuvent être, à un moment donné, des cibles pour les services spéciaux étrangers. (...) Une des priorités dans cette tâche de sensibilisation concernait les chefs d'entreprises dont les réalisations risquaient d'être menacées par les différentes formes de l'espionnage économique* »<sup>128</sup>. La DST se déplace donc fréquemment sur le terrain, dans des entreprises, des laboratoires, des institutions, des universités dans le seul but de marquer les esprits, et de nous familiariser avec cette notion nouvelle d'espionnage industriel. L'auditoire est en général composé de personnages clés susceptibles d'être un jour ou l'autre des « cibles » : responsables administratifs, cadres commerciaux, chercheurs, secrétaires, etc. On leur raconte des histoires concrètes et les principales techniques utilisées par la concurrence étrangère ou même nationale : se faire prendre en photo avec le

---

<sup>126</sup> PORCH (D.), *La culture française du renseignement – Une perspective historique et politique*, in *Approches françaises du renseignement*, Fondation pour les études de Défense, Paris, 1996, p.119.

<sup>127</sup> Notamment le formidable ouvrage de FALIGOT (R.), KAUFFER (R.), *Histoire mondiale du renseignement- Tome 1 et Tome 2*.

<sup>128</sup> CECILE (J.-J.), *Le renseignement français à l'aube du XXIème siècle*, Lavauzelle, Paris, 1998, 256p.

directeur de l'usine devant des machines « intéressantes », ou encore laisser tremper sa cravate « par mégarde » dans un bain destiné au lavage des machines-outils.

Il serait également avantageux de sensibiliser les Haut-Fonctionnaires et les décideurs gouvernementaux. Le cycle du renseignement commence par leurs demandes d'informations, lançant ainsi tout un processus d'acquisition et de traitement du renseignement. Leur sensibilisation permettrait un meilleur ciblage des objectifs, ainsi qu'un recours plus systématique aux services des agences spécialisées. Mais au-delà des anecdotes, le temps contribuera sans doute à créer ou consolider un esprit de Défense et une culture du contre-renseignement, pour ensuite dériver vers une culture du renseignement.

La diffusion de cette nouvelle culture doit se faire à tous les échelons de la société. Il existe en France un certain nombre de formations spécialisées dans les problèmes de Défense. Mais elles ne touchent qu'un public réduit et ayant fait une démarche pour s'intégrer dans ce cursus. Il serait bon de développer davantage ces programmes, en y adjoignant une politique de communication efficace. Les récentes publicités pour l'engagement volontaire dans l'armée de Terre sont la preuve « par excellence » des bonnes capacités de relations publiques du ministère de la Défense. L'école des officiers de Saint-Cyr Coëtquidan propose, depuis peu, un enseignement concernant l'histoire et la culture du renseignement, grâce à l'impulsion d'un ancien directeur du service Action de la DGSE, le général Costedoat<sup>129</sup>.

Pourquoi ne pas non plus développer des sites Internet officiels concernant les services de renseignement, comprenant une rubrique « recrutement » et expliquant le rôle du renseignement dans notre politique ? Jadis, la culture se propageait par la diffusion de livres. Aujourd'hui, il faut tenir compte des nouvelles technologies de la communication pour permettre la diffusion plus large d'une telle culture dans nos esprits.

En guise de conclusion, nous pourrions reprendre les propos du général Jean Pichot-Duclos : « *Pour les Allemands, servir le renseignement c'est faire un « métier de seigneurs » (Herrendienst); pour les Anglais, c'est une activité de gentleman ; dans*

---

<sup>129</sup> ISNARD (J.), Le Monde, 27 février 1998, p.1.

*l'armée israélienne, les chefs d'état-major sont pratiquement tous issus du deuxième bureau ; dans l'ex-URSS, le KGB et le GRU ont drainé l'élite des cadres ; l'actuel président des Etats-Unis est l'ancien directeur de la CIA... Français, réveillons-nous !*»<sup>130</sup>.

Les activités de renseignement doivent faire l'objet d'une meilleure approche de la part de nos responsables politiques et militaires. Cela passe, nous venons de le voir, par une meilleure définition des objectifs, par un soucis renouvelé des enjeux du nouveau millénaire et par un changement de mentalité. La France ne doit plus seulement être un pays qui participe. Elle doit aussi être un pays qui gagne. Or si les esprits de nos responsables et de nos concitoyens vont grandement participer au nouveau visage du renseignement français, il est nécessaire de faire de notre système de coordination un élément plus efficace de notre politique de renseignement.

## **CHAPITRE 2 - L'IMPORTANCE DE LA COORDINATION EN MATIERE DE RENSEIGNEMENT**

La coordination du renseignement a pour but de mettre en relief les informations obtenues par les différents services spéciaux, afin de procéder à leur synthèse. Nous allons observer, à travers différents exemples, de quelle manière est conduite la coordination aux Etats-Unis (Section 1), puis étudier la situation française qui, malgré quelques défaillances évidentes, est sur le chemin d'un renouveau et d'une prise de conscience des progrès à effectuer (Section 2).

### **Section 1 - L'exemple américain**

L'organisation du renseignement aux Etats-Unis est prise en compte à plusieurs niveaux. Mais ce pays dispose d'une véritable structure de coordination des services de renseignement en raison de la grande multiplicité des différentes agences. La coordination

---

<sup>130</sup> PICHOT-DUCLOS (J.), *Pour une culture du renseignement*, Défense Nationale, mai 1992, p.17.

de la sécurité se fait tant au niveau du Conseil National de Sécurité qu'au niveau du *Director of Central Intelligence* (DCI).

### **§1- Le Conseil National de Sécurité**

Ce Conseil a été créé par le *National Security Act* de 1947, et par des amendements de 1949. Il a pour fonction d'incarner le lieu de rencontre entre le président des Etats-Unis et les différents conseillers et membres des cabinets ministériels, chargés de des affaires relatives à la sécurité nationale et à la politique étrangère. Depuis la présidence Truman, le Conseil est le principal conseiller du Président en matière de sécurité nationale. Une de ses principales fonctions est cependant d'être le coordonnateur des politiques gouvernementales avec les différentes, et très nombreuses, agences fédérales, ce qui permet de maintenir une certaine cohérence de l'action présidentielle en matière de politique de sécurité.

Présidé par le Président, le Conseil est notamment composé du Vice-Président et des ministres des Affaires étrangères et de la Défense. Le *Director of Central Intelligence* en est également membre et représente la communauté américaine du renseignement au sein du Conseil.

Le Conseil dispose d'une équipe de conseillers et de spécialistes travaillant à plein temps. Leurs activités sont nombreuses. Ils préparent les rencontres du Président avec les leaders étrangers, ses interventions publiques et les réponses aux questions du Congrès dès qu'il est question de sécurité et de politique étrangère. Il existe une multitude de bureaux au sein du Conseil, et chacun est chargé d'un domaine spécifique de recherche et d'analyse : par exemple les Affaires africaines, la politique de Défense et le contrôle des armements, les affaires économiques internationales ou encore la non-prolifération et le contrôle des exportations de matières fissiles. Il existe aussi un sous-comité du renseignement permettant au Conseil de proposer des orientations en matière de renseignement stratégique<sup>131</sup>. Ce comité est essentiellement conseillé par le DCI.

---

<sup>131</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, p.358.

## §2- Le *Director of Central Intelligence*

Le DCI est à la fois, le Directeur de l'agence américaine civile de renseignement extérieur et le chef de la communauté américaine du renseignement<sup>132</sup>. Sa position centrale lui permet d'être le principal conseiller du Président en matière de renseignement. Il reçoit ses instructions de la part des *National Security Council Intelligence Directives* (NSCIDs)<sup>133</sup>, c'est à dire les orientations prises par le Conseil National de Sécurité, et donc du Président. La NSCID n°1 du 17 février 1972 assigne quatre responsabilités majeures au DCI. Il doit :

- Planifier, suivre et évaluer les activités des agences fédérales de renseignement ainsi que leurs budgets.
- Produire les renseignements requis par le Président et tous les commanditaires autorisés de l'Administration.
- Présider et animer les Conseils pour les affaires de renseignement.
- Etablir un équilibre entre les besoins, les priorités américaines en renseignement et les contraintes budgétaires.

Il existe en fait huit directives du NSC présentant le rôle du DCI dans la politique américaine du renseignement. Par exemple, la seconde directive charge le DCI de planifier et d'organiser l'utilisation des moyens de collecte d'informations par les différentes agences fédérales. La directive n°3 charge le Département d'Etat de produire des renseignements politiques et sociologiques concernant tous les pays du monde. La CIA est, elle, chargée du renseignement économique et scientifique. Le ministère de la Défense est quant à lui responsable du renseignement militaire. La sixième Directive fait de la National Security Agency (NSA) le responsable de l'intelligence économique. La Septième directive est très intéressante et symptomatique de la volonté de rendre le système américain du renseignement le plus efficace possible. Il s'agit d'établir un système de communication du

---

<sup>132</sup> La Defense Intelligence Agency, la National Security Agency, le National Reconnaissance Office, la Defense Mapping Agency, le Central Imagery Office, le Armed Services Intelligence, la Central Intelligence Agency, le Bureau of Intelligence and research, le Office of Intelligence and National Security, le Federal Bureau of Investigation, la Drug Enforcement Agency et le US Secret Service.

<sup>133</sup> RICHELSON (J.), *The U.S. Intelligence community*, Westview Press, San Francisco, Third Edition, 1995, p.386.

renseignement critique<sup>134</sup> chargé de transmettre, dans un temps record, au Président et aux principaux officiels du gouvernement, des renseignements d'une importance particulière pouvant concerner des évènements, tels que le déclenchement d'une crise imminente ou l'assassinat d'un leader politique étranger. A titre d'exemple, la NSA aurait été chargée de déposer, en moins de dix minutes, un rapport de situation sur le bureau du Président<sup>135</sup>.

En somme, la coordination du renseignement aux Etats-Unis passe systématiquement par le DCI, le NSC et donc par le Président. Quelques organes suffisent à gérer et coordonner une « multinationale » du renseignement, brassant un budget équivalant au septième de celui de la France, soit près de 200 milliards de francs. La culture d'un renseignement efficace en France n'a pas encore atteint le niveau d'outre-Atlantique, laissant la coordination française du renseignement dans un état en pleine évolution.

## **Section 2- L'état de la coordination en France**

La France est certes dotée d'instruments de coordination du renseignement, mais rien d'équivalent à ce qui existe aux Etats-Unis. Plusieurs facteurs, propres à la « non-culture » française, démontrent à quel point la construction d'une coordination unifiée et centralisée est une œuvre difficile.

### **§1- La guerre des services**

Une des premières préoccupations des responsables français du renseignement devrait être, dans un premier temps, de mieux repenser l'action de tous leurs services. Il existe en France, à l'instar des Etats-Unis, une multitude d'agences dont les attributions et les compétences sont variées. Pourtant, il arrive souvent que des affaires médiatisées entachent le manque de coordination entre les services. Ce fut, par exemple, le cas en Corse dans le cadre de la lutte anti-terroriste, montrant la triste guerre que se livraient la Police Judiciaire, la Division Nationale AntiTerroriste, les Renseignements Généraux (RG) et la DST, chacun désirant tirer vers soi la couverture du succès. Jean-Jacques Cécile le souligne : « *La situation idéale serait celle où tous les services français impliqués dans le*

---

<sup>134</sup> CRITICOMM System.

<sup>135</sup> RICHELSON (J.), *op.cit.*, p.388.

*recueil et l'exploitation du renseignement auraient à cœur de travailler main dans la main avec le seul soucis de fournir aux décideurs politiques des synthèses de grande valeur »<sup>136</sup>.*

Une des tensions, entre services français, la plus regrettable et la plus connue est celle existant entre la DST et la Direction Générale de la Sécurité Extérieure (DGSE). Un ancien inspecteur de la Division antiterroriste de la DST, Daniel Burdan, enfonce le clou et écrit : *« les responsables de la DST ont déjà compris que l'anti-terrorisme est payant puisque les résultats, si minimes soient-ils, sont propulsés sur le devant de la scène médiatique. Le chacun pour soi devient la règle, relance la guerre des polices, au détriment d'une stratégie sur le long terme. Nous n'avons plus rien à attendre des RG et de la DGSE »<sup>137</sup>*. Le tableau dressé par Burdan est sans doute plus noir qu'il ne l'est réellement. Cela étant, cette guerre des services est ancrée dans l'esprit de beaucoup d'entre nous, ce qui constitue déjà un échec en soi. Pourtant, en examinant les attributions de chacun de ces deux services, nous constatons que l'un est chargé du renseignement sur le territoire national, l'autre à l'étranger. La coopération devrait être de mise. Mais ces dernières années, les actes de terrorisme ont souvent touché la France métropolitaine, engageant ainsi la DST aux sources du terrorisme, c'est à dire dans les pays fortement suspectés de financer et de fournir en armes les divers groupuscules criminels.

