Romain Foliard. 2008

Master II – Etudes Stratégiques.

Université Paris 13.

Renseignement et lutte contre le terrorisme:

De la fin de la Guerre Froide jusqu'à nos jours.

Ifas
Institut français d'analyse stratégique

UNIVERSITÉ PARIS 13 NORD

Sous la direction de :

Stéphane Folcher (Université Paris 13 / Ministère de l'Intérieur)

François Géré (Président de l'Institut Français d'Analyse Stratégique – IFAS)

Sommaire

Introduction Générale

La fin de l'antagonisme Est-Ouest accompagnant la chute du Mur de Berlin en 1989, puis les attentats terroristes contre les Etats-Unis le 11 septembre 2001, on fait rentrer le monde dans une nouvelle ère.

L'affrontement des deux blocs où chacun des protagonistes connaissait son ennemi et savait contre qui et quoi il se battait, a laissé la place à une situation largement troublée par l'émergence de nouveaux dangers, en provenance d'acteurs toujours plus nombreux et très difficilement prévisibles.

Les nouvelles formes de rivalités économiques, les organisations criminelles transnationales, les extrémistes violents, etc., sont apparus en même temps que la mondialisation et représentent aujourd'hui des menaces majeures sur le plan international.

Mais depuis quelques années, c'est bien le terrorisme islamique qui est au cœur des préoccupations. Il représente la menace avec le plus fort pouvoir de nuisance. Les 3000 morts des attentats du 11 septembre 2001, ainsi que les centaines de victimes à déplorer de par le monde annuellement, font de ce terrorisme l'élément de déstabilisation potentiellement le plus redoutable, le plus médiatique aussi.

Cet adversaire diffus, aux contours mal définis et utilisant à bon escient toutes les possibilités offertes par la mondialisation au sens large (notamment celles issues de la révolution des technologies de l'information), évolue dans un nouvel environnement, caractérisé non plus par l'affrontement idéologique mais par l'imbrication des enjeux et la multiplication des risques. La rupture avec la période de la Guerre Froide est donc totale.

Aujourd'hui, la menace première est avant tout « asymétrique » et elle impose de reconsidérer les moyens mis en œuvre pour assurer la défense et la sécurité des Etats, de les adapter en permanence également.

Ainsi à la chute du mur de Berlin, mais plus encore depuis les attentats à New-York et Washington en 2001, les Etats et organisations internationales concernés, ont entrepris de faire évoluer leurs appareils de lutte contre le terrorisme.

La capacité d'adaptation de ce terrorisme islamiste est très rapide, elle constitue sa plus grande force, et elle est un défi perpétuel pour ceux qui le combattent.

L'anticipation est primordiale et le renseignement indispensable pour prévenir les opérations terroristes et les déjouer. Il est quasiment le seul moyen efficace pour éviter que ces acteurs ne passent à l'action.

Les services de renseignements, chargés de collecter, d'analyser, puis de transmettre les informations utiles aux décideurs politiques, ont donc pris une importance considérable.

Eux aussi, ont eu à s'adapter au sortir de ces décennies de Guerre Froide qui les avaient vus se développer et se structurer conformément et autour de leur mission d'origine, à savoir une fonction de défense, tournée sur l'extérieur et à visée militaire.

Mais quelle place le renseignement occupe-t-il dans le cadre de la lutte anti-terroriste ? Quel est son rôle? Quels changements se sont produits depuis le 11 septembre 2001 et plus globalement depuis la fin du monde bipolaire à partir de 1989 ? Quelles sont les perspectives souhaitables et envisageables pour le renseignement, dans le cadre de la lutte contre le terrorisme transnational ?

Dans un premier temps, nous verrons d'un point de vue général en quoi consiste le renseignement, quels sont ses moyens, son organisation mais aussi ses spécificités dans la lutte antiterroriste. Nous aborderons également ce nouveau contexte, ce nouvel environnement post Guerre Froide auquel le renseignement a dû faire face. Nous tenterons de dégager les principaux changements ayant influé sur la pratique du renseignement pendant cette période.

Puis, nous nous concentrerons sur la période post-11 septembre 2001, qui marque une réelle accélération dans l'évolution des services de renseignement, pour s'adapter à la menace du terrorisme islamique.
Comprendre les mesures mises en place par les Etats (Etats-Unis, France et pays européens principalement) et les organisations internationales (OTAN, ONU, Union Européenne) pour faire évoluer le cycle du renseignement, voir comment se sont réagencées les coopérations internationales, etc., seront quelques-uns de nos thèmes de réflexion dans cette deuxième étape.

Enfin dans une troisième et dernière partie nous tenterons de dresser un bilan et d'instaurer des perspectives. Quelles solutions peuvent être envisagées pour continuer de faire progresser la collecte, l'analyse puis la transmission du renseignement, dans le cadre de la lutte contre le terrorisme? Nous évoquerons enfin les problèmes éthiques que soulève le renseignement, son contrôle institutionnel mais aussi par sa « privatisation » grandissante, ou encore les voies futures offertes par les sources ouvertes ou l'« *Intelligence-Led Policing* ».

Introduction Chapitre 1 :

Les années 90 vont marquer la fin de l'affrontement idéologique bipolaire, l'arrivée de la mondialisation et de la révolution des nouvelles technologies de l'information et des télécommunications, etc.
Ces changements soudains vont aller de pair avec l'émergence de nouveaux acteurs qui non seulement ne vont pas être affiliés aux Etats mais qui en plus, vont contester leur souveraineté.
La politique internationale dans son ensemble va en subir les conséquences.
Le schéma « classique » hérité de la Guerre Froide n'est plus d'actualité. Les menaces deviennent de plus en plus connectées aux risques, elles sont diffuses, transnationales, les adversaires sont multiples et imprévisibles. Le terrorisme islamiste apparaît comme la menace la plus dangereuse.
Les concepts de sanctuarisation du territoire national, de séparation entre sécurité intérieure et sécurité extérieure ne sont plus valables. Assurer la sécurité et la défense d'un territoire, d'un Etat, demande désormais une approche et une connaissance globale des enjeux.

Ce contexte incertain fait de l'anticipation l'élément clé, et le renseignement devient l'arme la plus efficace pour combattre ces nouvelles menaces.

Dans ce chapitre, nous aborderons tout d'abord le rôle du renseignement. Il s'agira de rappeler des notions clés le concernant, puis d'envisager certaines spécificités dans le cadre de la lutte anti-terroriste.

Nous décrirons ensuite le nouveau contexte international qui s'est développé après la Chute du Mur et verrons quels changements il a induits dans les services de renseignement, depuis leur réorientation, dans les années 90 vers les moyens « techniques » de collecte, à visée économique, jusqu' à leur incapacité à anticiper la menace et les attentats terroristes du 11 septembre 2001.

Chapitre 1 : Le renseignement à l'ère post-bipolaire.

I) Le renseignement : pilier de la lutte anti-terroriste.

1) Présentation générale du renseignement.

a) Définition du « Renseignement ».

Avant d'étudier dans notre deuxième partie l'évolution du renseignement dans les années 90, il nous faut au préalable définir ce qu'il est, aborder son rôle, préciser sa place et sa spécificité au sein de la lutte anti-terroriste.

Comme toute notion, le renseignement est l'objet de diverses définitions.

Parmi les plus élémentaires, citons celle-ci : « *activités relevant du domaine secret* »[1].

Ou celle plus généraliste de l'amiral Lacoste : « *l'information utile […] utile à l'entreprise, à la tache assignée, à l'objectif que l'on veut atteindre* »[2].

Mais, notre travail privilégiant l'aspect « sécuritaire » du renseignement, nous retiendrons en priorité la définition donnée par Jacques Baud : « *Ensemble des activités visant à rechercher et exploiter des informations au profit d'un Etat et de ses forces armées. Il est exécuté aux niveaux stratégique, opératif et tactique, dans les domaines les plus variés* »[3].

La recherche du renseignement n'est pas nouvelle. Elle peut même être considérée comme l'une des plus anciennes activités menées par l'homme, sachant qu'elle a pu prendre des formes bien différentes au cours du temps. Elle consiste à satisfaire un besoin de connaissance, voire de curiosité sur une chose, un individu, un groupe, etc. Cependant le renseignement se distingue de la simple « information » à partir du moment où cette dernière devient un enjeu de puissance, de pouvoir, et donne lieu à la création de méthodes, d'outils et de services particuliers pour sa collecte puis son exploitation.

Il est avant tout une aide à la prise de décision, dans des domaines divers et variés : Economie, Industrie, Diplomatie, Sécurité, Défense, etc., tous sont susceptibles de faire appel au renseignement dans le cadre de leurs activités. Il s'agit de s'informer sur les intentions

[1] Frédéric Guelton, *Pourquoi le renseignement ? De l'espionnage à l'information globale*, Larousse, 2004, 152p.
[2] *Ibid.*
[3] Jacques Baud, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 2002.

d'« autrui », pour disposer de l'autonomie et de la connaissance nécessaire à la prise de décision et donc à l'action.

b) Le cycle du renseignement.

Il existe différents types d'approches, mais globalement le cycle du renseignement s'organise autour de quatre grandes phases :

- La définition de la recherche. C'est l'expression d'un besoin qui dans le cas de la lutte anti terroriste émane de l'autorité politique. Le service de renseignement, et plus particulièrement l'agent (ou les agents) sait donc ce qu'il doit chercher et dans quelle direction.

- L'action ou la collecte. Il s'agit du moment de la recherche de l'information proprement dite, et des moyens divers par lesquels elle s'effectue (activation de sources, de recherche clandestine, etc.).

- L'exploitation / analyse. C'est le travail des analystes qui doivent « trier » l'information utile, pertinente et la dissocier du reste.

- La diffusion. C'est la dernière phase du cycle, celle ou le renseignement recueilli est transmis au(x) décideur(s) politique(s) qui décideront de lancer (ou non) une action. C'est dans cette phase que le renseignement devient véritablement un outil d'aide pour la décision.

c) Les moyens du renseignement.

Le renseignement peut s'obtenir à partir d'une multitude d'outils, de méthodes, de capteurs issus de deux grands types de sources : les sources dites « ouvertes » et les sources dites « fermées »[4].

Les premières représentent l'ensemble des moyens d'informations accessibles à tous, gratuitement ou non. Aujourd'hui on estime que près de 80% de l'information utile aux services de renseignement en matière de lutte anti-terroriste, provient de ces sources « ouvertes », en premier lieu d'Internet.

Les sources dites « fermées » englobent tous les moyens clandestins de collecte de l'information qu'ils soient illégaux ou non. L'essence même de ces sources « fermées »

[4] Lieutenant-colonel Barmon, *La fonction renseignement*, Objectif Doctrine, Octobre 2000.

repose sur le secret, sur la discrétion, l'important étant de ne pas se faire repérer par la cible. Les moyens pour mener la recherche peuvent être de deux types : techniques ou humains.