Si des progrès ont été effectués à une époque où les responsables des services « concurrents » entretenaient des relations amicales, un rapport préparé par le préfet Masson précisa en quelques mots les difficultés relationnelles entre nos principaux services spéciaux : *« Il y bien incompatibilité de traditions et de méthodes entre les deux services dont la complémentarité est évidente et la rivalité historique. [...] Il est significatif de constater que lorsque la DST souhaite obtenir des renseignements, soit sur le terrorisme à l'étranger, soit sur les points d'appui du terrorisme international hors de nos frontières, elle s'adresse plus volontiers à certains services étrangers qu'à ses homologues de la DGSE »<sup>138</sup>*.

---

<sup>136</sup> CECILE (J.-J.), *Le renseignement français à l'aube du XXIème siècle*, Lavauzelle, Paris, 1998, p.133.

<sup>137</sup> BURDAN (D.), *DST – Neuf ans à la division antiterroriste*, Robert Laffont, Paris, 1990, p.135.

<sup>138</sup> CECILE (J.-J.), *op.cit.*, p.135.

Le général de Gaulle se consternait de voir à quel point certaines personnes négligeaient parfois l'intérêt national et préféraient leur « *petite popote cuite sur leur petit réchaud* »<sup>139</sup>. Le monde français du renseignement est certes composé de personnes très qualifiées et dévouées à leur travail. Cela étant, le problème reste patent. Il existe pourtant un certain nombre d'organismes chargés de coordonner les actions françaises en matière de recherche d'informations.

## **§2- Les structures de coordination**

L'identification des risques et des menaces, ainsi que le type de traitement nécessaire, se doivent d'être pris en compte à un niveau supérieur de l'Etat, c'est à dire supra ministériel. A l'exception de la criminalité ou de la délinquance de droit commun, les menaces émergentes auxquelles doit faire face l'Etat français, ne se limitent pas à une sphère intérieure, et se lient chaque jour davantage avec des facteurs extérieurs, nécessitant des institutions de coordination. Il n'existe pas en France de véritable organe autonome, regroupant tous les services de renseignement français, excluant de fait la nécessaire unité dont aurait besoin ces derniers.

Pour l'instant, seuls des organismes détachées des services du Premier ministre sont chargés de coordonner la politique française du renseignement. Parmi eux, le Secrétariat Général de la Défense Nationale (SGDN). Celui-ci a plusieurs missions établies par le décret n°78-78 du 25 janvier 1978. Il assure, entre-autres, le secrétariat des conseils et comités de Défense. Il assiste également le Premier ministre dans l'exercice de ses responsabilités en matière de direction générale de la Défense, c'est à dire tout ce qui concerne la coordination des études sur les données de la politique de Défense, le suivi des crises et des conflits internationaux et la coordination des mesures de Défense. Mais ce service du Premier ministre est également chargé du secrétariat du Comité Interministériel du Renseignement (CIR).

L'article 3 du décret de 1978 précité le précise : « *Le SGDN assure le secrétariat du CIR. En exécution des plans, orientations et décisions arrêtés en conseil de Défense ou en*

---

<sup>139</sup> KLEN (M.), *La crise d'identité du renseignement*, Défense Nationale, juillet 1998, p.97.

*CIR, il notifie les objectifs en matière de renseignements. Il anime la recherche du renseignement dans les domaines intéressant la Défense et il en assure l'exploitation au profit du gouvernement et des organismes concernés* ». Ainsi le secrétariat prépare les réunions du CIR et présente le projet de plan national de renseignement (PNR). Ce plan traduit la volonté des autorités politiques en matière de renseignement et retient un nombre limité de domaines jugés prioritaires.

Créé par l'ordonnance du 7 janvier 1959 et accompagné par le décret d'application du 20 octobre 1962 et placé sous la présidence du Premier ministre, le CIR comprend dans sa collégialité, les ministres de la Défense, de l'Intérieur, des Affaires étrangères, de l'Economie, des Finances et de l'Industrie, de la Recherche, de l'Outre-mer et de la Coopération. Y sont également conviés, le Directeur de cabinet du Président de la République, le chef d'état-major de l'Elysée, le Secrétaire général du gouvernement et le Secrétaire général de la Défense Nationale. D'autres membres du gouvernement, ou certaines personnes ayant des compétences dans un domaine de recherche précis, peuvent être amenés à y participer, en cas de nécessité<sup>140</sup>. La principale fonction du CIR est toutefois d'animer, d'orienter et de coordonner toutes les activités de recherche des services de renseignement.

Malgré la présence de telles institutions de coordination, la France ne possède toujours pas d'organe central de coordination, ce qui fait penser à certains auteurs que la création d'un Conseil national de sécurité serait un pas très encourageant pour le futur du renseignement français.

### **§3- Vers la création d'un Conseil national de sécurité**

Le SGDN assure une bonne coordination avec quelques comités interministériels. Mais d'autres organismes, agissant pour la sécurité nationale, ne lui sont pas rattachés. Ainsi en est-il du comité de coordination des télécommunications, du groupement interministériel

---

<sup>140</sup> RENOARD (I.), *La coordination du renseignement en France*, in Les Cahiers de la sécurité intérieure, n°30, 1997, p.12.

de contrôle<sup>141</sup> et du comité interministériel de lutte anti-terroriste. Les rattacher au SGDN ne pourrait que renforcer et globaliser la coordination en France.

En effet, sans ces organes, le SGDN, dans le cadre de sa mission de tenir informés les autorités gouvernementales en temps réel lors des crises internationales, ne peut pas obtenir tous les renseignements qui permettraient une analyse complète et percutante de la situation. Cet état de fait a amené certains auteurs à proposer la création d'un Conseil National de Sécurité à l'instar de ce qui existe aux Etats-Unis ou en Russie. Ainsi, Eric Denécé rapporte des observations allant dans ce sens : « *La conduite des affaires de Défense et de sécurité étant devenue une manœuvre permanente d'appréciation de situations et de prises de décisions, il apparaît éminemment souhaitable que soit instaurée une entité qui puisse, en permanence, appuyer les décideurs du plus haut niveau, le Président de la République et le Premier ministre, dans cet exercice* »<sup>142</sup>. Il serait donc très avantageux de regrouper au sein d'un seul organisme toutes les institutions ayant un lien avec le renseignement, afin d'éviter, dans un premier temps, le double-emploi des travaux d'études et d'analyse menés par chacun<sup>143</sup>, et dans un second temps, renforcer la valeur des renseignements transmis aux décideurs politiques. Ce constat a rapidement été fait dans le monde de l'informatique avec la création de bases de données. En saisissant un mot clé, l'utilisateur a accès immédiatement à une multitude d'informations contenues dans de nombreux fichiers différents. Pourquoi ne pas appliquer à notre système de renseignement un tel processus ? Nous y gagnerons du temps, de l'efficacité et de la qualité dans notre traitement de l'information.

Ainsi la présence de l'Homme dans le cycle du renseignement doit, non seulement être maintenue, développée et mieux réfléchi au niveau de la définition des objectifs et de la coordination de tout l'ensemble de la politique de renseignement, mais aussi être réhabilitée au niveau de l'action sur le terrain.

---

<sup>141</sup> Chargé des écoutes téléphoniques.

<sup>142</sup> BAER (A.), in DENECE (E.), *Pour un Conseil national de sécurité*, Défense Nationale, novembre 1995, p.31.

<sup>143</sup> DENECE (E.), *op.cit.*, p.32.

## TITRE 2- LA REHABILITATION DE L'ACTION HUMAINE SUR LE TERRAIN

Le renouveau de l'action humaine dans le renseignement est d'autant plus actuelle que les américains, maîtres d'œuvre du plus grand réseau d'espionnage technique au monde, posent ouvertement le problème, ainsi que le montre l'entrevue accordée à l'hebdomadaire *Le Point*, par un ancien directeur de la CIA. A la question : « *Que pensez-vous de la critique selon laquelle la CIA a trop mis l'accent sur la technologie ?* » Robert Gates répondit : « *Ce débat entre l'espionnage technologique et les sources humaines dure depuis trente ans. On a besoin des deux. Mais la technologie en matière d'espionnage est très coûteuse. Si vous dépensez dix fois plus en technologie, cela ne signifie pas que vous avez des renseignements dix fois meilleurs. Pendant l'administration Carter, on a moins mis l'accent sur les agents parce que Carter était mal à l'aise avec l'espionnage humain. Ce n'est plus vrai. Le rôle des agents est encore plus important aujourd'hui, en particulier à cause des groupes terroristes «freelance» qui ne sont pas sponsorisés par un Etat. La pénétration de ces groupes là est la seule manière de savoir ce qu'ils préparent. Car ils pourraient construire une bombe atomique dans leur chambre sans que les satellites n'en sachent rien* »<sup>144</sup>.

Le renseignement d'origine humaine a, semble-t-il donc, de beaux jours devant lui. Pourtant, la fin de la guerre froide a mis beaucoup d'agents spéciaux sur la touche. Il apparaît pourtant clairement que les besoins en éléments compétents, bien formés et expérimentés, soit nécessaire. Pour cela, il faut mettre en exergue les capteurs utilisables (Chapitre1), pour ensuite repenser et renforcer la mise en œuvre de ces moyens sur le terrain (Chapitre2).

### CHAPITRE 1- LES MOYENS DU RENSEIGNEMENT HUMAIN

Un service de renseignement ayant une vocation tournée vers l'étranger, ou davantage axée sur la surveillance à l'intérieur des frontières de l'Etat, doit impérativement disposer, en permanence, d'informations fiables. Celles-ci peuvent provenir de sources très diverses, mais l'une d'entre elles est particulièrement précieuse : la source humaine. Les

---

<sup>144</sup> AUDIBERT (D.), *CIA – Enquête sur un mythe*, Le Point, n°1420, 3 décembre 1999, p.85.

agents de renseignement peuvent présenter des profils très divers, et remplir des tâches propres à certains domaines (Section 2). Mais pour qu'un service se dote de capteurs humains efficaces, encore faut-il qu'il les trouve et qu'il engage un processus complet de formation (Section 1).

## **SECTION 1- LA QUETE DE RESSOURCES HUMAINES EFFICACES**

Un des nombreux problèmes auquel doit faire face un responsable de Centre de renseignement est certainement celui du renouvellement des effectifs, surtout lorsque l'environnement mondial est en constante mutation et que les domaines de compétences recherchés varient de jour en jour.

### **§1- Le recrutement officiel**

Le recrutement est une partie essentielle du travail d'un service de renseignement. Un tel organisme est composé de personnels très différents, aussi bien administratifs qu'opérationnels. Bien sûr, certains agents, notamment les analystes, ne quittent que rarement les murs de leur Centre, et sont chargés de synthétiser les masses de documentations mises à leur disposition par les différentes sources du service. Mais, dans notre étude, nous allons plutôt nous attacher aux agents de terrain, c'est à dire ceux qui cherchent l'information à la source, quel que soit l'endroit où elle se trouve. Ces personnes nécessitent de présenter un certain nombre de qualités adaptables aux besoins des missions.

Loin de l'image hollywoodienne de l'agent secret, l'officier de renseignement doit être quelqu'un de cultivé, discret et capable d'analyser très rapidement les situations dans lesquelles il se trouve. Ceci explique un recrutement effectué dans les milieux académiques, qu'il s'agisse d'universités, d'écoles ou instituts. Les domaines jugés intéressants par les responsables de services ont d'ailleurs quelque peu évolué depuis une décennie. Du temps de l'affrontement idéologique entre l'Est et l'Ouest, les fonctionnaires et contractuels du renseignement étaient notamment recrutés parmi les historiens ou les politologues. Aujourd'hui, on recherche davantage des économistes, des sociologues, des ingénieurs en

électronique ou plus généralement des scientifiques. Ceci a permis une « *plus large intégration des femmes* »<sup>145</sup>.

Chaque pays dispose d'un système particulier de recrutement. Les soviétiques, puis les russes, ont souvent retenu la solution du recrutement de père en fils, tout en ne négligeant pas l'approche discrète des établissements académiques. Les américains, forts de leurs universités réputées, disposent d'un potentiel important de candidats. Cela étant, à l'instar des britanniques, ils n'hésitent pas à passer des annonces, plus ou moins codées à une époque, et beaucoup plus explicites aujourd'hui, dans les journaux, hebdomadaires du pays ou même sur Internet. Ainsi peut-on lire sur le site du service de contre-espionnage britannique, le MI5, une annonce disant : « *Si tu es anglais, photographe, en bonne santé, que tu aimes les grands espaces et que tu n'es pas claustrophobe, rejoins les services secrets britanniques* »<sup>146</sup>. Les américains ne sont pas en reste.

Le site Internet de la CIA<sup>147</sup>, fort bien réalisé d'ailleurs, présente tout un dossier relatif à l'emploi dans l'agence, en évoquant notamment, les missions et les formations demandées. Plus de quarante cinq types d'emploi sont proposés. Cela va de l'infirmière à temps partiel, à l'économiste ou l'agent clandestin. Le site aurait enregistré près de 50.000 demandes en 1998<sup>148</sup>. Cette démonstration d'inventivité technologique, n'a cependant pas été fortuite. En effet, la CIA aurait perdu environ quatre mille emplois depuis la chute de l'empire soviétique. Le journal *Le Point* précise qu'en 1995, vingt cinq agents clandestins ont été recrutés, tandis que cent vingt cinq prenaient leur retraite, faisant dire à un ancien directeur adjoint du renseignement de la CIA, dans le *New York Times* : « *On ne peut pas faire tourner un réseau de renseignement mondial avec seulement vingt cinq recrues par an !* »<sup>149</sup>. Les américains ont donc lancé une vaste campagne de recrutement, avec pour objectif avoué « *d'attirer 2000 à 3000 jeunes parmi les plus brillants des Etats-Unis sous peine d'assister à la mort lente du renseignement américain* »<sup>150</sup>. Une ligne téléphonique a même été ouverte pour recevoir des candidatures, ou répondre à diverses questions<sup>151</sup>. Nous

---

<sup>145</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, p.403.

<sup>146</sup> [www.mi5.gov.uk](http://www.mi5.gov.uk)

<sup>147</sup> [www.odci.gov/index.html](http://www.odci.gov/index.html)

<sup>148</sup> AUDIBERT (D.), *op.cit.*, p.80.

<sup>149</sup> AUDIBERT (D.), *idem.*

<sup>150</sup> AUDIBERT (D.), *idem.*

<sup>151</sup> Numéro de téléphone : 800.562.72.42.

pouvons nous étonner qu'il n'y ait pas, en France, de site Internet officiel des services de renseignement. Un membre de la DGSE nous a cependant fait savoir que le projet était en marche<sup>152</sup>. La méthode de recrutement semble moins «branchée » en France, le recrutement passant essentiellement par voie de concours administratifs.

Un débat quant au recrutement dans la police nationale est apparu au cours de l'année 2000. La question était de savoir pourquoi les effectifs policiers, exerçant dans les zones sensibles du pays, n'étaient pas davantage issus de l'immigration, dans le but de faciliter les relations entre la police et les «jeunes » . Cette question peut également se poser dans les services de renseignement.

La France, de par sa position géographique extrême sur le continent européen et sa qualité de vie, est un point de passage et de sédentarisation des mouvements de l'immigration venant, soit de l'Europe même, soit du continent africain. Un agent de renseignement français, originaire du Lubéron, rencontrerait sans doute plus d'obstacles dans sa quête d'informations dans un pays de la péninsule arabique, qu'un agent originaire d'un pays du Maghreb. De même que la tâche consistant à combattre, par exemple, le terrorisme islamiste à l'intérieur de nos frontières se fera d'autant plus facilement que nous aurons à notre disposition des agents d'origine arabe. Il serait donc bon d'encourager de manière conséquente, dans un premier temps, leur recrutement, soit dans l'armée, soit dans un service de police, pour ensuite les amener vers les services spéciaux, et leur dispenser une formation particulière.

## **§2- La formation**

Un agent de terrain doit, en permanence, être en contact avec des sources intéressantes et jugées fiables par le service. Nous avons observé auparavant que l'espionnage économique et industriel était devenu une des principales préoccupations des agences de renseignement. Il ne s'agit plus seulement de connaître l'état des troupes du Pacte de Varsovie et le nombre de missiles capables de transporter des ogives nucléaires. Le renseignement du siècle prochain est davantage axé sur les capacités industrielles et

---

<sup>152</sup> Conférence donnée par un Colonel de la DGSE au DEA de Défense à l'Université de Lille II en avril 2000.

économiques d'un pays, ou plus précisément d'une entreprise. Un agent devra donc maîtriser au mieux le domaine concerné par sa recherche.

Un spécialiste en électronique sera plus à l'aise pour comprendre le fonctionnement d'un système ultramoderne fabriqué, par exemple, au Japon, qu'un historien. Bien sûr, les services spéciaux bénéficient de leur propre réseau d'enseignement, scientifique notamment, mais ils ne suffisent pas à « l'éducation » d'un agent de renseignement opérationnel. En effet, dès qu'un agent part en mission, il doit faire face à des éléments étrangers. C'est ainsi que toute une politique d'enseignement linguistique est mise en œuvre dans les écoles de renseignement. « *Sans le don des langues, l'agent secret se sent comme un soliste d'opéra sans voix* »<sup>153</sup>.

Nous l'avions observé, la NSA, chargée des interceptions électroniques, est l'une des institutions américaines les mieux dotée en traducteurs et spécialistes de civilisations étrangères. Il existe en France une école spécialisée dans ce domaine, l'EIREL (Ecole interarmées du renseignement et des études linguistiques) située à Strasbourg. La nécessité absolue de connaître des langues étrangères se manifeste aussi bien dans le renseignement militaire que politique, diplomatique ou économique. Ainsi, les militaires n'ont pas d'autres choix que de pratiquer la langue de Shakespeare, puisque l'anglais est devenue la référence mondiale en matière de communication, notamment sur les théâtres d'intervention extérieurs, et lors des échanges entre états-majors français et alliés<sup>154</sup>. De même, les agents clandestins n'ont pas d'autre choix que de maîtriser parfaitement la langue du pays ciblé, sous peine de ne plus être clandestin. Cela étant, il existe encore des lacunes dans l'enseignement linguistiques, notamment en ce qui concerne le contenu des cours. Ainsi que le précise Michel Klen, « *ces certificats linguistiques[...] devraient être plus pragmatiques, faire moins appel au « bachotage » et surtout mieux développer l'aptitude des cadres à pouvoir maîtriser le plus grand nombre de situations linguistiques* »<sup>155</sup>.

---

<sup>153</sup> AGRANOVSKY (V.), *Confessions d'un espion russe*, Messidor, Paris, 1990, p.63.

<sup>154</sup> Les opérations menées par les soldats français à l'étranger ont toutefois montré les limites à l'efficacité des Certificats militaires de langue (CML) français. En effet, ceux-ci fondaient principalement leur enseignement sur l'étude d'organigrammes et négligeait l'étude purement pratique de la langue telle que parlée sur le terrain.

<sup>155</sup> KLEN (M.), *La crise d'identité du renseignement*, Défense Nationale, juillet 1998, p.101.

En plus de leur formation linguistique, les agents de renseignement, agissant sur le terrain, bénéficient, en plus de leur formation initiale, d'une formations spécifique.

En premier lieu, on enseigne aux nouveaux venus les principes de bases du renseignement, c'est à dire sa définition, les différentes formes qu'il peut prendre, sa valeur. Puis, les instructeurs vont leur expliquer les rudiments du métier, notamment <sup>156</sup>:

- « Les structures et organigrammes des services adverses
- Les méthodes du contre-espionnage
- Les mesures de sécurité
- La nature, valeur et cotation du renseignement
- L'observation
- L'utilisation du matériel
- Tout ce qui concerne les faux et reproductions
- Une initiation aux techniques de cambriolage et de photographie
- La radiocommunication et les échanges furtifs
- Les différentes manières d'établir un contact ».

Les agents chargés du renseignement militaire reçoivent une formation complémentaire. Celle-ci contient les rudiments de la lutte de guérilla, des patrouilles profondes, des missions d'exfiltration, des captures de prisonnier, et plus généralement d'acquisition du renseignement militaire. En outre, ils reçoivent une formation plus « sportive » concernant par exemple la navigation, l'escalade, le parachutisme, l'orientation ou les techniques de combat sous-marin.

Seuls les agents de terrain bénéficient d'une telle formation, tout d'abord en raison de son coût très élevé, mais aussi du fait du caractère extrêmement confidentiel des matières enseignées. Ensuite, les agents considérés comme aptes à partir en mission, aussi bien sur le territoire national, s'ils agissent pour un service de contre-espionnage, qu'à l'étranger, s'ils travaillent pour une centrale de renseignement extérieur, sont assez peu nombreux. Ainsi le réseau de l'agent clandestin soviétique Richard Sorge, implanté au

---

<sup>156</sup> DESMARETZ (G.), *Le grand livre de l'espionnage*, Editions Chiron, Paris, 1999, p.38.

Japon dans les années trente, ne comptait que deux agents professionnels qui employaient une vingtaine de « sous-agents ».

Le monde du renseignement a l'inconvénient, pour les observateurs extérieurs, de représenter une zone de flou artistique, difficile à saisir et volontairement entretenue. Vouloir dessiner le portrait-type d'un agent de renseignement, d'un espion, est sans doute une mission impossible, à l'exception peut-être pour les anciens du métier. Il est toutefois possible d'opérer une typologie de ces soldats de l'ombre.

## **Section 2- Typologie des agents de renseignement**

Une fois la formation assurée, un agent de renseignement est opérationnel. Mais ces agents, entraînés et rémunérés par des structures étatiques, ne constituent pas une catégorie unique d'agents. En fait, il en existe une multitude, chacun disposant de qualités indispensables, non seulement pour la réussite de leur travail, mais aussi pour la longévité, soit de leur carrière (dans le meilleur des cas), soit de leur vie (dans les cas extrêmes).

### **§1- Catégorisation des agents de renseignements**

Le rapport final de la commission sénatoriale américaine du renseignement daté du 26 avril 1976 donne cette définition de l'agent : « *Individu qui agit sous la direction d'un service de renseignements ou d'un service de sécurité afin d'obtenir ou d'aider à obtenir des informations pour le renseignement ou le contre-renseignement* »<sup>157</sup>. Ceci est une explication très large du rôle d'un agent. Pourtant chaque type d'agent remplit une fonction spéciale.

**L'agent légal** : c'est un professionnel du renseignement implanté sous une couverture dite légale, c'est à dire appartenant à une ambassade en tant qu'attaché militaire, directeur du service des relations publiques, ou diplomate. Ainsi les soviétiques comptaient, parmi le personnel de certaines de leurs ambassades, près de 60% d'agents du KGB. Leur rôle n'est pas le plus dangereux, car en cas d'allégations d'espionnage à leur rencontre, ils sont déclarés *persona non grata*, et priés de quitter rapidement le pays hôte.

---

<sup>157</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, p.18.

**L'agent clandestin ou illégal**<sup>158</sup>: celui-ci agit dans un pays étranger en se faisant passer, en général, pour un ressortissant d'une tierce nationalité. Les soviétiques ont, ainsi, souvent envoyé des agents « canadiens » aux Etats-Unis. Il n'est pas membre d'une mission diplomatique, et ne bénéficie donc pas de l'immunité diplomatique. Les conséquences, en cas d'arrestation, peuvent être dramatiques, à moins de faire l'objet d'un échange d'espions entre les deux Etats concernés.