- Renseignement technique :

Il relève essentiellement de deux domaines:

- Le renseignement électromagnétique (*SIGINT, Signal Intelligence*) qui comprend à la fois le renseignement électronique (*ELINT, Electronic Intelligence*) et le renseignement sur les communications (*COMINT, Communication Intelligence*) ;

- Le renseignement par imagerie (*IMINT, Image Intelligence*).

A l'intérieur de chacun d'eux, il est possible d'établir des « sous catégories » selon les moyens spécifiquement employés : renseignement laser, des signatures électromagnétiques, optiques, acoustiques, photographiques, radars, etc.

Le renseignement technique utilise le plus couramment des aéronefs, des systèmes satellitaires (satellites, drones…), la cryptographie et des écoutes *COMINT* (*Communication Intelligence*).

La plupart des grandes nations du monde occidental disposent d'un service spécifique de renseignement technique, ou bien d'un système d'interception.

Il s'agit par exemple du *GCHQ* (*Government Communications HeadQuarters*) en Grande Bretagne, de la *NSA* aux Etats-Unis, de la *FAPSI* en Russie, et du système nommé « *Frenchelon* » en France.

Les avantages du renseignement technique sont multiples : il fournit une information concrète, fiable, pratiquement en temps réel et de n'importe quel endroit de la planète en s'affranchissant des difficultés inhérentes aux conditions politiques, géographiques ou environnementales. Mais surtout la collecte de l'information peut s'effectuer sans mettre en danger des vies humaines, et sans se faire repérer par les adversaires.

- Renseignement d'origine humaine (*ROHUM* ou *HUMINT* en anglais).

Il est obtenu par le biais d'agents de renseignement utilisant des méthodes de collecte légales ou illégales. Il englobe à la fois le *« renseignement acquis par un mode conversationnel pour lequel un capteur humain interroge une source, et le renseignement acquis par l'observation sans contact avec l'adversaire »*[5]. Le renseignement humain recouvre l'appellation MICE : « *Money, Ideology, Contraint, Ego* » par référence aux quatre méthodes principales de collecte utilisées par l'*HUMINT* :

- « Money » décrit l'achat de renseignement par le versement d'argent.
- « Ideology » évoque l'obtention de renseignement par sympathie ou conviction idéologique. Un individu accepte de transmettre des informations à l'« ennemi » parce qu'il rejette les valeurs de la société, du gouvernement, de l'entité, etc. auquel il appartient.
- « Contraints », renvoie à l'usage des méthodes de chantage, d'intimidation, voire de torture (mais qui elle concerne des cas bien spécifiques), pour l'obtention d'une information.
- « Ego » signifie appâter un individu en flattant son égo, en entretenant sa « mégalomanie » et/ou lui promettant une reconnaissance personnelle importante.

L'étude de la collecte du renseignement peut donc être abordée à partir de la méthode, en différenciant moyens « techniques » et « humains ».

Mais elle peut l'être également selon la « finalité », en envisageant par conséquent le type de « production ».

En effet, le renseignement obéit à des objectifs, à des orientations plus ou moins strictes qui vont influencer la recherche. Et lorsqu'il arrive au stade du « produit fini », il est censé répondre à la demande initiale. La recherche ne se fait pas au « hasard ».

Ainsi, on distingue plusieurs niveaux et catégories de renseignements en fonction de la nature du travail de collecte et de celle du produit analytique. Les typologies varient d'un spécialiste à l'autre, cependant nous allons tenter de faire une synthèse d'ensemble :

[5] Colonel Emmanuel Poucert, *Le renseignement de source humaine, espoirs et problèmes*, Doctrines N°09, Juin 2006.

Au sommet de la « hiérarchie », on trouve le niveau du Renseignement politico-stratégique :

Il vise à reconstituer l'« environnement général », de donner une image fidèle et à grande échelle des questions stratégiques, par la compréhension globale d'une situation, en associant comme son nom l'indique les éléments politiques et stratégiques, mais aussi sociaux, économiques, militaires, etc. Il est le fruit de la mise en commun des renseignements de tous les services, qu'ils soient militaires, civils ou sécuritaires. Dans la lutte anti-terroriste, il doit permettre d'appréhender correctement le phénomène en identifiant ses vulnérabilités et sa stratégie générale. Ce niveau de renseignement est malheureusement trop souvent négligé par les autorités politiques, car il se conçoit sur le long terme, et surtout il ne débouche pas sur des résultats susceptibles d'avoir un impact médiatique. Pourtant il apparaît tout à fait indispensable dans un domaine ou l'anticipation tactique se révèle extrêmement compliquée.

A l'intérieur de ce renseignement politico-stratégique on peut décliner deux sous catégories :

- Le Renseignement de Défense et de Sécurité Intérieures : on le retrouve parfois également sous l'appellation simple de « Renseignement de Défense » Il recouvre des situations très larges, ses contours sont assez flous. Il est censé faire la synthèse de tous les types de renseignement relevant de la Défense et de la Sécurité Nationale (renseignement politico-stratégique, militaire, économique, de police, etc.), mais dans la majorité des Etats, il n'existe pas d'entité (ou alors elle ne dispose pas de la légitimité et des moyens nécessaires) capable d'y parvenir. Dans le cadre spécifique de la lutte contre le terrorisme, cette catégorie de renseignement opère au niveau tactique pour arrêter les membres des réseaux et les mener ensuite en justice pour condamnation. Sa vocation est à la fois réactive (réunir les preuves après un attentat) mais aussi préventive puisqu'il cherche à démasquer les terroristes potentiels, à détecter des matériels pouvant servir à une opération (armes, explosifs, etc.) et qu'il s'intéresse également à la détection et la surveillance des infrastructures pouvant servir à ces mêmes actions.

- Le Renseignement militaire : il concerne les renseignements relatifs aux activités militaires et forces armées. Il prend ses directives du plus haut sommet de l'Etat, sa mission est de renseigner les autorités militaires (les Chefs d'Etats-majors) toujours dans une optique de planification des opérations. Ainsi le renseignement fonctionne à la fois en temps de paix et en temps d'engagement :

    - **En temps de paix**, il sert à la collecte puis à l'analyse des informations concernant un adversaire, ou un adversaire potentiel. Concrètement, il permet l'évaluation de ses moyens, de ses infrastructures, de ses méthodes, etc. Il s'agit par exemple de connaître les effectifs des forces armées, leur niveau de développement, la localisation des bases militaires, de repérer d'éventuels signes ou preuves d'un programme nucléaire, etc. Mais son champ d'action est

bien plus large que la simple évaluation des capacités militaires d'un ennemi. Depuis quelques années, et surtout depuis la fin du monde bipolaire, le renseignement militaire a considérablement étendu son champ d'analyse. Ainsi on parle davantage aujourd'hui de « renseignement d'intérêt militaire ». De par l'évolution des menaces il est désormais obligé de collecter des informations plus générales (connaissances du milieu géographique, du contexte politique, économique, culturel, etc.). C'est pourquoi il se confond parfois, et de plus en plus, avec le renseignement de Défense.

- **En temps d'opération militaire**, il peut concerner à la fois les niveaux stratégiques, opérationnels, et tactiques. Il apporte aux forces armées ainsi qu'à leurs responsables des renseignements qui leur seront utiles pour la planification et la conduite des opérations, des actions ou des engagements. On peut alors distinguer le « renseignement militaire de situation » qui s'intéresse à la « planification » et le « renseignement militaire de combat » qui se passe en temps réel et permet aux militaires sur le terrain de mener leurs actions.

Dans l'optique de la lutte contre le terrorisme, le renseignement militaire peut apparaître moins approprié par exemple que le renseignement de police, car par essence, la force des groupes terroriste tient justement au fait qu'ils n'engagent pas leurs actions contre les Etats sur un plan militaire, mais à partir de méthodes asymétriques, ne faisant pas appel aux forces armées conventionnelles. Cependant, contre des adversaires qui utilisent les méthodes du terrorisme mais tout en fonctionnant et agissant comme des groupes armés de guérilla, le renseignement militaire est un moyen efficace pour collecter de précieuses informations.

D'autres classifications existent : on pourra parler spécifiquement de renseignement d'anticipation, d'investigation, de documentation, de base, biographique, économique, etc., en fonction de la finalité recherchée.

Mais comment s'organise dans la réalité, la collecte du renseignement ?

d) L'orientation du renseignement.

Si le renseignement peut être catégorisé à partir des sources ou capteurs par lesquels il est collecté, l'orientation géographique qu'on lui donne est également très importante pour comprendre les nuances de cette activité, la qualifier.

Il peut être ainsi divisé selon l'espace ou le territoire visé. On distingue donc :

- **Le renseignement extérieur** : politique, diplomatique, économique, militaire, etc., l'espionnage au sens classique du terme.

- **Le renseignement intérieur** : principalement concentré sur la veille, l'infiltration et la surveillance.

Mais nous verrons par la suite, que la distinction entre le renseignement intérieur et le renseignement extérieur n'est plus adaptée, spécialement dans le cadre du terrorisme transnational et que dans de nombreux pays, elle est en train de s'effacer.

Néanmoins, elle demeure plus ou moins encore visible et c'est toujours l'« orientation » géographique du renseignement qui différencie les services œuvrant dans ce domaine entre :

- Les **services de renseignement extérieur** : En France il s'agit de la *DGSE*, de la *DRM*, de la *DST* et des *RG* (ces deux derniers forment la DCRI depuis 2008), de la DPSD ainsi que la Gendarmerie, les Douanes et la Police judiciaire de manière indirecte. On pourra citer également la *CIA* aux Etats-Unis, le *MI-6* au Royaume-Uni, le *BND* (*Bundesnachrichtendienst*) en Allemagne.

- Les **services de renseignement intérieur** : c'est par exemple la nouvelle « *Direction Centrale du Renseignement Intérieur (DCRI)* » en France, le FBI aux Etats-Unis, le *MI-5* au Royaume-Uni, le *BFV* (*Bundesant für verfassungsshutz*) en Allemagne.

- Les différentes **organes de coordination** : c'était le *CIR* en France avant la publication du livre blanc en 2008 ; il sera remplacé par le *CNR* (*Conseil National du Renseignement)* très bientôt. Il s'agit du *NSC* (*National Security Council*) aux Etats-Unis, du *DIS* (*Direction pour l'Information et la Sécurité*) en Italie, et du *Joint Intelligence Committee* au Royaume-Uni.

Enfin, le renseignement peut être appréhendé par la nature de ses activités :

e) Les activités du renseignement.

Le renseignement peut se diviser en différentes activités[6], mais qui relèvent de deux grandes catégories :

- Tout d'abord l'**espionnage** (toujours à vocation offensive) et le **contre espionnage** qui peut être défensif (protection des armées et du personnel) ou offensif (retournements d'agents, etc.).