**L'agent d'influence** : celui-ci fait usage de sa situation personnelle, en fonction de l'influence ou plus encore de l'autorité qu'il représente, et donc de la confiance qu'il véhicule, pour tenter d'influencer l'opinion publique ou certains responsables, de toutes natures, ayant un poste jugé intéressant par l'agent ou son employeur, dans le but de faire promouvoir les intérêts de son pays ou de son entreprise. Dès le début de l'époque soviétique en Russie, Lénine décida d'en faire un usage immodéré, jugeant que ces « idiots utiles », comme il les dénommait, pouvaient être d'une grande utilité pour le régime. Dans les années soixante, le régime communiste utilisa de tels agents, afin de donner une apparence démocratique aux pays du bloc soviétique, en faisant notamment usage de politiciens plus modérés que les communistes (les sociaux-démocrates, par exemple), ou même des hommes d'Eglise. Tous ces agents ne sont pas conscients de leur action. Les anglo-saxons ont ainsi établi une distinction entre les agents conscients et inconscients. Mais leur domaine de compétence sont variés, puisqu'il peuvent concerner aussi bien les questions politiques, diplomatiques, économiques que militaires. Ainsi, la méthode du lobbying est très utilisée aux Etats-Unis. Déclarée légale, sous certaines conditions, elle fait appel à des agents d'influence. Mais ceux-ci agissent ès qualité, et n'ont pas le caractère clandestin existant dans le monde du renseignement.

**L'agent dormant** : il s'agit d'un agent clandestin implanté dans un pays étranger, exerçant une activité normale, c'est à dire n'ayant aucun lien avec le monde de l'espionnage, et dont le travail d'agent est suspendu pour une période donnée, avant d'être « réveillé » pour une mission précise. Ce type d'agent a été utilisé afin de commettre les attentats de septembre 2001 aux Etats-Unis.

---

<sup>158</sup> Les expressions « agents clandestins » et « agents illégaux » sont utilisées respectivement, en Occident et en Russie.

**L'agent double**<sup>159</sup> : il s'agit ici d'un agent de renseignement professionnel travaillant pour un service de renseignement ou de contre-espionnage, mais retourné par une agence d'un pays adverse, et amené à trahir son service d'origine, tout en restant en place. Les raisons d'une telle trahison ont fait l'objet de nombreuses interrogations des spécialistes du renseignement. Elle peut être la conséquence de ce que les agences appellent le processus MICE (*Money, Ideology, Constraint, Ego*), c'est à dire une trahison due à l'argent, l'idéologie politique, la contrainte (souvent en raison d'un chantage sexuel, entre autres) ou le caractère narcissique de la personne. Cela étant, ce type de recrutement est valable pour tous les types d'agents, mais d'autant plus remarquable quand il touche un professionnel du renseignement.

**L'agent provocateur** : personne dont le rôle est de faire commettre à certaines personnes ou organisations, des actes illégaux, dans le but de les discréditer auprès de l'opinion publique.

**L'agent de pénétration** : un tel agent est intégré, par un service secret, dans un service de renseignement étranger, ou dans une organisation, dans le but d'y collecter un maximum d'informations. Il s'agit sans aucun doute de la mission la plus délicate et dangereuse pour un agent. En effet, il doit, en premier lieu obtenir la nationalité du pays ciblé, puis il doit se faire engager par le service<sup>160</sup>, ce qui n'est pas donné à tout le monde, en raison des mesures de sécurité étoffées des agences gouvernementales. Il doit pouvoir faire valoir une biographie solide, sans « trous », et particulièrement cohérente, ce qui peut prendre beaucoup de temps. Le secret qui les entoure doit être particulièrement hermétique, et les archives ne dévoilent guère les exploits et les identités de tels artistes du renseignement.

---

<sup>159</sup> Dans l'Art de la guerre de Sun Tzu, celui-ci fait dire à Li Ch'uan, dans la partie consacrée à l'utilisation des agents secrets : « *Lorsque l'ennemi envoie des espions pour fureter dans ce que j'accomplis ou n'accomplis pas, je leur dispense libéralement les pots-de-vin, je les retourne, et je fais d'eux mes propres agents* ».

<sup>160</sup> Leur situation dans un service sera en général à un niveau secondaire, pour ne pas faire l'objet de trop de surveillance.

Tous ces agents remplissent des fonctions précises, à des degrés plus ou moins importants. Mais leur utilité et leur efficacité dans le monde du renseignement dépend grandement des qualités dont ils font preuve en intervenant sur le terrain.

## §2- Les qualités propres aux capteurs humains

L'intérêt concernant l'utilisation de capteurs humains, dans la partie « recherche » du cycle du renseignement, est évident. Ils sont les seuls capables de véritablement saisir l'ambiance régnant dans un pays, une organisation, une entreprise, un syndicat ou une personne. Bien sûr, les machines possèdent beaucoup d'avantages, mais à l'heure actuelle, elles ne répondent qu'à une logique binaire. Soit tout est noir, soit tout est blanc. La psychologie n'intervient pas dans ce type de capteurs. L'Homme est donc en mesure de saisir une multitude de détails comportementaux, *a priori* sans intérêt, mais qui, une fois regroupés, fournissent un renseignement valable.

Cela étant, le capteur humain doit posséder certaines qualités s'il veut pouvoir se transformer en une sorte de radar passif, sans attirer l'attention vers lui, surtout lorsqu'il travaille sous une couverture clandestine. Un livre écrit par un romancier soviétique, a raconté l'histoire de l'agent clandestin russe Gordon Longsdale, alias Konon Trofimovitch, dont la ouverture était celle d'un riche homme d'affaires (Longsdale sera même anobli par la Reine en obtenant le titre de *Sir* puis démasqué quelques années après). Cet ouvrage<sup>161</sup>, au-delà de la narration des nombreuses péripéties de ce génie de l'espionnage, s'est principalement attaché à analyser les qualités et la psychologie dont devait faire preuve un agent de renseignement clandestin sur le terrain. Certaines de ces qualités sont également requises pour un agent opérant sous couverture légale, généralement diplomatique.

Selon l'auteur, la qualité première d'un agent de renseignement est de pouvoir « *dissoudre dans la foule* ». Puis il ajoute : « *Je savais bien que si l'on devait remarquer cinq personnes sur trente installées dans une brasserie, je devais être parmi les vingt-cinq quidams anonymes* »<sup>162</sup>. Ce soucis de ne pas vouloir « défiler sur les Champs Elysées le 14

---

<sup>161</sup> AGRANOVSKY (V.), *Confessions d'un espion russe*, Messidor, Paris, 1990, 191p. Bien qu'étant soviétique, ce livre a connu un vif succès en Occident.

<sup>162</sup> *idem*, p.16.

juillet »<sup>163</sup> est essentiel et vital. Toute la réussite d'un travail de renseignement repose sur le fait qu'un agent doit ressembler à une personne-type du pays dans lequel il travaille. Chaque pays, chaque région, chaque catégorie socio-professionnelle, est connu pour ses particularismes dans la manière de se comporter ou de se vêtir, et l'agent doit le savoir. Pour cela il doit préalablement étudier les mœurs et la façon de vivre des gens avec qui il sera en contact. Par exemple, l'anglais est un buveur de bière, au même titre que le russe est un grand consommateur de kvas<sup>164</sup>. « *Si, en URSS, quelqu'un refuse obstinément un verre de kvas, je vous assure que c'est un espion* »<sup>165</sup>. L'auteur cite également l'exemple du médecin anglais : « *ils ne portent jamais de blouse, sauf dans le bloc opératoire.[...]Un médecin qui consulte porte un pantalon à rayures, une veste noire avec une fleur à la boutonnière* »<sup>166</sup>. Il en va de même dans la façon de parler une langue. Un homme d'affaires britannique travaillant à la City n'a pas l'accent « cockney » des ouvriers de la banlieue de Londres. Pourtant la situation géographique est quasiment identique. De même, l'agent clandestin ne doit, à aucun moment, montrer ses origines véritables. Agranovsky cite le fait que Longsdale était amateur de jeux d'échecs. « *Moi, je jouais aux échecs, moyennement pour un soviétique, mais pas mal du tout pour les anglais de l'époque. Je grattais tous mes collègues hommes d'affaires, ce qui pouvait d'ailleurs paraître suspect. Or je n'avais pas le droit de me « mouiller ». Alors, la mort dans l'âme, je me laissais manger des pions* »<sup>167</sup>.

Ensuite, l'agent clandestin doit être un bon comédien. Il doit pouvoir jouer un rôle « *convenant à son caractère, son tempérament, ses penchants, son état concret et sa vocation naturelle : qui est artiste, qui ingénieur, qui garçon de café, qui journaliste, qui médecin, qui concierge. Ce qui importe encore plus que la profession, c'est qu'on ne trouve rien à redire à qui la pratique. Si je suis businessman (Longsdale est agent soviétique), mon caractère ne doit pas m'empêcher de payer mes impôts dans les formes* »<sup>168</sup>. L'auteur rappelle qu'Al Capone a été arrêté pour non-paiement des impôts.

---

<sup>163</sup> Agranovsky précise qu'un « *homme de gloire et en proie à une ambition démesurée ne peut devenir agent de renseignement : la clandestinité paralyse, elle estompe les talents, elle empêche de s'épanouir et de se distinguer, elle restreint l'éventail des connaissances et n'autorise que les liaisons nécessaires aux besoins de la cause, elle fait obstacle à la reconnaissance sociale* », *idem*, p.27.

<sup>164</sup> Boisson fermentée fabriquée à partir du pain noir.

<sup>165</sup> *idem*, p.92.

<sup>166</sup> *idem*, p.26.

<sup>167</sup> *idem*, p.156.

<sup>168</sup> *idem*, pp.25-26.

L'agent doit aussi avoir un minimum de «jugeote », selon les propos d'Agranovsky, c'est à dire « *être toujours correct, modeste, judicieux, réfléchir avant de parler, être maître de soi, avoir le sens de l'analyse rapide, prendre des décisions et des mesures sages* »<sup>169</sup>. En effet, l'agent est considéré comme un capteur «à fonctions multiples ». Son rôle ne doit pas se limiter à saisir une situation particulière, mais à la comprendre et à prendre des mesures allant dans le sens de son travail. L'analogie au jeu d'échecs est claire. Jouer, mais penser à ce que pourront être les manœuvres adverses afin de pouvoir constamment réactualiser sa stratégie. L'auteur précise que la tête n'est pas uniquement faite pour porter le chapeau (Longsdale a exercé principalement en Angleterre), mais aussi pour penser. En somme, l'agent clandestin ne ressemble pas à l'image de l'espion que nous pourrions avoir. L'auteur fait dire à Longsdale : « *je ne me suis jamais collé de moustaches, ni de barbes[...]. Tout cela n'est que bêtise parce que le résident et ses informateurs n'ont besoin ni de pénétrer secrètement quelque part (à de très rares exceptions près !), ni de grimper aux fenêtres avec une échelle de corde. Non, c'est un travail d'abord et avant tout minutieux, difficile, qui requiert de grands efforts, de l'attention, de la volonté, des connaissances sérieuses et une compétence considérable* »<sup>170</sup>.

Afin d'obtenir un maximum de renseignements de la part d'informateurs conscients ou non, l'agent doit pouvoir se faire des amis « nécessaires ». Pour cela, il existe une méthode d'approche expliquée dans un ouvrage de Dale Carnegie, *Comment se faire des amis*<sup>171</sup>, dans lequel sont expliqués certains principes de la communication, les moyens de rallier quelqu'un à votre point de vue, les moyens de plaire aux gens ainsi que les moyens de faire changer quelqu'un d'avis sans l'indigner ni le vexer. En fait, l'agent, clandestin ou non, doit être fondamentalement curieux, le rapprochant ainsi du métier de journaliste, activité fréquemment choisie comme couverture par les agents de renseignement.

L'agent passe son temps à mentir. C'est une question de survie. Mais pour mentir, une excellente mémoire est vitale. Non seulement pour retenir toutes les informations recueillies, mais aussi pour être constamment cohérent avec sa biographie. Agranovsky cite le cas où l'agent Longsdale s'était présenté au guichet d'un aéroport londonien avec un faux

---

<sup>169</sup> *Idem*, p.32.

<sup>170</sup> *idem*, p.54.

<sup>171</sup> *idem*, pp.65-68.

passport. Mais lorsque le guichetier lui demanda son nom, comme ce fut longtemps la règle en Angleterre, il ne s'en souvenait plus. *«Impossible de jeter un coup d'œil, je n'avais plus le passeport en main. Me voilà dans de beaux draps... Que faire ? Il attend. Je ne dis pas un mot. Enfin, après un temps de silence, je lui dis tranquillement : mettez le nom de famille qui figure dans le passeport. Il m'a regardé d'un air éberlué, puis il a éclaté de rire comme si je l'avais chatouillé »*<sup>172</sup>.

La réussite d'une opération de renseignement dépend donc essentiellement de la valeur d'un agent. Mais ceux-ci sont rares, non seulement en raison des nombreuses qualités requises, mais aussi en raison du temps que nécessite la formation et l'implantation d'un agent dans un pays ou dans une organisation. Le temps et la patience sont des éléments clés du renseignement. En outre, un agent ne travaille quasiment jamais seul, bien qu'il puisse disposer d'une marge de manœuvre plus ou moins grande. Il fait alors partie d'un réseau, d'un orchestre, dont il est soit le chef, soit un musicien parmi d'autres.

## **CHAPITRE 2- LA MISE EN ŒUVRE DES MOYENS**

Dans ce chapitre, nous avons décidé d'évoquer davantage les techniques de renseignement mises en œuvre à l'étranger. Le renseignement intérieur n'en reste certes pas moins passionnant, mais il fait appel à des moyens différents. Les réseaux en sont bien sûr une partie non négligeable, mais le danger que peut représenter la collecte d'informations en territoire étranger, et souvent hostile, rend la tâche beaucoup plus complexe, tant pour les opérations d'espionnage que pour celles intervenant dans le domaine du contre-renseignement. En plus des réseaux classiques diplomatiques (Section 1), il est nécessaire d'entretenir des réseaux clandestins (Section 2) qui ont eu tendance à être désactivés depuis quelques années.

---

<sup>172</sup> *idem*, p.170.

## Section 1- L'importance du réseau diplomatique

En ce qui concerne les opérations de renseignement à l'étranger, le principal point d'attache est incontestablement la mission diplomatique. Elle possède des avantages non négligeables, et, bien qu'étant la principale suspecte des services de contre-espionnage du pays hôte, quelques-uns de ses membres exercent une fonction importante en matière de renseignement.

### §1- Les avantages diplomatiques

Le premier point est celui du caractère international de l'implantation diplomatique. Chaque Etat a le droit d'implanter une représentation diplomatique dans un pays avec lequel il entretient des relations. Il peut arriver que les relations deviennent si tendues que l'un des deux Etats décide de rompre, provisoirement, les relations diplomatiques officielles. Dans ce cas, les ambassadeurs, les consuls et les diplomates sont tous rappelés dans leur pays d'origine. Ce cas de figure n'est certainement pas le meilleur moyen de recueillir un maximum d'informations sur le pays concerné, mais la politique internationale obéit à des règles particulières. Dans ce cas, il paraît indispensable de disposer de réseaux parallèles, de type clandestin, ainsi que nous l'étudierons plus tard.

L'avantage d'une représentation diplomatique est de constituer une parcelle territoriale de l'Etat implanté sur le terrain de l'Etat hôte. L'expression «Etat dans l'Etat» prend ici tout son sens. Les conséquences sont les suivantes : l'ambassade ou le consulat sont théoriquement protégés contre toute intrusion des forces de l'ordre du pays d'accueil, sous peine de violer l'intégrité territoriale du pays représenté. De même, le personnel diplomatique bénéficie d'une immunité qui leur permet, en cas de délit ou de crime, de ne pas être jugé par les autorités locales. Il existe cependant un moyen de « punir » le fautif. L'espionnage est partout considéré comme un crime. Si un diplomate est suspecté d'exercer une telle activité, il sera déclaré *persona non grata*, c'est à dire « non-acceptable », selon les termes de la Convention de Vienne sur les relations diplomatiques et consulaires<sup>173</sup> du 18 avril 1961. Selon Jacques Baud, « l'Etat-hôte peut décréter en tout temps et sans

---

<sup>173</sup> Respectivement les articles 9 et 23.

*notification préalable une personne non grata.. [Elles] sont alors expulsées vers leur pays de provenance, où elles sont soumises à la juridiction de leur pays* »<sup>174</sup>. Certes, le but d'un « diplomate » n'est pas de se faire expulser. Mais dans cette éventualité, sa couverture officielle lui évitera, notamment dans certains pays considérés comme très sensibles, et étrangers à toute considération humaine, de finir devant un peloton d'exécution, dans le meilleur des cas.

L'ambassade peut naturellement être considérée comme un nid d'espions. C'est une de ses fonctions principales. Bien sûr, chaque pays possède sa propre doctrine quant à l'utilisation du réseau diplomatique pour les affaires de renseignement. Les anglo-saxons, les russes et les israéliens en font, à juste titre, un usage immodéré. Le MI6, le service de renseignement extérieur britannique, est par exemple subordonné au *Permanent Undersecretaries Committee on Intelligence Services* du *Foreign Office* (Ministère des Affaires étrangères britannique) et non pas au ministère de la Défense, comme c'est le cas en France. Les relations entre la diplomatie française et le renseignement ont souffert du manque de culture, des responsables politiques, dans ce domaine.

Les avantages diplomatiques sont nombreux et permettent la mise en œuvre de composantes, plus ou moins nombreuses selon le choix politique des services de renseignement d'un pays.

## **§2- Les composantes du réseau**

L'ambassade est le lieu idéal, car protégé juridiquement, pour mettre en œuvre les différents réseaux de renseignement. Il est vrai que les locaux diplomatiques font l'objet d'une surveillance policière particulière. Mais nous allons voir, avec l'exemple de l'ambassade soviétique à Paris, que l'antenne locale du KGB était, à l'époque, très développée, à l'instar de nombreuses ambassades soviétiques.

L'antenne d'un service de renseignement, dans une ambassade, est placée sous la direction d'un résident. Celui-ci fait partie de ces services. Sa fonction principale est de

---

<sup>174</sup> BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, p.375.

coordonner les opérations de renseignement en cours dans le pays d'accueil. La couverture, censée dissimuler sa véritable fonction, peut être purement diplomatique ou subalterne (chauffeur par exemple). Le nom donné, non seulement à l'organisation du réseau de renseignement de l'ambassade, mais aussi aux quartiers réservés à cette organisation, est la « résidence ». Les soviétiques la désignait sous le nom de *Rezidentura*. Située généralement aux étages supérieures, ou dans les sous-sols de l'ambassade, la résidence constitue une zone à part. A Paris, elle occupait les trois derniers étages supérieurs. Selon Thierry Wolton, « on y entre par un sas spécial, où chaque officier du KGB doit décliner son identité. Les murs, le plancher et le plafond sont équipés de doubles parois, avec isolation phonique externe pour prévenir toute écoute. Ce système est complété par l'émission permanente de sonorités multifréquences entre les parois »<sup>175</sup>. En outre, la résidence était divisée en plusieurs services ayant chacun sa compétence propre. La « Ligne X » était chargée du renseignement économique et technologique, la « Ligne PR » s'occupait de rassembler des informations à caractère politique et pratiquait la désinformation, la « Ligne N » gérait les agents illégaux, etc. Quelques salles spéciales contenaient une grande quantité d'équipements de type électronique, à des fins d'écoutes des fréquences de la police et d'interception des communications transitant par satellites. Il n'est pas interdit de penser que beaucoup d'autres pays ont organisé leur résidence selon ce type de schéma.

Les diplomates en poste à l'étranger, que ce soit en ambassade ou dans un consulat, remplissent par nature, une fonction de renseignement. En ce qui concerne le renseignement militaire, le principal capteur est l'attaché militaire<sup>176</sup>. Celui-ci dirige un service, plus ou moins grand, au sein de l'ambassade, et peut être entouré de collaborateurs parmi lesquels un attaché de l'air, de terre et un attaché naval. Les attachés sont généralement placés sous la direction des autorités militaires du pays d'origine, et l'ambassadeur ne représente qu'un supérieur hiérarchique administratif<sup>177</sup>. Chargé de recueillir des données sur l'état des forces militaires du pays hôte, les attachés militaires ont l'avantage d'être, en plus de leur statut diplomatique, protégés par une disposition de la Convention de Vienne de 1927 précisant dans son article 29, et s'ils agissent en uniforme, que : « *Ne peut être considéré comme espion que l'individu qui, agissant clandestinement, ou sous de faux prétextes, recueille ou*

---

<sup>175</sup> WOLTON (T.), *Le KGB en France*, Grasset, Paris, 1986, pp.289-290.

<sup>176</sup> Les Prussiens ont été les premiers à installer des attachés militaires en ambassade.

<sup>177</sup> Les attachés français sont placés sous l'autorité directe de la Direction du Renseignement Militaire (DRM).

*tente de recueillir des renseignements dans la zone d'opération d'un belligérant, ce dans l'intention de les communiquer à l'adversaire »<sup>178</sup>.*

Toutefois, nous pouvons considérer que le plus important agent de renseignement officiel est certainement l'ambassadeur lui-même. Dès son arrivée dans le pays d'accueil, ce dernier doit apprendre certaines données nécessaires au bon déroulement des relations diplomatiques : la géographie physique, la composition de la population, l'histoire du pays, « *ses réalisations et ses espérances* »<sup>179</sup>. L'ambassadeur doit profiter de chacun de ses déplacements à l'intérieur de son pays d'affectation pour saisir un maximum d'informations, qu'elles soient de nature visuelle ou psychologique. Comme le précise l'ambassadeur Georgy, « *tout est pour moi matière à prospection : voyages, réunions protocolaires et mondaines, visites de courtoisie aux notabilités, aux centres de production, aux fêtes populaires, aux marchés provinciaux* »<sup>180</sup>. Puis plus tard il ajoute, « *En France, les gens ont une vision très réductrice du rôle des ambassadeurs qui pratiqueraient uniquement des ronds de jambe en déambulant dans les cocktails. Or, il faut savoir que les cocktails sont les seuls endroits fréquentables. L'ambassadeur trouve à chaque instant devant sa porte trois factionnaires du pays d'accueil qui sont au courant de ses moindres déplacements. Dans ces conditions, le cocktail est le seul endroit propice aux réelles prises de contact. Le bruitage y est parfait* »<sup>181</sup>.

Du fait de ses nombreux contacts, le diplomate n'est pas seulement un capteur, mais aussi un diffuseur d'informations, notamment auprès des principales autorités du pays. « *La mission qui vous a été confiée exige que vous accédiez à l'oreille des responsables, notamment du chef d'Etat de votre résidence, des ministres de son gouvernement et en particulier de votre interlocuteur permanent, le ministre des Affaires étrangères. Il va sans dire que les contacts exigent beaucoup de psychologie et de doigté* »<sup>182</sup>. L'ambassadeur doit également mener une véritable enquête sur le passé de ses interlocuteurs, ce qui permet très souvent de mieux comprendre leur action, leur comportement présent, et surtout à venir. Ainsi est-il bon de connaître la formation dont il a bénéficié, l'endroit dans lequel il a passé

---

<sup>178</sup> DESMARETZ (G.), *Le grand livre de l'espionnage*, Editions Chiron, Paris, 1999, pp.41-42.

<sup>179</sup> GEORGY (G.), *La diplomatie française et le renseignement*, in *Approches françaises du renseignement*, Fondation pour les études de Défense, Paris, 1996, p.71.

<sup>180</sup> *idem*, p.72.

<sup>181</sup> *idem*, p.75.

<sup>182</sup> *idem*.

son enfance, les personnes qu'il a fréquentées, s'il a passé quelques années à l'étranger et pourquoi. « *On ne saurait que conseiller à l'ambassadeur de prendre sa voiture et se rendre dans les lieux qui tiennent à cœur l'intéressé* »<sup>183</sup>.

C'est un des aspects fondamentaux du renseignement humain, qu'une machine, que n'importe quelle technologie, ne pourra jamais saisir. Nous sommes tous dominés par notre façon de voir les choses, notre psychologie. Nos actions en dépendent. Notre passé, notre éducation, nos rapports aux autres font que nous agissons d'une manière et pas d'une autre. Seul un capteur humain peut tenter de le comprendre, et d'en tirer les conséquences.

Bien que le statut diplomatique permette d'exercer des fonctions de renseignement très importantes, il ne faut pas écarter le fait que les diplomates agissent, qu'ils le veuillent ou non, toujours en tant que tels, du fait de la surveillance permanente dont ils font l'objet. Une politique de renseignement nécessite donc la mise en place de réseaux illégaux, clandestins, c'est à dire sans aucune attache diplomatique, et donc sans protection. Ce moyen peut s'avérer très utile, notamment dans certains cas où la voie diplomatique ne permet aucune action, ce qui peut, par exemple, être le cas lorsque les diplomates sont soumis à des restrictions de déplacement.