  Ces activités d'espionnage ou de contre espionnage sont le fait d'individus que l'on nomme :

  - « Agent infiltré » ou « Taupe » pour l'espion au sens classique du terme. L'agent est infiltré dans le milieu qu'il doit surveiller. Il peut être soit « actif », soit « dormant », c'est-à-dire provisoirement et délibérément inactif (ou mis en sommeil) dans le but de renforcer sa couverture et/ou sa sécurité et il sert à informer l'organisme ou l'entité de tutelle qui l'emploie sur les agissements du milieu en question. L'objectif est le recueil de l'**information**.

  - « Agent retourné » ou « Agent double » dans le cas d'un agent au départ infiltré mais qui a été découvert et que, selon le contexte et la situation, plutôt que de le juger et le condamner, on préfère utiliser en le « retournant » contre l'organisme ou l'Etat pour le compte duquel il opérait initialement. Il va alors devoir non seulement informer son nouvel « employeur » sur ce dernier mais aussi colporter auprès de lui et bien évidemment à son insu, de fausses informations dans le but de le déstabiliser, de le leurrer. Le rôle de ce type d'agent (qui est le plus souvent « actif ») est, on le comprend, très important et stratégique. L'objectif est la **désinformation** ou l'**intoxication**.

  - « Agent provocateur » pour désigner un infiltré, implanté au sein d'un groupe, réseau ou entité, etc., qui a pour mission de recruter, de compromettre des sympathisants, de les engager dans une action de manière à les faire tomber et à les éliminer. Ainsi, pour prendre un exemple concret, pendant des années, le responsable du recrutement des activistes de l'IRA était un agent « provocateur » du service britannique MI-5 dont la mission consistait à recruter les membres de cette organisation[7]. L'agent provocateur est extrêmement précieux dans le cadre de la lutte contre le terrorisme puisqu'il permet de surveiller les membres d'un groupe terroriste, de connaître leurs projets mais aussi de repérer les personnes susceptibles de les rejoindre. Cependant il faut qu'il soit absolument fiable et que les services de sécurité

[6] *Ibid.* Frédéric Guelton Op.cit.p4

[7] Bien qu'il ne les incitait pas directement à perpétrer leurs actions, le simple fait de les recruter représentait par essence un « encouragement » indirect.

soient en mesure d'agir au moment opportun, à savoir assez tard pour que les terroristes puissent être arrêtés et poursuivis en justice, mais suffisamment tôt, avant que l'action ne soit mise à exécution. L'objectif est l'**incitation** ou la **provocation**.

- Les **actions clandestines** recouvrent l'utilisation de moyens spéciaux[8] par les services « Action » d'organismes étatiques spécialisés dans le renseignement (ex : service action de la *DGSE*), ou par des groupuscules pro-gouvernementaux.

Mais quelles sont les spécificités du renseignement au regard du terrorisme ? Quel est son apport au sein de la lutte anti-terroriste par rapport à l'action policière ou judiciaire

2) Spécificités du renseignement dans la lutte anti-terroriste.

a) Le pivot de la lutte anti-terroriste.

Le renseignement est le pivot de tout dispositif anti-terroriste, car il cherche à supprimer l'effet de « surprise » sur lequel le terrorisme s'appuie pour frapper et nuire.

Par définition, le terrorisme trouve son efficacité dans le caractère « soudain » et imprévisible de ses actions, davantage que dans sa capacité de destruction. L'efficacité première d'un attentat repose avant tout sur le « choc » instauré au sein d'un groupe ou d'une société. Nous irons même plus loin en disant que les dommages directs engendrés par l'acte terroriste (victimes, destructions etc.) sont moins importants que l'impact psychologique qu'il suscite. Comme son nom l'indique, le terrorisme entend « terroriser », provoquer le doute et la peur au sein d'une population.

Il est l'une des menaces multiformes et diffuses que compte le monde post-bipolaire, sans doute est il la plus emblématique.

Mais alors qu'il s'agissait pendant la Guerre Froide de collecter des informations sur un ennemi connu et bien déterminé, aujourd'hui le challenge principal pour les forces de sécurité et de défense est d'abord de « trouver » l'adversaire, avant même d'envisager d'obtenir des informations plus précises sur lui et en dernier lieu, de mener des actions pour le contrer.

De plus, la menace n'est pas seulement imprévisible, elle est transnationale. A l'heure où le terrorisme ne connaît plus de frontière aussi bien concernant ses cibles que ses implantations, la notion de sanctuarisation du territoire n'est plus pertinente et la collecte du renseignement,

[8] Assassinats ciblés, opérations de destruction, de sabotage, de déstabilisation, etc.

mais surtout la coopération entre les services concernés, que ce soit à l'intérieur de l'Etat ou entre les Etats eux-mêmes, est devenue une absolue nécessité et priorité. Elle s'est d'ailleurs largement développée depuis la fin de la guerre froide et davantage encore depuis le 11 septembre 2001.

Dans ce contexte le renseignement, la transmission de l'information est l'élément absolument central.

Concernant la lutte contre le terrorisme, le renseignement vise à mieux appréhender les réseaux, afin de connaître leurs moyens, leurs motivations, les opérations en préparation, les cibles potentielles, etc.

Il est le centre de toute action anti-terroriste (qu'elle soit armée ou non), et aucune opération judiciaire ou de police ne peut être lancée sans l'apport du renseignement, dont la mission première est de trouver cet adversaire « invisible ».

Il intervient en « amont » de l'action terroriste, dans une logique de prévention, pour permettre aux forces de police de démanteler les opérations en préparation, de désorganiser les réseaux, etc.

Mais il est présent aussi en « aval » soit pour appuyer l'action armée contre les groupes (le renseignement militaire joue alors un rôle central), soit dans une posture plus « classique », pour seconder les services de police dans les enquêtes en vue de la condamnation des auteurs.

Quelles sont les forces du renseignement et à l'inverse ses faiblesses dans la lutte anti-terroriste, par rapport aux autres types d'actions qui peuvent être menées contre le terrorisme (police, judiciaire, militaire…) ?

b) Forces et faiblesses.

- Renseignement technique :

Il permet de « contourner » l'impossibilité quasi-totale d'infiltration des réseaux terroristes qui, par définition, sont des structures extrêmement hermétiques.

Mais il demande la mise en œuvre de moyens technologiques souvent coûteux et très pointus que peu d'Etats dans le monde sont en mesure de financer. De plus, il délivre une information figée dans le temps à partir de laquelle il est difficile d'« extrapoler » et bien évidemment il ne peut pas atteindre le domaine « souterrain » au sein duquel de nombreux terroristes trouvent refuge.

Mais l'inconvénient majeur provient de la quantité d'information, qui est aujourd'hui largement supérieure aux capacités d'analyse des services de renseignement, les communications se comptant chaque jour par millions voire milliards.

A titre d'exemple, on estime que la *NSA* (*National Security Agency*) - la plus grande agence de renseignement technique du monde - n'est en mesure de traiter qu'entre 4 et 10% des informations collectées. Ainsi, par manque de temps, des renseignements qui auraient pu se révéler déterminants pour anticiper et empêcher les attentats du 11 septembre 2001, n'ont été analysés que le lendemain de l'opération.

- Renseignement humain :

Les moyens de collectes « humains » permettent « *d'anticiper les intentions et d'expliquer les actions de l'adversaire* »[9]. Ils donnent accès à une information « concrète » qui contrairement à celle obtenue techniquement, peut s'insérer dans un environnement global et permettre alors une meilleure vision et une évaluation des situations dans des crises ou problématiques dont la complexité et la dispersion sont devenues les traits dominants.

De plus, dans le cadre de la lutte contre le terrorisme spécifiquement, le renseignement humain se révèle pertinent par rapport au renseignement technique. En effet, beaucoup de membres des réseaux sont revenus ces dernières années à l'utilisation de modes de communications « basiques » reposant sur la transmission orale ou par le biais de « technologies » aujourd'hui « dépassées » (talkie-walkie par exemple). Ils ont compris qu'ils bénéficieraient ainsi d'une discrétion leur permettant de protéger leurs activités, sans se faire repérer par les services de renseignement, qui eux ont eu largement tendance à privilégier les moyens techniques d'interceptions pendant la dernière décennie.

Mais le renseignement humain comporte également d'importantes faiblesses. Tout d'abord il fait intervenir des hommes et des femmes dans des conditions parfois très dangereuses. Mais surtout, le recueil d'information par l'infiltration des réseaux se révèle quasiment impossible, spécialement pour les agents des services occidentaux.

En effet les réseaux terroristes et notamment islamistes fonctionnent de manière extrêmement resserrée. Les membres se connaissent depuis des années et souvent ils viennent des mêmes régions voire des mêmes villages, parlent le même dialecte, etc., l'infiltration est donc quasi impossible pour les agents de renseignement et surtout est extrêmement dangereuse.

Voici donc présentée de façon très générale, l'architecture du renseignement dans le cadre de la lutte anti terroriste. Il s'agissait d'avoir en tête les éléments clés avant de passer désormais à une approche plus concrète.

Avant d'aborder toutes les évolutions du renseignement après les attentats du 11 septembre, intéressons nous tout d'abord aux changements amorcés dès la fin de la Guerre Froide, à partir du début des années 90.

[9] Jacques Baud, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 2002.

II) Emergence d'un nouveau « contexte » et réorientation des services vers l'intelligence économique et le renseignement technique dans les années 90.

1) Emergence de nouvelles menaces et nouveaux acteurs

a) De nouvelles menaces…

La chute de l'URSS met fin à l'affrontement idéologique qui perdurait depuis près de 50 ans. Mais la « stabilisation » attendue du monde n'a pas lieu, et au contraire, des crises et des conflits se développent. L'économie s'impose comme le domaine majeur de concurrence entre les nations et de nouveaux acteurs non gouvernementaux émergent en marge des Etats, et dans certains cas s'opposent à eux (il existe au contraire des acteurs non gouvernementaux qui « assistent » l'Etat, les ONG en premier lieu). Au cours de l'histoire l'Etat-nation a toujours été contesté que se soit par des groupes religieux, des mouvements d'oppositions, etc., mais jamais ces groupes n'avaient acquis la capacité de nuisance qu'on leur connaît aujourd'hui.

Ces nouvelles menaces qui bouleversent en profondeur la politique internationale et donc la pratique du renseignement ont trait:

- Au « terrorisme islamique », « personnifié » par Al-Qaïda, organisation terroriste d'un nouveau type qui n'est soutenue par aucun Etat. Mais Al-Qaïda est avant tout une « centrale d'assistance », au sein de laquelle il n'existe aucune hiérarchie ni véritablement de stratégie concertée, et qui ne manifeste aucune revendication territoriale. Seules les cibles et l'inspiration du combat contre l'occident sont communes aux différentes cellules ou filiales se réclamant de l'organisation de par le monde. Certains spécialistes avancent même qu'elle ne remplit qu'un rôle purement « symbolique » pour les apprentis terroristes. Toujours est-il qu'Al-Qaïda (ou des mouvements menant la lutte en son nom) est présente dans plus de 60 pays, et que son pouvoir de nuisance est indiscutable.