## **SECTION 2- LE DEVELOPPEMENT DES RESEAUX CLANDESTINS**

La nécessité de développer une quantité suffisante de réseaux clandestins est manifeste, notamment en raison des conséquences intéressantes qu'ils peuvent engendrer quant à la qualité des informations collectées. Mais leur activation, ou leur réactivation, nécessite une organisation très complexe.

### **§1- Les conséquences bénéfiques de leur mise en œuvre**

Le monde du renseignement comporte un nombre important de facettes. La moins connue d'entre elles est incontestablement celle touchant le côté le plus sombre de l'ombre : les réseaux clandestins. Par définition, ce type de pratiques ne doit jamais être révélé au

---

<sup>183</sup> *Idem.*

grand jour. Les quelques ouvrages consacrés à l'histoire du renseignement évoquent pourtant certaines anecdotes retraçant les exploits de certains agents particulièrement brillants. Mais leur révélation ne peut qu'être le constat d'un échec.

Les agents clandestins composant ces réseaux doivent être considérés comme des artistes du renseignement, davantage que des professionnels. Le parcours de certains d'entre eux, montre à quel point une mission réussie peut apporter une manne inespérée de renseignements. Un des bénéfices majeurs exploitables d'une opération clandestine est, incontestablement, l'infiltration de « taupes » dans les institutions adverses. Toutes les écoles d'espionnage ont certainement évoqué le travail formidable du directeur des services secrets est-allemands, Misha (ou Markus) Wolf, dans les années soixante-dix. En effet, deux de ses agents avaient réussi à infiltrer les institutions politiques et secrètes de la République Fédérale Allemande, à une époque où les relations entre les deux territoires allemands étaient très tendues<sup>184</sup>. La première, Gabrielle Gast, avait été recrutée dans le département III des services secrets ouest-allemands en 1973, quatre années après avoir intégré les services secrets de l'est. Ce service était chargé de suivre les opérations concernant l'Union Soviétique, constituant ainsi un poste hautement stratégique. Elle deviendra, par la suite, chef de section au Département Analyse. Elle ne sera arrêtée qu'en 1990, après les révélations d'un collègue « retourné » des services est-allemands. Les auteurs de *l'Histoire mondiale du renseignement* précisent : « A cette époque, elle lisait avant le chancelier Kohl les notes confidentielles sur les activités est-allemandes »<sup>185</sup>.

La seconde taupe était incarnée par l'espion devenu célèbre depuis la démission du chancelier Brandt, Günter Guillaume. Considérée comme un véritable succès sur le plan théorique, cette infiltration n'aurait pas eu les conséquences espérées, car Willy Brandt, la principale victime de l'affaire, misait beaucoup sur un rapprochement entre l'est et l'ouest. Toujours est-il que Guillaume s'était installée en RFA, en 1956, en tant que responsable de réseau. Inscrit au parti social-démocrate ouest-allemand (SPD) en 1957, il devient chef du groupe socialiste au conseil municipal de Francfort, en 1968. Des enquêtes du contre-espionnage allemand sont pourtant menées à son encontre, mais elles ne révèlent, *a priori*,

---

<sup>184</sup> FALIGOT (R.), KAUFFER (R.), *Histoire mondiale du renseignement- Tome 2:De la guerre froide à nos jours*, Robert Laffont, Paris, 1994, pp.377-379.

<sup>185</sup> *idem*.

rien d'anormal. En 1972, il devient le secrétaire du chancelier Brandt, chargé des relations avec le parti et les syndicats. Brandt demandera même à Guillaume de l'accompagner lors de ses différents voyages. Depuis sa position, l'agent est-allemand avait accès à une incroyable quantité d'informations qu'aucune technologie n'aurait pu collecter, notamment en ce qui concerne l'état d'esprit du chancelier. En dépit des nombreuses mesures de sécurité, beaucoup de pays ont connu des affaires d'infiltration de leurs services de renseignement, ou d'organisations politiques, militaires ou scientifiques.

Au-delà de l'apport en renseignements de grande valeur, les réseaux clandestins permettent aux services secrets de mener des « opérations secrètes », ou *Covert actions* selon la terminologie américaine. Le but de telles opérations est d'intervenir dans les affaires internes d'un pays tiers par l'intermédiaire de moyens secrets, sans que ce pays n'ait connaissance, à aucun moment, de l'intervention de l'Etat menant l'opération. Il existerait cinq types d'opérations secrètes<sup>186</sup> :

- **Les opérations psychologiques et de propagande** : il peut s'agir de propagande plus ou moins secrète (dite propagande grise), mais utilisant les médias connus du public, tels la télévision, la radio, ou la presse écrite. Ou bien il peut s'agir de propagande totalement secrète, consistant à produire des informations fausses transitant par des canaux moins publics.
- **Les opérations politiques** : leur but est de tenter d'influencer des hommes politiques afin de déstabiliser des ennemis ou adversaires, ou bien de maintenir des personnes au pouvoir.
- **Les opérations d'assistance militaire clandestine** : il s'agit ici de fournir des matériels de guerre, des instructeurs et des informations à des groupuscules situés à l'étranger, et constituant soit des groupes d'opposition au pouvoir, soit des militaires favorables au régime en place.

---

<sup>186</sup> D'AUMALE (G.), FAURE (J-P.), *Guide de l'espionnage et du contre-espionnage*, Le cherche midi éditeur, Paris, 1998, p.325.

- **Les opérations spéciales** : celles-ci ont davantage un caractère purement militaire puisqu'il s'agit en général de sabotages ou d'exfiltration d'hommes et de matériels situés en zone de guerre.
  
- **Les opérations économiques** : leur but est de déstabiliser un Etat en menant, à son encontre, un certain nombre d'attaques visant son économie (Les embargos ou blocus ne sont pas concernés puisqu'il s'agit de sanctions officielles prises publiquement). Elles peuvent toucher aussi bien les entreprises florissantes d'un pays, que la valeur d'une monnaie nationale ou régionale.

L'activation, ou la réactivation, de réseaux clandestins semble absolument nécessaire en ce qui concerne le format des politiques de renseignement du futur. Il suffit de voir, aujourd'hui, quels sont les principaux risques de déstabilisation inhérents à la sécurité des Etats, pour constater qu'ils proviennent d'Etats ou de groupuscules très fermés et difficilement accessibles. Pendant la guerre froide, le seul moyen de pénétrer en Union Soviétique de manière discrète était l'infiltration. De plus, les diplomates en place à Moscou étaient souvent limités dans leurs déplacements. Comment donc savoir ce qui se passait du côté de Mourmansk ou d'Irkoutsk sans que les « diplomates » puissent y accéder ? Nous croyons, pour beaucoup d'entre nous, que l'effondrement de l'URSS a résolu tous nos problèmes de sécurité. Mais les risques concernent, aujourd'hui, des pays dont l'ouverture au monde est loin d'être assurée : la Corée du Nord, l'Iran, la Libye, la Syrie, etc. Ces « *rogue states* » sont devenus une préoccupation majeure, car ils n'hésitent pas à financer ou abriter des entreprises terroristes dirigés à l'encontre des intérêts occidentaux.

Nous devrions repenser notre action clandestine à l'encontre de ces milieux très fermés. L'infiltration est une mission certes difficile et périlleuse, mais l'action des services de renseignement doit aller dans ce sens. Les composantes de ces groupes utilisent certainement des moyens technologiques pour communiquer, mais ils sont les premiers à s'en méfier. Comment se fait-il que personne ne sache précisément où se trouve le présumé terroriste Ben Laden ? Seuls des agents clandestins infiltrés dans ces organisations pourraient apporter un élément de réponse. Pour cela, est-il nécessaire de savoir organiser la mise en place de réseaux adaptés.

## §2- Organisation d'un réseau clandestin

Un réseau consiste en une structure verticale de chaînes et de cellules qui permettent une transmission des informations recueillies, de la base vers le sommet. Il peut exister une multitude de cellules, composées indifféremment d'un ou de plusieurs éléments.

Une des règles de sécurité fondamentale, dans un réseau, est l'herméticité de celui-ci. En effet, pour éviter une chute en chaîne, comme avec les dominos, les agents agissant dans un réseau ne sont tenus au courant que des informations absolument capitales à l'accomplissement de leurs tâches. Ainsi, il est rare qu'ils connaissent l'identité des autres membres de la cellule, et encore moins du réseau tout entier. Seuls les éléments de coordination des missions en ont plus ou moins connaissance, selon leur place dans la hiérarchie de l'organigramme : l'officier traitant et le résident. Ils constituent en même temps des cloisonnements horizontaux du réseau. Dans le cas où un intermédiaire serait démasqué, les autres éléments ne risquent pas d'être compromis.

Le résident est situé au sommet de la pyramide. Il peut être un agent légal ou illégal. Son rôle est d'assurer le bon fonctionnement, la sécurité et la productivité du réseau. Pour cela, il s'immisce dans les procédures de recrutement et d'instruction d'agents, effectuées par d'autres intermédiaires, les officiers recruteurs. Le résident entretient également des contacts discrets avec ses officiers traitants qui sont chargés de le représenter dans la gestion d'une partie du réseau, les cellules. Un officier traitant de qualité doit : *« être pénétré de sa mission ; posséder une certaine autorité sur ses sous-agents, instruire son sous-agent des procédures de sécurité et des moyens d'utilisation du matériel technique, ne jamais un sous-agent dans un domaine qui ne le concerne pas, exploiter la source ou le sous-agent au maximum de ses possibilités, veiller en permanence à la sécurité du réseau, renforcer la motivation des sous-agents, donner des directives »*<sup>187</sup>.

Les liaisons entre les membres du réseau sont assurées soit par des rencontres, en public ou en privé, soit par un système de boîte aux lettres mortes.

---

<sup>187</sup> DESMARETZ (G.), *Le grand livre de l'espionnage*, Editions Chiron, Paris, 1999, pp.87-88.

En ce qui concerne les entrevues, plus ou moins rapides, elles sont toujours sécurisées au maximum. Les agents peuvent décider de se rencontrer dans un endroit très fréquenté en faisant mine de se connaître, et discuter, comme tout le monde. L'important est de ne pas montrer que l'on veut dissimuler un échange. D'autres méthodes consistent à se retrouver dans un lieu isolé, tout en prenant le soin de ne pas entrer par les mêmes accès, et de prévoir un itinéraire de fuite, en cas d'intervention des services de contre-espionnage. Ceci demande aux membres du réseau de préparer leurs rencontres dans les moindres détails. Ainsi des signaux d'alerte doivent être convenus à l'avance, dans les cas où un des agents aurait des doutes quant aux conditions de sécurité de la rencontre. Il existe cependant des moyens d'échange beaucoup moins risqués, notamment depuis l'apparition d'Internet.

En effet, le principe des boîtes aux lettres mortes a été modernisé grâce aux réseaux informatiques. A la base, il s'agissait, pour un agent, de sélectionner quelques emplacements (généralement dans une ville) capables d'abriter des messages ou des objets divers, afin qu'un autre membre du réseau puisse les récupérer plus tard. Il peut s'agir d'une véritable boîte à lettre non utilisée, d'un trou dans un arbre, d'un plafond de toilettes de restaurant, etc. Les lieux sont cependant très étudiés puisqu'ils doivent permettre un dépôt et un retrait discrets de courrier. Mais grâce à l'Internet, sont apparus les courriers et boîtes à lettres électroniques, les *e-mails*. Ils permettent d'acheminer, non seulement des messages simples, tels que le texte, mais aussi des images pouvant contenir des micro-points difficiles à découvrir, ou même des vidéos. Dans ce cas, le danger est inexistant, car il est possible de se connecter sur le réseau, à partir de n'importe quel ordinateur branché sur une ligne téléphonique.

En outre, un réseau sera d'autant plus efficace que ses membres disposeront de couvertures crédibles. Cette précaution ne concerne généralement pas les informateurs recrutés ponctuellement, mais les agents NOC (*Non official cover*) illégaux, membres d'un service secret. Une couverture sert à masquer les activités d'espionnage d'un agent NOC, en lui donnant un aspect extérieur respectable, aux yeux des personnes avec qui il est en contact. L'activation, ou la réactivation, de réseaux clandestins, ne peut se passer d'une telle formalité. Il en va de même pour la «biographie» de l'agent, c'est à dire l'histoire officielle de sa vie. Celle-ci doit parfaitement coller au caractère de l'agent, sans quoi il sera assez facile de le démasquer.

Mais, au-delà de ces éléments très pratiques, nous pouvons constater que l'organisation d'un tel réseau demande beaucoup d'efforts d'observation et d'analyse de l'environnement dans lequel un agent va se plonger. De même, l'autre élément important est le facteur temps. On ne peut pas arriver dans un pays, et immédiatement entamer des activités d'espionnage. Il faut le temps de s'implanter, de se familiariser avec les lieux, de se faire des « amis », etc. En somme, il ne faut pas attirer les regards indiscrets vers soi. De telles implantations peuvent durer des années, pendant lesquelles le lien avec le monde du renseignement doit être rompu. Mais existe-t-il, aujourd'hui, des personnes capables de mener une telle double-vie, séparé du cadre familial et, de surcroît, à l'étranger, dans des milieux souvent très hostiles ?

Inversement, un agent trop bien implanté, notamment en cas d'infiltration dans une organisation criminelle, ne risque-t-il pas de subir une sorte de dérivé du syndrome de Stockholm vis à vis de ses « collègues », et se rapprocher, petit à petit, de leur idéologie ou de leur façon de voir les choses ? De même, une infiltration trop poussée ne risque-t-elle pas d'avoir des conséquences fâcheuses pour l'agent, en cas d'intervention des forces de l'ordre ? Ce fut le cas avec l'agent britannique Ian Mc Leod. Ecossois<sup>188</sup>, celui-ci a fait partie de la *Royal Air Force* (RAF) au début des années soixante. Quelque temps après, il faisait partie du MI6, et travaillait en poste à Stuttgart, en Allemagne. En 1968, il semble attiré par les mouvements gauchistes allemands, et prend l'apparence physique des jeunes militants : cheveux longs et pattes d'éléphant. Il réussit à intégrer les différents groupuscules, et nouera des contacts avec l'autre RAF (*La Rote Armee Fraktion* ou Fraction Armée Rouge), notamment en leur fournissant des armes. Ainsi, le MI6 a pu informer les autorités allemandes sur les opérations de l'organisation terroriste, sans pour autant dévoiler leur source. Mais, lors d'une intervention policière, Mc Leod fut pris pour un terroriste par les agents du *Bundeskriminalam*, et tué au cours de la fusillade.

---

<sup>188</sup> FALIGOT (R.), KAUFFER (R.), *Histoire mondiale du renseignement- Tome 2:De la guerre froide à nos jours*, Robert Laffont, Paris, 1994, pp.275-276.

## CONCLUSION

*Science sans conscience n'est que ruine de l'âme.*

Rabelais

L'objet de notre étude n'a pas été de dénigrer l'importance de la technologie. Elle nous sert tous les jours, nous facilite la vie, et nous ne pouvons que nous en accommoder. Mais le constat que nous avons pu faire, au cours des nombreuses lectures, est clair. La place de l'Homme dans le monde du renseignement a changé depuis une décennie. Il n'est plus mis au centre des préoccupations des responsables du renseignement. Même si les budgets, concernant ce domaine de la Défense, sont en constante progression, l'objectif premier est de se doter d'outils technologiques spatiaux, au détriment de la force humaine sur le terrain. Or les deux sont importants. Ils doivent se compléter. L'un doit permettre de recouper les informations captées par l'autre. La technologie doit servir l'Homme dans sa tâche d'acquisition de l'information cachée. Mais la tendance ne va pas dans ce sens.

Les décideurs ont trop rapidement pensé que la technologie était l'instrument clé qui leur donnerait accès à toutes les informations recherchées. Il n'est pas faux de dire qu'ils ont les moyens de savoir beaucoup de choses, notamment par l'intermédiaire des satellites d'observation et d'écoute. Mais est-il bon de tout savoir ? Avons-nous ce besoin là ? Même un pays comme les Etats-Unis, fort de sa communauté du renseignement technique, rencontre des difficultés dans la recherche et le traitement de l'information. Ils ont fait le choix de tout savoir, sans poser la question de savoir ce qu'ils désiraient vraiment connaître. Leur budget de renseignement technique est colossal. Celui de la CIA, ne concerne plus qu'une petite part du budget global de leur multinationale de l'espionnage. Et les résultats ne sont pas vraiment convaincants. Leurs récents échecs ont mis en colère certains politiques américains, fustigeant un budget non justifié, au regard des résultats obtenus.

Les ordinateurs, les technologies en général, n'ont pas encore atteint un degré d'intelligence artificielle suffisant pour se passer des directives de l'Homme. S'ils ne sont

pas programmés correctement, ils n'iront pas rechercher une information non demandée. Pour cela, il faut des Hommes capables de savoir où se trouve l'information. Derrière chaque machine, il y a un Homme. Celui-ci est omniprésent. Il est présent dans toutes les étapes du cycle du renseignement. Pourquoi tout miser sur la technologie, quand il suffit de collecter les synthèses rédigées quotidiennement, à l'attention des décideurs, pour connaître les orientations d'un pays ou d'une entreprise ?

Bien sûr, il existe des domaines dans lesquels seule la technologie peut apporter une aide décisive, notamment dans le cadre du renseignement militaire. Mais les temps ont changé. Nous l'avons vu plus tôt, ce n'est plus principalement le domaine militaire qui pose problème. Les préoccupations sont devenues globales: la lutte contre le terrorisme international, la guerre économique, le développement des mafias, etc. Pour qu'une technologie soit utile, il faut que les informations recherchées soient décelables par elle. Or il n'est pas possible de savoir ce qui se passe dans la tête d'un homme ou d'une femme, à moins de le fréquenter et de converser avec. Le renseignement devrait davantage être tourné vers l'aspect psychologique. Pour cela il faut pouvoir gagner la confiance de la personne ciblée, de connaître sa vie. Seule une personne sensible pourra comprendre son interlocuteur. Une machine n'a jamais été sensible. Ce n'est pas sa fonction.

En outre, le haut niveau de sophistication des technologies actuelles, permet de connaître beaucoup d'informations ne concernant pas exclusivement les personnes ciblées. Le fait de tout savoir implique le fait que tout ce qui est émis par quelqu'un, ou par une machine, est intercepté par les services spéciaux. Ce qui ne va pas sans poser quelques interrogations. Les pays utilisant ces moyens technologiques se réclament, pour la plupart, d'un idéal démocratique. Or, une démocratie fonctionne selon certaines règles, notamment le droit aux libertés publiques. Où se situe la frontière entre la nécessité de maintenir la sécurité d'un pays, et celle de respecter la vie privée des individus ? Certains diront que les gens qui n'ont rien à se reprocher, n'ont rien à dissimuler. Cela nous paraît très excessif, car tous les fondements de notre société libre seraient ainsi remis en cause. Cela étant, certains pays sont totalement étrangers à ces préoccupations, et n'hésitent pas à employer les moyens les plus répréhensibles pour mener à bien leurs opérations de renseignement. Un pays démocratique peut-il se permettre de respecter une certaine éthique, quand ses adversaires n'en ont pas ?

Finalement, l'utilisation non équilibrée des nouvelles technologies, tant dans notre vie quotidienne, que dans le monde du renseignement, doit nous interpeller sur le rapport que nous entretenons avec le progrès. Devons-nous reposer exclusivement sur les avantages apportés par ce qui ne constitue en fait que des machines, ou devons-nous davantage faire confiance à nos propres capacités ? La seconde solution nous paraît la plus appropriée. Bien sûr, tout est question de complémentarité entre les moyens dont nous disposons. Aucun élément n'est à exclure radicalement. Mais pour que le renseignement humain retrouve ses lettres de noblesse, il faudra engager une véritable stratégie de ressources humaines au sein des différents organismes chargés de recueillir le renseignement.

## Bibliographie

### OUVRAGES

ALEM (J.), *L'espionnage et le contre-espionnage*, Paris, PUF, Collection Que sais-je ?, n°1819, 1980, 124p.

AUER (F.), *Comment se protéger de l'espionnage, de la malveillance et de l'intelligence économique*, Secret Consulting, Malakoff, France, 1997, 153p.

AGRANOVSKY (V.), *Confessions d'un espion russe*, Messidor, Paris, 1990, 191p.

ANDREW (C.), GORDIEVSKY (O.), *Le KGB dans le monde*, Fayard, Paris, 1990, 754p.

BAUD (J.), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris, 1997, 524p.

BAUD (J.), *Encyclopédie des terrorismes*, Lavauzelle, Paris, 1999, 270p.

BESSION (B.), POSSIN (J-C.), *Du renseignement à l'intelligence économique*, Dunod, Paris, 1996.

BURDAN (D.), *DST – Neuf ans à la division antiterroriste*, Robert Laffont, Paris, 1990, 385p.

CECILE (J-J.), *Le renseignement français à l'aube du XXIème siècle*, Lavauzelle, Paris, 1998, 256p.

CECILE (J-J.), *Les SAS – Commandos secrets de Sa Majesté*, Histoire & Collections, Paris, 1997, 373p.

CROZIER (B.), HUYN (H.), MENGES (C.), SABLIER (E.), *Le Phénix Rouge*, Editions du Rocher, Monaco, 1995, 326p.

D'AUMALE (G.), FAURE (J-P.), *Guide de l'espionnage et du contre-espionnage*, Le cherche midi éditeur, Paris, 1998, 510p.

DAN (U.), *Mossad – 50 ans de guerre secrète*, Presses de la Cité, Paris, 1995, 394p.

DASQUIE (G.), *Secrètes affaires, les services secrets infiltrent les entreprises*, Flammarion, Paris, 1999, 323p.

DESMARETZ (G.), *Le grand livre de l'espionnage*, Editions Chiron, Paris, 1999, 253p.

- DEWERPE (A.), *Espion – Une anthropologie historique du secret d’Etat contemporain*, Gallimard, Paris, 1994, 478p.
- ETIENNE (G.), MONIQUET (C.), *Histoire de l’espionnage mondial*, Editions du Félin, Paris, 1997, 446p.
- FALIGOT (R.), *Nai sho*, La Découverte – Enquêtes, Paris, 1997, 381p.
- FALIGOT (R.), KAUFFER (R.), *Histoire mondiale du renseignement- Tome 1 :1870-1939*, Robert Laffont, Paris, 1993, 572p.
- FALIGOT (R.), KAUFFER (R.), *Histoire mondiale du renseignement- Tome 2 :De la guerre froide à nos jours*, Robert Laffont, Paris, 1994, 563p.
- FALIGOT (R.)& KAUFFER (R.), *DST Police secrète*, Flammarion, Paris, 1999, 670p.
- GUISNEL (J.), *Guerres dans le cyberspace*, La Découverte – Enquêtes, Paris, 1995, 252p.
- HENRI (B.), *Le renseignement – Un enjeu de pouvoir*, Economica, Paris, 1998, 182p.
- IHEDN (Institut des Hautes Etudes de Défense Nationale), *Comprendre la Défense*, Economica, Paris, 1999, 258p.
- KISH (J.), *International law and espionnage*, Martinus Nijhoff Publishers, The Hague (NDL), 1995, 162p.
- KNIGHT (A.), *Spies without cloaks – The KGB’s Successors*, Princeton University Press, Princeton, New Jersey, USA, 1998, third printing, 318p.
- KOSTINE (S.), *Bonjour Farewell*, Robert Laffont, Paris, 1997, 333p.
- KROP (P.), *Les secrets de l’espionnage français*, Editions Payot & Rivages, Paris, 1995, 782p.
- LE DORAN (S.) , ROSE (P.), *Cyber Mafias*, Editions Denoël, Paris, 1998, 342p.
- MALLERET (T.), DELAPORTE (M.), *L’Armée rouge face à la Perestroï ka*, Editions Complexe, Paris, 1991, 303p.
- MARIE- SCHWARTZENBERG (N.), *Le KGB*, PUF, Collection Que sais-je ?, Paris, n°2757, 1993, 126p.
- PILLAS (J-M.), *Nos agents à La Havane*, Albin Michel, Paris, 1995, 267p.
- RICHELSON (J.), *The U.S. Intelligence community*, Westview Press, San Francisco, Third Edition, 1995, 524p.
- SCHWEIZER (P.), « *Les nouveaux espions : le pillage technologique des USA par leurs alliés* », Grasset, Paris, 1993, 344p.