- A la « criminalité transnationale », l'autre menace majeure. Comme le terrorisme islamique, elle a su tirer parti de toutes les possibilités offertes par la mondialisation, notamment celles venues de la révolution des technologies de l'information et de la démocratisation des transports. En effet, grâce aux circuits économiques globalisés, elle a pu développer ses affaires qui concernent au niveau international, le trafic d'armes, de drogue, parfois même humain et qui représentent près de 6% de l'économie mondiale. Ces organisations criminelles sont un facteur d'instabilité très fort surtout dans les régions où l'Etat s'est construit sur des bases fragiles. En effet, leur objectif premier ne réside pas dans la conquête du pouvoir à des fins politiques. Mais indirectement le contrôle de territoires leur octroie la main mise sur les

institutions, ainsi que sur les entreprises. Affaiblir l'Etat est donc pour elles un moyen d'asseoir leur « business » et d'optimiser les profits.

- Aux technologies proliférantes. Et au premier rang d'entre elles, la prolifération nucléaire, toujours présente dans ce monde post-Guerre Froide bien qu'ayant changé de nature. En effet, elle reste l'une des préoccupations majeures de la communauté internationale. Les dossiers Iraniens et Coréens, autrefois Libyens ou Sud Africains sont là pour en témoigner. Mais aujourd'hui, le risque le plus redouté n'est plus un affrontement nucléaire de grande ampleur pouvant mettre en péril la survie d'une partie de l'humanité mais une action terroriste perpétrée par le biais d'une arme atomique. A la chute du Mur, du matériel et de la matière fissile ont disparu des installations d'anciens pays soviétiques, et un certain nombre de savants ont mis leur expérience au service d'Etats proliférants. Ces fuites et cette situation pourraient elles être utilisées par un groupe terroriste ? C'est probable. Si actuellement la fabrication d'une arme atomique demeure au stade de la science fiction puisque le processus demande des moyens et un savoir faire que seuls les Etats (et encore les plus riches) sont en mesure de mobiliser, son vol constitue une hypothèse et un danger très réalistes. Et un attentat perpétré par le biais d'une « bombe sale » contenant de la matière fissile est également de l'ordre du possible. Mais les autres types de technologies proliférantes telles que les armes biologiques, bactériologiques et chimiques représentent tout autant (si ce n'est davantage) des méthodes susceptibles d'être employées lors d'un attentat.

- Aux « nouvelles rivalités économiques ». La fin du monde bipolaire et l'arrivée de la mondialisation ont transféré la compétition entre les nations, du domaine « militaire » au domaine « économique ». De nos jours, plus que la puissance de son armée, c'est le rayonnement économique d'un pays qui détermine sa place sur le plan international. Pour intégrer ce profond changement, les services de renseignement occidentaux ont d'ailleurs réorienté leur activité à compter de la décennie 90, comme nous le préciserons ultérieurement.

- A la compétition pour l'accès aux ressources et énergies stratégiques. Elle concerne particulièrement le pétrole (mais aussi le gaz) qui peut être à l'origine de tensions voire dans certains cas de conflits ouverts entre Etats non seulement pour assurer son exploitation mais aussi son transit. Ce le sera surement davantage encore dans le futur, à mesure que les ressources vont s'amoindrir et vont faire de cette matière première un produit encore plus convoité qu'il ne l'est aujourd'hui. De nombreux conflits interétatiques dans le monde concernent ces questions. Il peut être aussi un vecteur indirect de la montée des tensions. La Chine a ainsi augmenté significativement son budget militaire depuis quelques années, afin d'assurer la sécurité de ses approvisionnements énergétiques. Car globalement la concurrence entre les pays pour accéder à ces matières premières implique de renforcer la sécurité et donc de développer leur secteur militaire, ce qui a pour résultat d'instaurer de la crainte entre les Etats et d'attiser des tensions.

- Au retour de la Russie au premier plan. Après une période très difficile au début des années 90, elle remonte la pente dans tous les domaines depuis quelques années. Cependant après une phase de normalisation, marquée par une pacification politique avec de nombreux pays, on assiste depuis peu au retour de tensions. C'est le cas par exemple avec la Chine en raison de l'influence grandissante de cette dernière en Sibérie. C'est le cas également avec les américains à propos du projet de bouclier anti-missile que ces derniers voudraient installer sur le sol d'anciennes républiques soviétiques ou encore du dossier du nucléaire iranien, dans lequel le rôle du Kremlin est mal perçu par les américains et les européens.

- A la montée en puissance de la Chine. Elle pourrait engendrer des tensions importantes notamment avec les Etats-Unis qui tentent actuellement de s'implanter sérieusement en Asie alors même que la Chine entend s'approprier des espaces, notamment maritimes, qu'elle considère lui appartenir. Taïwan est toujours un sujet d'opposition majeur entre les deux pays, et Washington voit d'un très mauvais œil le rapprochement des chinois avec des pays « ennemis » tels que l'Iran, le Pakistan, la Corée du Nord ou la Birmanie.
  A ce titre, et avec toutes les précautions qui s'imposent, de plus en plus de spécialistes des questions stratégiques émettent l'hypothèse que les américains instrumentaliseraient la lutte anti-terroriste pour faire voter des budgets de défense et de sécurité toujours plus conséquents, dans l'hypothèse d'un conflit armé futur contre la Chine.

  En outre, les relations Chine/Russie après avoir connu une amélioration sensible à la fin des années 90, sont de nouveau tendues, pour des causes tenant essentiellement aux questions énergétiques et démographiques.

- Aux possibles déstabilisations liées aux éléments environnementaux et climatiques. Nous en sommes certains aujourd'hui, le climat à la surface du globe est en train de changer, et il le fera davantage encore dans les années à venir. Les épisodes climatiques violents d'origines naturelles mais aussi les catastrophes environnementales engendrées par l'activité devraient se multiplier. Nous en mesurons déjà les conséquences : sols et cours d'eau pollués, assèchement des ressources en eau, désertification, disparition d'espèces animales et végétales, etc.

  Les populations seront alors contraintes d'aller chercher ailleurs ce qu'elles ne trouveront plus sur leur propre territoire. Des migrations importantes, internes ou externes aux Etats, devraient se produire et on peut craindre ainsi qu'elles soient une source de déstabilisation importante et ce d'autant plus que dans beaucoup de régions du monde, ces facteurs climatiques et environnementaux vont se connecter à d'autres problèmes tels que l'explosion démographique.

Enfin, nous ajouterons ce que l'on pourrait nommer les « nouveaux extrémistes violents »[10]. Œuvrant le plus souvent dans les pays développés, ils remettent en cause le fonctionnement des sociétés capitalistes. Il s'agit des antimondialisations, des antis-consommations, des groupes de défense de l'environnement, de défense des animaux qui parfois ont débouché sur la naissance de groupes aux méthodes radicales et éventuellement très violents. C'est le cas d'*ALF* (*Animal Liberation Front*) par exemple concernant la défense des animaux, ou *ELF* (*Earth Liberation Front*) au nom de la protection de la nature. Cependant, nous ne les incorporons pas aux éléments majeurs de déstabilisation précédemment cités car leur dangerosité est certes réelle mais limitée.

La période post-Guerre Froide marque donc le développement de nouvelles menaces mises en œuvre par de nouveaux acteurs. Le monde est caractérisé aujourd'hui par « l'incertitude » liée à ce nouveau contexte. Les crises peuvent surgir n'importe où, n'importe quand, et pour des raisons très diverses.

Mais concrètement, pourquoi ces nouveaux acteurs sont-ils nés et comment ont-ils acquis leur pourvoir de nuisance ? Intéressons nous rapidement aux principaux éléments explicatifs :

b) …développées dans un contexte « globalisé ».

La mondialisation (ou globalisation) existe en réalité depuis que l'homme a décidé de découvrir d'autres territoires, d'élargir son horizon et l'apparition de nouveaux moyens de transports en a toujours été le moteur. Mais ce qui lui a conféré son caractère exceptionnel à la fin du XXème siècle, c'est la concordance de l'arrivée de moyens de transports toujours plus rapides et bon marché (avion, train, voiture) avec la révolution des nouvelles technologies de l'information et des communications (téléphones portables, Internet, etc.). Ainsi « *au-delà du physique, il y a un horizon intellectuel (information, connaissance, compréhension) que la communication a franchi à la fin du XXème siècle pour tisser une toile à travers le monde. Aujourd'hui chacun est conscient de ce qui se passe à l'autre bout de la planète, voire y participe : le monde est un village, c'est-à-dire un espace de proximité où l'on est plus étranger mais proche, davantage concerné* »[11].

- **Explosion des échanges économiques grâce à la révolution des transports.**

  L'amélioration des systèmes de communications a permis que les systèmes d'échanges commerciaux puissent intégrer les endroits les plus reculés du globe mais pour autant, elle n'a pas supprimé les différences géographiques. Au contraire, les zones qui ne font pas partie des réseaux d'échanges se trouvent plus marginalisées qu'avant. Le processus n'est en effet pas homogène et se concentre sur quelques « pôles », en excluant des régions entières. Ainsi Amérique du Nord, Europe et Asie principalement

[10] Eric Denécé, *La révolution du renseignement*, Revue Stratégie Globale n° 4 - Eté 2008, 13p.
[11] Revue : *Sécurité et Stratégie*, N° 93, Mai 2006.

réalisent à eux trois près de 65% des flux du commerce mondial, mais l'Afrique seulement 2.0 % et Amérique Latine 3.5%[12].

Par ailleurs, la révolution des transports qui s'est opérée à partir du 19ème siècle a entraîné une augmentation des capacités de déplacements, mais aussi et surtout la hausse de la vitesse et la baisse des coûts. Dans le domaine du fret maritime, on est passé d'un coût de transport à 95 dollars la tonne en 1920, à 29 dollars en 1990[13].

Cette explosion de la mobilité a renforcé l'interdépendance des économies et intensifié la compétition entre les « espaces ». En effet, la concurrence économique ne se situe plus uniquement au niveau du bassin d'emplois, de la région ou même du pays, mais à l'échelle du monde entier pour bon nombre d'activités et de secteurs.
Ainsi, les appels d'offres pour des entreprises telles que Boeing s'adressent à des entreprises de toute la planète.

La encore, cette « démocratisation » des transports qui peut être envisagée comme un véritable progrès est cependant répartie de façon très inégale selon la catégorie sociale des individus, selon les entreprises, selon les territoires, etc.

- **Explosion des télécommunications.**

Elles ont permis au XXème siècle de communiquer de façon quasi instantanée sur la quasi-totalité du globe, pour un coût de plus en plus « dérisoire ». Si en 1950 le prix de trois minutes de communication par téléphone s'élevait à 53 dollars, il n'était plus que de 3 dollars en 1990[14]. En 2003, le volume total des communications sonores dans le monde atteignait 180 milliards de minutes, soit plus de 340 années de temps en un an[15].
Internet à lui seul a représenté une véritable « révolution ». Alors que l'on comptait dans le monde environ 2 ordinateurs pour 1000 habitants connectés à Internet en 1990, on en compte 319 en 2005, et 478 à l'horizon 2010. En seulement cinq années (de 2000 à 2005) le nombre d'internautes dans le monde a enregistré une croissance de plus de 180% et jusqu'à 480% dans certaines régions (au Moyen Orient en particulier)[16].
Mais là encore, cette « démocratisation » de l'accès à Internet s'est réalisée de façon très inégale. On peut citer 2 exemples :

[12] Laurent Carroué, *Géographie de la mondialisation (3ème édition)*, Armand Colin, 2007, 295p.

[13] *Ibid.*
[14] *Ibid.*
[15] *La lutte contre le terrorisme islamiste*, Le Monde Dossier et Documents, juillet 2007.
[16] Source : http://www.itrmanager.com/

- Les pays du G8 qui regroupent 15 % de la population mondiale représentent 50 % du nombre d'internautes alors que la cinquantaine de pays d'Afrique a moins d'internautes que la France.

- Il existe trente pays dans le Monde dont le taux de pénétration d'accès à Internet est inférieur à 1 %.

Aujourd'hui, grâce aux télécommunications et Internet en particulier, il est possible et facile d'accéder à tout type d'information, depuis n'importe quel ordinateur. Et si dans la majorité des cas, il s'agit d'une avancée formidable, Internet peut également servir à la transmission et la diffusion d'informations dangereuses, de propagandes, d'appels à la violence, etc. Plus encore, il octroie une nouvelle capacité de « médiatisation » à des causes dont on n'aurait jamais entendu parler auparavant.

Pour les terroristes, la couverture et le retentissement médiatiques sont désormais plus importants que l'action elle-même. En effet, c'est l'information véhiculée et la peur ou l'angoisse qu'elle instaure au sein d'une population qui « terrorise » véritablement, un groupe, une société, etc.

Sans vecteur auprès de l'opinion publique, le terrorisme n'aurait aucun impact et cesserait d'exister, car par essence c'est la dimension psychologique qui alimente sa puissance et donc son pouvoir de nuisance.

Dans un monde où l'information et la communication jouent un rôle clé, le terrorisme a puisé une réelle force et trouvé de fidèles relais.

De même la « démocratisation » du transport a renforcé et souvent même créé une interconnexion entre les différentes régions du monde. Les personnes circulent, voyagent partout dans des délais très courts (quelques dizaines d'heures tout au plus pour rallier n'importe quel point du globe) et parmi elles, des candidats au Djihad. Eux aussi usent de cette nouvelle mobilité pour partir combattre en Irak ou s'entraîner en Afghanistan sans les difficultés d'acheminement et les contraintes de temps qui par le passé auraient probablement dissuadé la plupart d'entre eux de rejoindre ces théâtres d'opérations très éloignés…un phénomène qui n'est pas sans lien avec la révolution des technologies de l'information puisque nombre de ces individus ainsi embrigadés l'ont été en fréquentant des sites, Chat ou autres forums Internet islamistes radicaux.

La mise en place de ce nouveau contexte marqué par l'effacement des deux « ennemis historiques » et l'émergence d'acteurs et de menaces d'une nouvelle nature, va influer considérablement sur le domaine du renseignement dans les années 90.

2) Réorientation des services vers l'intelligence économique et le renseignement technique dans les années 90.

Au lendemain de la chute du Mur, les Etats-Unis sortent « vainqueur » de la Guerre Froide, mais se retrouvent dépourvus d'ennemi.

Pendant près de 50 ans, les moyens du renseignement qui avaient été mis en œuvre pour contrer l'adversaire soviétique deviennent « inutiles ». Mais avec l'apparition de ce nouvel « environnement », les Etats-Unis (et plus globalement l'ensemble des pays occidentaux) vont opérer des changements concernant le renseignement.

D'un point de vue général, ce dernier va connaître une double évolution :

- **Une extension du spectre traditionnel de son activité**. Avec l'imbrication croissante des enjeux politiques, économiques, militaires, etc., les services de renseignement vont devoir étendre considérablement leur domaine de compétence.
- **Un bouleversement des méthodes de travail**. La période post bipolaire caractérisée par de nouvelles menaces venues d'acteurs non étatiques oblige à reconsidérer le métier du renseignement. Et si les technologies de l'information et des communications apportent des supports et ouvrent des perspectives, elles n'en posent pas moins de nombreux problèmes aux agences.

Concrètement les Etats-Unis vont se lancer dans une spécialisation vers le renseignement technique, c'est-à-dire augmenter et ajuster les capacités déjà exploitées en la matière pendant la Guerre Froide.

Mais surtout, la collecte autrefois centrée sur des informations à visée « militaire » et « stratégique » va peu à peu acquérir une finalité « économique » dès lors qu'après la disparition des blocs, l'économie devient le champ majeur d'affrontement entre les nations.

Les services de renseignement occidentaux - et en premier lieu américains - s'orientent ainsi dans le renseignement économique (intelligence économique) collecté à l'aide de moyens techniques. Les thèmes du terrorisme, de même que les problématiques liées au Moyen-Orient ne comptent pas encore parmi les préoccupations prioritaires des autorités des Etats-Unis.

Pendant toute la Guerre Froide le « *monde Musulman n'était regardé que par le prisme déformant de le guerre froide et de la maitrise du pétrole* »[17] et les pays du monde occidental n'ont pas réussi à anticiper la menace islamiste alors naissante.

[17] Bruno Delamotte, *Le renseignement face au terrorisme*, Editions Michalon, 2004, 133p.

Quoiqu'il en soit, l'essentiel des moyens américains de renseignement a donc été réorienté vers l'économie, dans le but de soutenir la croissance alors déclinante. L'intelligence économique n'est pas apparue à cette époque et ne représentait donc pas une activité inédite pour les services de renseignement américains. En revanche, la véritable nouveauté, c'est qu'une grande partie des moyens du renseignement issus de la guerre froide (et donc basés sur la collecte d'informations militaires principalement) fut réorientée vers les activités économiques.

C'est ainsi par exemple, que le réseau d'interception: « *Echelon* » qui servait à l'écoute des communications de l'autre côté du Mur, fut utilisé après la guerre pour l'intelligence économique.

Cette réorientation s'est faite notamment sous l'impulsion notamment du directeur de la CIA de l'époque : Robert Gates, qui note en 1992 l'importance du renseignement de nature économique. James Woolsey son successeur se place dans la même logique et présente l'intelligence économique comme « *le sujet le plus brûlant de la politique du renseignement* ». Mais c'est surtout sous l'administration Clinton que l'exécutif américain décide véritablement de développer la coopération et d'entreprendre un rapprochement entre le secteur public et les entreprises américaines, dans le but de faire gagner à ces dernières des parts de marché à l'étranger. A partir de 1993, plusieurs organes de coordination sont créés pour orienter l'effort des services de renseignement dans le sens de la collecte d'informations de nature économique.

Au début des années 90, le renseignement électronique est donc à son apogée du côté américain. L'économie dépasse toutes les autres considérations, notamment sécuritaires.

C'est ainsi qu'à la fin de la décennie on estime que 40% du budget total de la CIA était consacré à l'intelligence économique.

Les moyens alloués au renseignement dans le cadre de la lutte anti-terroriste étaient donc très insuffisants. Les effectifs des agents spécialisés dans ce domaine avaient été divisés par 20 au Etats-Unis dans les années 90. Mais surtout la spécialisation dans un renseignement d'origine technique (et plus particulièrement électronique) s'avère assez inefficace contre un terrorisme qui est alors en pleine mutation ; qui commence à s'organiser en réseau et devient transnational.

Si le renseignement technique est très performant lorsqu'il s'agit de surveiller les mouvements d'armées adverses, d'évaluer leur arsenal, etc., en revanche contre les terroristes, son apport est beaucoup plus limité. Certes il est sûr, discret, et fournit des preuves concrètes et relativement fiables, mais il peut difficilement déjouer la pratique terroriste notamment depuis que cette dernière a changé de nature comme en témoigne d'une manière à la fois symbolique et tangible, Al-Qaïda[18] :

[18] Typologie inspiré de : *Reconstruire la sécurité après le 11 septembre* article intitulé *La communauté espagnole du renseignement face au terrorisme islamiste – de nouvelles menaces (par Javier Jordan)*, Les cahiers de la sécurité intérieure, INHES, 2004, 303p.

- Le fonctionnement s'opère via des réseaux quasi hermétiques qui ont très peu de relations avec l'extérieur.

- La multiplication des attentats suicides empêche que l'on puisse retrouver et interroger leurs auteurs.

- La décentralisation du commandement fait qu'un coup porté à l'une des cellules, même s'il est très important, n'entraîne pas l'effondrement de l'organisation car les informations récoltées sont d'une portée trop restreinte pour mettre en péril le reste du système.

- L'articulation en réseau favorise l'évolution très rapide de la structure. Les qualités principales de ces groupes terroristes sont l'adaptabilité, l'agilité, la flexibilité.

- Les communications en interne sont faibles et sont noyées dans le flot quasi infini des communications mondiales. Mais de toute façon les terroristes reviennent de plus en plus à l'utilisation de méthodes de communication « simples » tels que talkie-walkie, et de plus en plus les moyens radioélectriques (comme les stations de type UHF : *Ultra High Frequency*) délaissés par les services de renseignement.

Au-delà des évolutions « générales » évoquées plus haut, le développement du terrorisme islamiste va mettre le renseignement devant un certain nombre de faits nouveaux[19] :

- **La recherche de faits microscopiques**. Pendant la guerre froide, les objectifs étaient de grande taille (information sur les armées, les armements, sur les infrastructures, etc.) et relativement prévisibles. Mais avec le terrorisme islamiste, les services doivent identifier des centres de décisions multiples et extrêmement nébuleux. La recherche de l'information devient microscopique car on ne sait pas bien qui est l'adversaire ni quelles sont ses intentions.

- **Les limites de la collecte « technique »**. Malgré la progression des moyens d'interception (notamment les drones) identifier, intercepter, déchiffrer et traduire rapidement les communications des terroristes est une entreprise extrêmement complexe de par le manque de capacités analytiques touchant la plupart des services ou leur insuffisance face au volume des communications mondiales.