SILBERZAHN (C.), GUISNEL (J.), *Au cœur du secret*, Fayard, Paris, 1995, 330p.

SOUDOPLATOV (P&A.), *Missions Spéciales*, Seuil, Paris, 1994, 612p.

VOLKOFF (V.), *Petite Histoire de la Désinformation*, Editions du Rocher, Monaco, 1998, 291p.

WARUSFEL (B.), *Contre-espionnage et protection du secret*, Lavauzelle, Panazol, 2000, 496p.

WOLTON (T.), *Le KGB en France*, Grasset, Paris, 1986, 310p.

WOLTON (T.), *Le grand recrutement*, Grasset, Paris, 1993, 397p.

WRIGHT (P.), *Spycatcher*, William Heinemann, Australia, 1987, 392p.

## **ETUDES**

MANDEVILLE (L.), *Russie : quel système de sécurité ? Les ministères d'autorité*, La documentation française, Paris, Série Russie, n°778, 3-01-1997, 74p.

LACOSTE (P.) sous la direction de, *Approches françaises du renseignement*, Fondation pour les études de Défense, Paris, 1996, 157p.

PAECHT (A.), *Rapport sur la proposition de loi tendant à la création d'une délégation parlementaire pour les affaires de renseignement*, n°1951, novembre 1999, 99p.

De VILLEPIN (X.), *Opération « Force alliée » en Yougoslavie*, Rapport d'information n°464 de la Commission des affaires étrangères de l'Assemblée Nationale, 1998-1999.

Délégation à l'information et à la communication de la Défense, *Lancement du satellite Hélios 1B*, Défense Actu, n°39, 4 décembre 1999, pp.23-34

## **MEMOIRES & THESES & CONFERENCES**

CAPPELLE (F.), *Le monde du renseignement de l'An 2000 : restructuration des services et nouveaux enjeux*, Mémoire de DEA Défense Nationale et sécurité européenne, Université Lille II, 1998-1999.

VANDENBERGUE (N.), *Le renseignement scientifique, technologique et économique*, Mémoire de DEA Défense Nationale et sécurité européenne, Université Lille II, 1993-1994, 143p.

WARUSFEL (B.), *Le renseignement stratégique*, Conférence donnée à l'IHEDN le vendredi 3 mars 2000.

## ARTICLES

### Revues

ADAMAS (J.), *Day of the Pentagon mindbenders*, The Sunday Times, 3 décembre 1995, p.21.

ANDRONOV (A.), *American geosynchronous SIGINT satellites*, Zarubezhnoye voyennoye obozreniye, n°12, 1993, pp. 37-43.

BOTBOL (M.), *Le F.B.I. renforce ses liens en Europe centrale*, Le monde du renseignement, n°374, 20 janvier 2000, p.4.

BOUDEN (D.), *La nouvelle donne de l'espace militaire américain*, L'Armement, n°59, octobre 1997.

BRISARD (J-C.), *Services de renseignement et intérêts commerciaux américains*, Défense Nationale, juillet 2000, pp.98-112.

BRISSART (J.), *Les études dans le domaine des systèmes spatiaux*, L'Armement, n°65, mars 1999.

BRUNOT ( P.), *Le contrôle parlementaire des politiques de renseignement*, Défense Nationale, février 1997, pp.55-63.

CHAIX (N.), *Pour une adaptation du renseignement français ?*, Fondation pour les Etudes de Défense, 1996, pp.155-199.

CHAMBOST (G.), *Les avions sans pilote passent à l'attaque*, Science & Vie, n°965, février 1998, pp.114-123.

CRAG (M.), *Echelon, vers l'écoute totale de la planète*, Science & Vie, n°995, août 2000, pp.100-117.

DELMAIRE (G.), *Systèmes d'information mondiaux et renseignement par satellites*, Défense Nationale, Août-septembre 1997, pp. 137-145.

De KERZAUSON (Y.) entretien avec, *A l'écoute du monde... la DRM*, Armées d'aujourd'hui, n°245, novembre 1999, pp.14-17.

DENECE (E.), *Pour un Conseil national de sécurité*, Défense Nationale, novembre 1995, pp.29-35.

DOLLUBRY (M.), *Le renseignement dans les démocraties occidentales*, Les Cahiers de la sécurité intérieure, n°30, 1997, pp.53-85.

ELIE (B.), ABOUT (N.), BELLAIS (R.), CASTILLON (P.), DENECE (E.), *Dossier : Du renseignement*, Défense Nationale, janvier 1998.

ERHARDT (P.), *Le renseignement aérien piloté a-t-il encore un avenir ?*, Enjeux Atlantiques, n°15, juin 1997.

FAUCON (F.), *Guerre de l'information ou opérations d'information ?*, Défense Nationale, mars 1998, pp.65-77.

FELLWOCK (P.), *U.S. electronic espionage : a Memoir*, Ramparts, Vol.11, n°2, Août 1997, pp.33-50.

FESSARD de FOUCAULT (B.), *L'ambassadeur et le renseignement*, avril 1999, pp.87-100.

FORON (Lieutenant-Colonel), *L'utilisation militaire de l'espace*, Armées d'aujourd'hui, n°170, mai 1992, pp.50-52.

HERSH (S.), *The Intelligence Gap*, The New Yorker, 6 décembre 1999, pp.58-76.

ISNARD (J.), *Renseignement – L'indispensable évolution*, Armées d'aujourd'hui, n°203, septembre 1995, pp.108-111.

KLEN (M.), *Les coulisses de la Désinformation*, Défense Nationale, n°5, mai 1996, pp.83-94.

KLEN (M.), *La nouvelle bataille du renseignement*, Défense Nationale, juin 1993, pp.47-58.

KLEN (M.), *Le renseignement de l'an 2000*, Défense Nationale, octobre 1995, pp.29-43.

KLEN (M.), *La crise d'identité du renseignement*, Défense Nationale, juillet 1998, pp.93-105.

IVARNEZ (R.), *L'opération et le contrôle des satellites*, Bulletin de documentation de l'armée de l'air, n°523, mars 1998, pp.44-49.

LABBE (M-H.), *Les essais nucléaires et la non-prolifération*, Politique étrangère, Automne 1998, pp.531-547

LACOSTE (P.), *Du renseignement et des Hommes*, Défense Nationale, octobre 1994, pp.41-49.

LACOSTE (P.), *Une nouvelle stratégie pour le renseignement ?*, Politique étrangère, Printemps 1997, 83-97.

LAMBERT (D.), *La défense par les armes et la défense par l'esprit*, Défense Nationale, novembre 1995, pp.19-27.

LAVAUT (P.), *Contre-renseignement, contre-ingérence et maîtrise de l'information*, Défense Nationale, novembre 1998, pp.57-67.

MANICACCI (R.), *Le citoyen et la sécurité nationale*, Défense Nationale, novembre 1995, pp.83-93.

MELNIK (C.), GORDIEVSKY (O.), HELMS (R.), ISNARD (J.), *Plaidoyer pour les services secrets- La deuxième vie du KGB*, Politique, Politique Internationale, n°56, Juin 1992, pp.373-416.

MESMIN (O.), *L'enseignement d'un droit de l'espace applicable à l'espace militaire est-il aujourd'hui possible ?*, Bulletin de documentation de l'armée de l'air, n°505, mai 1996, pp.18-27.

PICHOT-DUCLOS (J.), *Pour une culture du renseignement*, Défense Nationale, mai 1992, pp.9-20.

RICHARDSON (D.), *Les drones – poussins qui deviennent vautours*, Armada International, mai 1995.

ROLLAND (I.), *Protection du patrimoine industriel, technologique et scientifique français*, Administration, n°180, décembre 1998, pp.42-46.

SCHWEIZER (P.), *The growth of Economic espionage*, Foreign Affairs, n°1, janvier 1996, pp.9-15.

SLAVINSKY (M.), *Le singulier renouveau des services spéciaux de la Fédération de Russie*, Horizons Nouveaux, n°104, Septembre 1992, pp.9-13.

TÖLLBORG (D.), *Réflexions sur les limites de la transparence démocratique – Quelques exemples à partir du cas suédois*, Les cahiers de la sécurité intérieure, n°30, 1997, pp.129-139.

Historia, *Dossier : Les services secrets français en action*, n°602, février 1997, pp.29-77.

Presse

AUDIBERT (D.), *CIA – Enquête sur un mythe*, Le Point, n°1420, 3 décembre 1999, pp.76-93.

CALABUIG (E.), *Après-guerre froide en Europe arctique*, Le monde diplomatique, septembre 1996, pp.22-23.

CHALET (M.), « Farewell », *espion anticonformiste*, Le Monde des Livres, 14 février 1997, p.14.

DE BEER (P.), *Les Etats-Unis se défendent d'utiliser le réseau d'espionnage Echelon à des fins industrielles*, Le Monde, 25 février 2000, p.3.

FEDARKO (K.), *Saddam's CIA coup*, Time Magazine, 23 septembre 1996, pp.20-22.

GUISNEL (J.), *Espionnage : les français aussi écoutent leurs alliés*, Le Point, 6 juin 1998, n°1342, pp.60-64.

INCIYAN (E.), *La police française lutte avec difficulté contre la cybercriminalité*, Le Monde, 22-09-1998, p.9.

ISNARD (J.), *Une alliance secrète entre la NSA et la CIA*, Le Monde, 23 février 2000, p.2.

ISNARD (J.), *La sainte alliance de l'espionnage*, Le Monde, 30 mars 2000, p.16.

ISNARD (J.), *Les espions font leur révolution culturelle*, Le Monde, 24 février 1995, p.1.

LE GENDRE (B.), *Opération « Overflight »*, Le Monde, 2 mai 2000, p.14.

Mc GEARY (J.), *Nukes ... They're back*, Time Magazine, 25 mai 1998, pp.22-29.

MELNIK (C.), *Les « écoutes » et le pouvoir personnel*, Le Monde, 22 octobre 1996, p.16.

NELAN (B.), *Bugging Saddam*, Time magazine, 18 janvier 1999, pp.30-31.

PEYROT (M.), *Francis Temperville, l'espion du CEA qui se disait menacé*, Le Monde, 25 octobre 1997, p.14.

POSTEL – VINAY (O.), *Cerveaux à vendre à Tomsk, l'Athènes de Sibérie*, Le Monde Economie, 9 septembre 1997, p.6

WALLER (D.), *Onward cyber soldiers*, Time Magazine, 21 août 1995, pp.22-30.

WALLER (D.), *Why the spies missed the desert blasts*, Time Magazine, 25 mai 1998, p.28.

ZECCHINI (L.), *Comment les Etats-Unis espionnent l'Europe*, Le Monde, 23 février 2000, p.1.

Courrier International, *Dossier : Attention, vous êtes sur écoutes*, n°387, semaine du 2 au 8 avril 1998, pp.39-41.

Courrier International, *Dossier : La fin de la vie privée*, n°474, semaine du 2 au 8 décembre 1999, pp.42-47.

L'Expansion, 10-07-1995, *Dossier : Comment la CIA déstabilise les entreprises françaises*.

Le Nouvel Observateur, *Dossier : Comment l'Amérique nous espionne*, 10-09-1998, n°1779, pp.10-28.

## Sites Internet

- [www.defenselink.mil](http://www.defenselink.mil)
- [www.indigo-net.com/lmr.html](http://www.indigo-net.com/lmr.html)
- [www.infowar.com](http://www.infowar.com)
- [www.fas.org](http://www.fas.org)
- [www.lemonde.fr](http://www.lemonde.fr)
- [www.odci.gov/index.html](http://www.odci.gov/index.html)
- [www.csis-scrs.gc.ca](http://www.csis-scrs.gc.ca)
- [www.courrier-international.com](http://www.courrier-international.com)
- [www.commongroundradio.org](http://www.commongroundradio.org)
- [www.kimsoft.com](http://www.kimsoft.com)
- [www.cnn.com](http://www.cnn.com)
- [cryptome.org](http://cryptome.org)
- [www.nytimes.com](http://www.nytimes.com)
- [www.the-times.co.uk](http://www.the-times.co.uk)
- [www.mi5.gov.uk](http://www.mi5.gov.uk)