- **Les limites de la collecte « humaine »**. Nous l'avons déjà mentionné, l'infiltration de ces réseaux terroristes est quasiment impossible parce que ces groupes fonctionnent de manière excessivement resserrée. Et même lorsque l'infiltration réussit, il est très compliqué de maintenir le contact avec les agents. Mais de toute façon très peu sont prêts à prendre de tels risques. La collecte « humaine » ne représente donc pas un

[19] Typologie inspirée d'Eric Denécé, *La révolution du renseignement*, CF2R, 13p.

moyen « miracle » par rapport aux moyens « techniques » comme on a eu tendance à le dire après le 11 septembre.

- **Interdépendance croissante entre les services**. Le fonctionnement de ces groupes terroristes en réseaux qui dépassent les frontières des Etats impose une coopération transnationale des services de renseignement. En effet, la distinction entre la sécurité intérieure et extérieure n'est plus d'actualité. Les investigations contre les réseaux terroristes sont forcément transfrontalières.

Mais comment le monde du renseignement (en particulier aux Etats-Unis) s'est-il adapté à ces faits nouveaux ?

Nous venons de fournir une partie de la réponse en voyant que la tendance générale – surtout au Etats-Unis – fut à une spécialisation dans le renseignement technique, ciblée sur les activités économiques qui délaissait la problématique du terrorisme islamiste alors naissante, et qui n'a pas permis de s'adapter correctement à la nouvelle donne stratégique post-guerre froide.

La seconde partie de la réponse va être apportée par les évènements du 11 septembre et les leçons tirées de l'échec à prévoir et empêcher l'opération.

3) L'incapacité de la « communauté » mondiale du renseignement, à prévoir les attentats du 11 septembre 2001.

Le 11 septembre 2001, une opération terroriste s'emparait simultanément de quatre avions de lignes américaines dans le but de les projeter, tels des missiles, sur des cibles bien précises, à New York et Washington. Nous connaissons tous la suite.

Le bilan tant humain que matériel (plus de 3000 morts, des centaines de blessés et plusieurs milliards de dollars de dégâts), le symbolisme des lieux ainsi que le mode opératoire, mais surtout la couverture médiatique « jamais vue » donnèrent à cette évènement un retentissement, une ampleur, un caractère encore inédits.

Mais surtout, il marqua la faillite des services de renseignements américains en premier lieu, mais au-delà, celle de l'ensemble des services mondiaux.

Comment une attaque d'une telle envergure a-t-elle pu se produire sur le sol de la première puissance mondiale ? Un certain nombre de défaillances, d'approximations, d'erreurs ont été commises en amont et sont révélatrices des lacunes du renseignement à cette période :

- Concernant l'« avant » opération, le parcours d'un individu nommé Zacarias Moussaoui est tout à fait parlant. Jacques Baud analyse cet exemple :

  Le 11 août 2001, Moussaoui se présente à l'école de la « Pan Am » à Eagon dans le Minnesota, pour prendre des cours de pilotage sur simulateurs de Boeing 737. Ses connaissances ne correspondant pas au profil habituel des élèves, un employé contacte le FBI qui ouvre une enquête. Dans le même temps, les services français de renseignement informent ce dernier que Moussaoui est affilié à des mouvements fondamentalistes. Il est placé en garde-à-vue au motif de l'expiration de son visa de résidence et très rapidement suspecté d'avoir l'intention de commettre un acte terroriste, éventuellement en prenant le contrôle d'un avion. Le « *Counter Terrorist* » du FBI est alors alerté. Le 4 septembre, la « *Radical Fondamentalist Unit (RFU)* » diffuse un message à l'ensemble de la communauté de renseignement contenant les interrogatoires du suspect. Mais aucun élément analytique sur l'objet et la nature même des plans de Moussaoui et sur l'importance de la menace qu'il représente n'est transmis. À aucun moment, les informations sur Moussaoui ne sont recoupées avec les indices par ailleurs collectés par la NSA. De même aucun rapprochement n'est fait avec une note d'un agent du FBI concernant la formation au pilotage d'extrémistes. Au final, Zacarias Moussaoui ne prit donc pas part à l'opération, mais pour autant, celle-ci eut lieu.

- Une multitude d'autres faits sont également à signaler[20] :

  - Dès le mois de Juin 98, les services de renseignement américains ont connaissance que Ben Laden projette de fomenter des attentats contre New York et Washington.

  - Août 98, les services de renseignement sont avertis qu'un groupe d'Arabes s'apprête à percuter le WTC avec un avion chargé d'explosifs venant d'un pays étranger. Le FBI et la FAA (*Federal Aviation Administration*) estiment et déclarent que compte tenu du secteur aéronautique du pays, c'est très peu probable, et que de toute façon un avion venant de l'étranger serait repéré avant d'atteindre sa cible. Le dossier est classé, mais depuis, les liens entre ce groupe et Al-Qaïda ont été clairement établis.

  - Septembre 98, les services américains sont alertés que le prochain attentat de Ben Laden pourrait consister à faire atterrir un avion bourré d'explosifs sur un grand aéroport national.

  - Février 2001, Hani Hanjour (un des participants à l'opération) prend des cours de pilotage en Floride. Son comportement suscite une enquête du FBI qui ne trouvera cependant rien d'anormal.

[20] Eléments tirés de : Michel Nesterenko, *Une guerre nouvelle a commencé. Internet : un nouveau champ de bataille. Le terrorisme à l'épreuve de l'informatique*, 2002, 151p.

- Juin 2001, Ben Laden donne une interview à une chaine de télé et annonce que les Etats-Unis doivent s'attendre à une attaque dans les semaines à venir.

- Le 2 juillet, le FBI prévient toutes les forces de police de se préparer à une attaque d'Al-Qaïda, surtout à l'étranger.

- Vers le 5 juillet, Ben Brock l'adjoint au directeur du centre de contre-terrorisme de la CIA donne des preuves inquiétantes de la probabilité d'une attaque spectaculaire. Toutefois la date exacte n'a pas été précisée.

- Le 10 juillet, un agent du FBI (Kenneth Williams) envoie un mémo (celui que nous venons d'évoquer à propos du cas Moussaoui) au centre à Washington et au centre anti-terroriste de New-York, sur certains élèves pilotes islamistes et radicaux, et suggère qu'Al-Qaïda essaie d'infiltrer le transport aérien…mais personne ne donne suite et ces éléments ne parviendront jamais aux décisionnaires.

- Vers la mi juillet, George Tenet le directeur de la CIA conduit un briefing pour Condoleza Rice et ses collaborateurs. Il leur prédit une attaque de grande envergure.

- Le 6 aout, George Tenet soumet une analyse approfondie au Président envisageant le cas de piraterie aérienne. Ce même jour Mohamed Atta (l'un des terroristes) loue la première de ses 3 voitures et fait près de 5000 km dans le mois qui suit. Il s'enregistre au club de plusieurs compagnies aériennes pour bénéficier des avantages réservés aux clients réguliers.

- Le 10 septembre, la NSA intercepte les conversations téléphoniques d'individus sous surveillance. La NSA et le FBI prétendent que les conversations n'ont été traduites que deux jours plus tard par manque de traducteurs comprenant l'arabe.

- D'autres anomalies furent démontrées par les enquêtes portant sur le déroulement de l'opération. Plusieurs terroristes réussirent à embarquer sans même être passés par les portiques de sécurité, suite à la négligence du personnel au sol et aucun d'entre eux ne fut détecté lors des contrôles d'identité. Pour revenir au cas Zacarias Moussaoui et à ses conclusions, nul doute que la transmission des informations faisant état de possibles détournements d'avions, aurait mis les aéroports en alerte.

Comment donc à la lumière de ces éléments, les services de renseignement américains n'ont-ils pu en prévoir avec plus de précision les modalités ?

A l'évidence, leur multiplication, ainsi que l'absence de structure efficace de fusion y sont pour beaucoup. Le 11 septembre a en fait révélé, hélas de façon très tragique, toute la

difficulté des services de renseignement et de sécurité américains à parvenir alors à une image commune de la menace, essentiellement par manque de coopération et de communication. Un meilleur partage des données aurait sans doute (mais pas avec certitude) permis une hausse de la vigilance, et donc une diminution du risque.

Selon Tom Ridge, premier directeur du *Department of Homeland Security* : « *C'est le manque de communication entre les agences de renseignement américaines avant le 11 septembre qui explique en partie que la menace n'ait pas été perçue à sa juste valeur et que l'opération n'a pu être contrecarrée* »[21].

C'est également significatif de la grande difficulté d'une grande bureaucratie de s'adapter à une évolution rapide de son environnement.

Les grands services de renseignement occidentaux ne se sont pas correctement adaptés – à la fois qualitativement et quantitativement – au nouveau contexte stratégique émergeant à partir de la chute du Mur.

Avec le 11 septembre, est apparue la notion de « *Home Grown Terrorist* », pour désigner des terroristes implantés dans le pays qu'ils prennent pour cible. En effet, la totalité des terroristes ayant pris part aux attentats étaient des citoyens intégrés, éduqués (souvent riches) vivant dans des pays occidentaux. De plus, certains d'entre eux avaient même séjourné aux Etats-Unis au cours des semaines précédentes. La menace peut donc désormais venir de l'« intérieur ». Cette réalité que l'on a découvert brutalement avec le 11 septembre, est particulièrement évocatrice du « temps de retard » des services de renseignement, par rapport à l'évolution du terrorisme depuis les années 90.

Face à cette faillite, l'explication la plus fréquemment avancée fut celle d'un délaissement américain du renseignement « humain » au profit du renseignement « technologique ».

Mais c'est plus vraisemblablement la trop forte prépondérance du renseignement tactique sur le renseignement stratégique qui constitue le facteur déterminant.

Selon Jacques Baud : « *Aux Etats-Unis avant le 11 septembre, trop de services de renseignement avaient une compétence tactique, très spécialisée. Il y avait très peu d'analystes stratégiques qui eux ont une vue d'ensemble du phénomène terroriste et qui peuvent percevoir des choses que les analystes tactiques ne peuvent pas voir. Par exemple, au* FBI *avant le 11 septembre, il y avait dix analystes tactiques pour un analyste stratégique. Et ce déficit analytique a considérablement limité les capacités du monde politique à comprendre la nature et l'intensité du problème et donc de prendre des décisions (…) la leçon du 11 septembre c'est que l'anticipation de l'action tactique est souvent impossible, ce qui donne à l'anticipation stratégique un rôle déterminant* »[22].

[21] Propos tenus le 28/3/2007 lors d'une conférence organisée par le magazine *Foreign Policy*, à l'Hôtel Georges V, Paris.

[22] Jacques Baud, *Le renseignement et la lutte contre le terrorisme*, Lavauzelle, 2005, 404p.

Pour autant, les agences de renseignement américaines sont-elles les seules concernées par ce constat ?

Non, car le 11 septembre signe la faillite de tout un système. En effet, même si des services européens (notamment français) avaient averti leurs homologues américains de la présence sur leur territoire d'individus potentiellement dangereux, les informations restaient très évasives et donc insuffisantes pour avoir une idée précise et concrète du danger. De plus, une grande partie de la préparation de l'opération s'est déroulée en Europe. Les services de renseignement et de sécurité des pays en question ont donc également une grande part de responsabilité.

Conclusion Chapitre 1 :

Le renseignement, pilier de la lutte contre le terrorisme, a donc fait face à des changements majeurs dès la fin de la guerre froide, à partir du début des années 90.
Les services de renseignement mondiaux - notamment ceux issus de pays occidentaux - organisés, structurés pour l'affrontement bipolaire ont connu de nombreux bouleversements.

Le développement des nouvelles menaces venues d'acteurs non étatiques imprévisibles et fonctionnant en réseau(x), a débouché sur la mise en place très rapide d'un nouvel environnement stratégique global dans lequel le terrorisme islamiste transnational s'est imposé progressivement comme la menace majeure dans ce monde post-bipolaire.

Pourtant le 11 septembre 2001 - et plus globalement la multiplication des attentats d'origine islamiste dans le monde - a mis en exergue l'inadaptation des services de renseignement contre ce terrorisme d'un nouveau genre. Les agences de renseignement, notamment aux Etats-Unis n'ont pas réussi à clairement appréhender l'opération en préparation, non pas à cause d'un manque d'information, mais d'une mauvaise interprétation et surtout par un défaut de coordination entre elles.

Contrairement aux acteurs non étatiques qui se sont développés grâce aux possibilités offertes par la mondialisation dans son acception la plus globale (développement des transports, des technologies de communication, d'information, fonctionnement en réseau, etc.), les agences de renseignement ont eu tendance à demeurer dans le fonctionnement et une approche bureaucratique et enclavée issus de la Guerre Froide. De plus, si la réorientation opérée dans les années 90 vers le renseignement technique à visée économique a permis aux Etats-Unis de soutenir efficacement leur croissance pendant cette période, le délaissement du terrorisme par les services de renseignement explique en partie leur inadaptation à cette menace.

Mais comment les services de renseignement ont-ils évolué après le 11 septembre ?

Introduction Chapitre 2 :

Dès le 13 septembre 2001, Ben Laden et Al-Qaïda sont désignés comme les responsables de l'opération. Cette dernière est vécue par les Américains, du simple citoyen au plus haut représentant de l'État, non pas comme une « simple attaque » mais comme un véritable « acte de guerre ». En réplique à cet évènement inédit, l'administration Bush va introduire le concept géopolitique de « guerre contre le terrorisme » ou « guerre contre la terreur » (« *war on terror* » ou « *global war on terror* ») à partir de l'énoncé suivant : si par l'intermédiaire d'Al-Qaïda la menace terroriste est devenue globale, la lutte, la riposte doivent l'être également.

La réaction des Etats-Unis au 11 septembre va s'organiser tout d'abord autour d'une riposte « internationale » avec les campagnes d'Afghanistan et d'Irak et plus généralement avec l'ensemble des opérations militaires visant à traquer au plan international les organisations et réseaux terroristes islamistes.

Mais dans le cadre de ce travail, nous nous intéresserons aux évolutions observées en matière de renseignement. Les réformes des agences (FBI, NSA, CIA), ainsi que la mise en place de législations à la fois sécuritaires mais œuvrant pour et à partir du renseignement (*Homeland Security*, *Patriot Act*, etc.) font partie des thèmes que nous étudierons dans cette seconde partie.

Notre but sera ici de mesurer la teneur et l'ampleur de la refonte de la communauté américaine du renseignement après le 11 septembre 2001.

Puis nous nous placerons au niveau de l'Alliance Atlantique, des Nations Unies et de l'Union Européenne qui certes ne sont pas des organisations prioritairement tournées vers le renseignement, mais qui sont (et seront) absolument incontournables dans la lutte internationale menée contre le terrorisme, au même titre que les Etats-Unis.

Enfin nous examinerons le cas du renseignement français, qui avec son système assez spécifique et en pleine mutation, a valeur de référence.

Chapitre 2 : L'évolution du renseignement à l'ère post-11 septembre 2001.

I) Refonte de la communauté américaine du renseignement.

Contrairement aux propos souvent avancés - et comme nous l'avons vu précédemment - les services de renseignement des Etats-Unis n'ignoraient pas (et n'écartaient pas) la possibilité d'une opération terroriste importante sur leur propre sol. Sans être considéré comme majeur ou vital pour les intérêts de la nation, le risque d'attentats était donc connu et préoccupait les dirigeants américains bien avant le 11 septembre 2001 et particulièrement dans les mois précédents. Mais il n'a pas été clairement et pleinement évalué par la communauté du renseignement américain et l'attaque s'est produite avec succès.

Quelles initiatives ont été engagées dans le domaine du renseignement, pour empêcher que cela se reproduise ?

1) Initiatives « sécuritaires ».

Elles concernent les décisions prises pour rehausser le niveau de sécurité aux Etats-Unis, en se protégeant contre une nouvelle attaque de terroristes.

Il ne s'agit donc pas d'initiatives centrées spécifiquement sur le renseignement, cependant ce dernier y prend souvent une place déterminante.

a) Création du « *Department of Homeland Security* ».

Le « *Department of Homeland Security* » (DHS) est la clé de voûte de la redéfinition de la politique américaine de contre-terroriste et de protection du territoire national. Issu de deux lois votées les 13 et 19 septembre 2002 son fonctionnement effectif date du 1er janvier 2003. Ce département a pour mission essentielle « *d'identifier les priorités et coordonner les efforts de collecte et d'analyse de l'information, touchant les menaces intérieures et extérieures* »[23].

Selon Tom Ridge, son premier directeur : « *L'objectif numéro 1 lors du lancement du Department of Homeland Security était de faire remonter l'information au sommet de la hiérarchie, de mettre en commun le renseignement des différentes agences américaines. Car*

[23] *Ibid.* Jacques Baud Op.cit. p27.

c'est leur manque de communication avant le 11 septembre qui explique en partie que la menace n'ait pas été perçue à sa juste valeur et que l'opération n'a pu être contrecarrée »[24].

Mais il ne s'agit pas d'une agence de renseignement à proprement parler. Le DHS est une entité de coordination dans le domaine de la « sécurité nationale » au sens le plus global du terme, mais en aucun cas il n'a vocation à faire de la collecte de renseignement, il n'existe que pour faciliter les relations entre les agences compétentes (qu'elles soient purement « sécuritaires » ou bien réellement des agences de renseignement). Officiellement c'est un service de sécurité civile.

Il est composé de 22 agences, emploie près de 180 000 collaborateurs et dispose d'un budget colossal.

La création de cette nouvelle entité seulement quelques semaines après le 11 septembre répondait alors à la priorité absolue pour les dirigeants politiques américains d'éviter que de tels actes puissent se reproduire. Fondées ou non, les nombreuses alertes et rumeurs faisant état de la probabilité élevée d'un autre attentat se multipliaient. Et dans un tel climat, il devenait indispensable d'améliorer rapidement les capacités de défense ou de protection de la nation (ou au minimum d'en donner l'impression).

Dans le même temps les enquêtes sur le déroulement de l'opération progressaient, introduisant la notion de « *Home Grown Terrorist* » particulièrement frappante et inquiétante. En outre, elles mirent rapidement en lumière de graves dysfonctionnements dans les services de renseignement et de sécurité avant l'opération, qui allaient motiver puis servir de base à la création du « *Department Of Homeland Security* » et justifier que lui soient alloués quarante milliards de dollars dès sa première année, en 2002.

Quatre axes sont jugés prioritaires :

- Prévention du bio terrorisme.
- Développement des secours d'urgence.
- Accroissement de la sécurité dans les aéroports et contrôles aux frontières.
- Amélioration des capacités de renseignement.

Ainsi le 11 septembre a donné naissance à une « *Nouvelle approche de la sécurité aux Etats-Unis, qui remet profondément en cause le schéma théorique et institutionnel hérité du*

[24] *Ibid.* Conférence du 28/3/2007 Op.cit.p28.

National Security Act de 1947 »[25] qui, s'il s'avérait adapté au contexte de la Guerre Froide, semblait en revanche peu pertinent depuis la chute du monde bipolaire.

Il est important de repréciser que le DHS est une entité qui entend œuvrer pour la sanctuarisation du territoire américain dans un aspect « global », dépassant largement le cadre spécifique du renseignement. Le budget alloué au renseignement n'était d'ailleurs que de 474 millions de dollars en 2005, pour un budget total du DHS de 47 milliards, soit environ 1%[26].

Mais dans les faits le « *Department of Homeland Security* » n'est que la face la plus visible de la refonte entreprise aux Etats-Unis, en réaction immédiate au 11 septembre.

En effet, le 8 octobre 2001 naît l'« Office de Sécurité Intérieure (*Office of Homeland Security*) » chargé d'élaborer et de coordonner une stratégie pour protéger le pays des menaces et des attaques terroristes.

Le « Conseil de Sécurité Intérieur (*Homeland Security Council*) » joue, quant à lui un rôle d'information pour le président, sur toutes les questions liées à la sécurité du territoire en définissant une « Stratégie nationale pour la sécurité intérieure (*National Strategy for Homeland Security*) ». Il assure la partie « théorique » de la mission. Ses prérogatives ont trait à l'organisation, il apporte des solutions pour mettre en place une communication étroite et efficace entre les secteurs publics, privés, civils, militaires jusqu'alors peu rompus à travailler en partenariat.

C'est l'ensemble de ce système que l'on nomme le « *Homeland Defense* ».

Le DHS constitue son axe « opérationnel » et veille à l'application sur le terrain, des plans énoncés par le Conseil de Sécurité Intérieur.

Il est donc limité à coordonner les différents acteurs. Mais s'il ne possède pas en tant que telle, une capacité « physique » d'intervention, il va néanmoins grandement influer sur la redéfinition des politiques des agences de renseignement.

Financièrement c'est un « poids lourd » puisqu'il se place au deuxième rang national, derrière le département de la Défense.

---

[25] Sabine Lavorel, *La politique de sécurité nationale de l'Administration Bush – Un facteur de présidentialisation du régime politique américain*, Arès Vol XX – N°50, 2003, 17p.

[26] Données : *Intelligence On Line - Édition française N° 494 :* http://www.intelligenceonline.fr/detail/detail_articles/p_detail.asp?DOC_I_ID=14688682&Context=ARC&ContextInfos=LMR|494&CodeAffilie=A_INDIGO&service=GRA

b) Le « USA *Patriot Act* ».

Le « *USA Patriot Act* » pour « *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme) » est voté par le Congrès le 26 octobre 2001.

Cette loi dite « d'exception » et prévue initialement pour une période de quatre ans seulement, fut reconduite par le *Sénat* et la *Chambre des Représentants* en juillet 2005 : quatorze de ses seize dispositions sont alors instituées de manière permanente, les deux autres se voyant prolongées pour dix ans.

C'est le second chantier de l'après 11 septembre sur le plan intérieur.

Il fournit au pouvoir exécutif des prérogatives très largement renforcées pour lutter contre le terrorisme : « *L'administration dispose de nouveaux pouvoirs en matière de collecte du renseignement, de surveillance des communications, de contrôle de l'immigration et de lutte contre le blanchiment d'argent* »[27].

Au même titre que le *DHS*, le *Patriot Act* n'est pas dédié uniquement au renseignement, il concerne la « sécurité » de façon globale.

Cependant il amplifie considérablement les attributions des services secrets, de renseignement, de police et de sécurité en leur donnant une liberté d'action accrue dans leurs activités liées au terrorisme.

L'article 213 autorise par exemple le *FBI* à pénétrer dans un domicile ou un bureau en l'absence de l'occupant, à prendre des photos, à examiner les disques durs des ordinateurs et à y insérer un dispositif digital d'espionnage.

L'article 214 légalise l'accès à des données de connexions électroniques entrantes et sortantes, mais sans l'obligation d'obtenir un mandat judiciaire.

Les articles 209 et 218 permettent respectivement de saisir des messages vocaux et de mener des recherches secrètes dans un domicile ou un bureau sur la base d'une simple « présomption raisonnable ».

D'autres articles (215 et 206) facilitent l'obtention de données bancaires, médicales et même de celles relatives aux d'emprunts effectués auprès des bibliothèques.

En vertu du statut de « combattants ennemis ou illégaux » créé par le *Patriot Act*, le gouvernement peut détenir sans limite de temps et sans inculpation, toute personne qu'elle présume terroriste.

[27] *Ibid.* Sabine Lavorel Op.cit.p31.

c) Les autres initiatives « sécuritaires ».

L'une des tendances lourdes depuis les attentats du 11 septembre 2001, est l'évolution vers un renseignement d'« identification de masse » qui consiste à repérer et identifier des suspects à très grande échelle.

Pour ce faire, il opère à partir de moyens « biométriques » qui permettent d'« *extraire des informations du corps et des traces laissées par les individus* »[28] ou de technologies informatiques qui collectent des données pouvant êtres filtrées, traitées, analysées et redistribuées ensuite aux services judiciaires et de polices compétents.

Ce type de renseignement est quelque peu différent de celui dit « classique » pratiqué par les agences de renseignement.

Ce dernier peut certes utiliser les mêmes méthodes d'origines techniques, mais pour se concentrer véritablement sur des cibles plus ou moins précises (il y a tout de même un objectif ciblé dans la majorité des cas).

Le renseignement d'identification ou de repérage est lui davantage dans une logique « sécuritaire », qui repose sur une surveillance large des individus.

Voyons comment il s'est développé et de quelles manières il s'exerce :

- La sécurité dans les transports, notamment le transport aérien, s'est nettement intensifiée depuis 2001 avec la mise en place de la « *Transportation Security Administration* » juste après les attentats. D'abord intégrée au Ministère des transports, elle est à présent rattachée au Département de la Sécurité Intérieure, lui-même crée en 2003.
  Par son intermédiaire quelques 6000 cabines de pilotage d'avions commerciaux furent renforcées, des milliers d'agents de sécurité déployés sur des vols intérieurs et 50 000 contrôleurs de sécurité engagés dans les aéroports pour remplacer les sociétés sous traitantes des compagnies aériennes. Mais surtout les normes de sécurité concernant la détection d'engins explosifs, la sensibilité des appareils lors des embarquements, etc., furent rehaussées. Ces dispositions se sont traduites par une augmentation de 93% des dépenses de sécurité du transport aérien entre 2001 et 2005.

- Par ailleurs, la « biométrie », incorporée notamment dans les passeports depuis 2006 et tous les systèmes de contrôle de sécurité (essentiellement dans les aéroports) sont en voie de généralisation et sont une émanation directe du 11 septembre.

- Les Etats-Unis ont également entrepris la création d'une base de données enregistrant tous les voyageurs transitant par leur territoire.

[28] Didier Bigo, *Renseignement, Police et contrôle démocratique : la collaboration européenne et transatlantiques*, Mars 2007.

- La « cyber-surveillance » existait déjà, mais elle a été augmentée après les attentats, via la création d'un poste de Conseiller du Président sur toutes les questions de cyber sécurité, et le vote d'une législation anti-terroriste qui a élargi les compétences du FBI et de la NSA relatives aux écoutes téléphoniques et à l'interception des messages électroniques. Car il ne fait aucun doute qu'Internet est devenu un outil privilégié par les terroristes djihadistes, qui s'en servent pour recruter directement de nouveaux activistes, mais également dans un but de propagande.

  Si une douzaine de sites Internet appelaient au Jihad en 97, on considère qu'ils seraient plus de 4000 actuellement[29]. Aujourd'hui « *L'équipement d'un Moudjahidin c'est une kalachnikov mais aussi un ordinateur portable* »[30].

  De plus, Internet met à disposition en libre service, des données parfois très sensibles et susceptibles d'être exploitées par les terroristes. A titre d'exemple « *le site internet de la Federation of Americain Scientists (FAS) permettait de télécharger avant le 11 septembre des clichés ainsi qu'un descriptif sommaire d'immeubles « sensibles » liés au gouvernement et tellement discrets que leur existence n'était même pas reconnue par Washington. D'autres ont pris le relais, comme Cryptome qui propose les « Cryptome Eyeball Series ». Celles-ci réunissent de véritables dossiers mêlant imagerie haute résolution et cartographie voir plan 2D ou 3D de l'extérieur et/ou de l'intérieur de certains bâtiments pouvant constituer des cibles de choix. Au rang des derniers ajouts, la zone de sécurité de la maison de Bill Gates ou encore la Maison Blanche. De même, avant le 11 septembre il était possible d'acquérir online une cartographie détaillée des installations militaires de l'Oncle Sam par l'intermédiaire du site de la National Imagery and Mapping Agency (NIMA puis rebaptisée NGA)* »[31].

  Mais si les terroristes peuvent utiliser Internet pour préparer et perpétrer leurs actions, les services de renseignement peuvent faire de même pour repérer et arrêter ces derniers. En effet, en infiltrant des forums, chats et groupes de discussions virtuels, en exploitant les bases de données, en retrouvant les « traces informatiques » laissées par des activistes sur « la toile » ou en étudiant les contenus de disques durs saisis lors d'opérations, etc., les services de renseignement sont en mesure d'obtenir des informations précieuses. Et depuis 2001, leurs activités dans ce domaine se sont étendues. Au-delà des écoutes téléphoniques « classiques », la surveillance s'est généralisée aux nouveaux modes de communication numériques (email, mais aussi messagerie instantanée, SMS, etc.). Et un certain nombre de législations ont été adoptées pour supprimer le principe d'anonymat lors de connexions sur le réseau, pour la conservation des login, pour multiplier les possibilités de croisements des fichiers administratifs entre juridictions, etc.[32].

---

[29] Jean-Jacques Cecile, *Internet. Outil de renseignement pour terroristes ?*, Histoire mondiale des conflits n°16, octobre 2004, 66p.

[30] Hamid Mir, journaliste pakistanais.

[31] *Ibid.* Jean-Jacques Cecile Op.cit.p 36.

[32] Source : http://www.zdnet.fr/actualites/internet/0,39020774,2100268,00.htm

- Enfin nous citerons quelques autres décisions relatives à la sécurité « globale » du territoire, telles que les nouvelles mesures prises pour la protection des infrastructures sensibles (installations nucléaires, usines chimiques, sites de stockage de matières dangereuses, etc.) ou encore l'amélioration de la sécurité aux frontières et dans les ports (surtout les cargaisons) etc.

Comme nous pouvons le constater, il est parfois ici davantage question de « systèmes de sécurité » que de renseignement au sens strict ou usuel du terme.

De plus, même si la plupart de ces initiatives ont été soit introduites soit poursuivies après le 11 septembre 2001 pour lutter contre le terrorisme, il nous faut souligner qu'elles mettent en œuvre des moyens « généraux » et qu'elles s'adressent à l'ensemble des citoyens. Pour autant, elles peuvent être considérées indirectement comme des formes de renseignement dès lors que toutes les informations collectées par ce biais peuvent se révéler utiles aux services de renseignement pour la localisation d'individus déjà connus et potentiellement dangereux, et pour le repérage d'individus « suspects ».

Et au final, elles contribuent donc, elles aussi, à rehausser le niveau général de sécurité.

La création du « *Department of Homeland Security* », le vote du *Patriot Act* ont donc répondu, immédiatement après les attentats, au besoin de « sécurité », de sanctuarisation du territoire américain et bien qu'elles soient d'une portée générale, le renseignement prend une part non négligeable dans ces deux initiatives.

Passons maintenant à l'étude des véritables acteurs du renseignement américain, c'est-à-dire les agences (FBI, CIA, NSA) et leur évolution après le 11 septembre.

2) Refonte des trois grandes agences de renseignement (FBI, CIA, NSA)[33].

Aux deux grandes « nouveautés » que sont le « *Department of Homeland Security* » et le « *Patriot Act* » viennent s'ajouter des changements au sein même des entités déjà existantes.

D'un point de vue global, l'évolution du renseignement aux Etats-Unis après 2001 apparaît comme la conséquence directe du constat d'échec tiré du 11 septembre et des deux principales causes de nature à l'expliquer, à savoir :

- Une trop grande spécialisation des agences américaines dans le renseignement technique et les effets contre productifs qu'elle a provoqués :

  - Mettre sur écoute tous les téléphones de la planète ou filtrer l'ensemble des communications passant par le biais d'Internet s'avère être une entreprise inutile et impossible à réaliser vu la masse gigantesque et sans cesse croissante des communications.

  - Ainsi, ce n'est que le 12 septembre 2001 que la NSA a traduit deux bouts de phrases prononcés par l'un des terroristes du 11 septembre : « *Le match important est sur le point de démarrer* […] *demain sera l'heure zéro* ». Aurait-t-on pu empêcher les attentats si elle l'avait fait plus tôt, lorsqu'il était encore temps ? La réponse ne pourra jamais être connue, mais cet exemple est significatif des limites du renseignement technique et plus exactement des capacités de traitements.

  - Les terroristes ont fini par abandonner les téléphones, messageries et autres technologies pour revenir à des « *moyens radioélectriques traditionnels aujourd'hui délaissés par les grands services d'interception* »[34]. Ainsi aujourd'hui, avec des stations de communications de type HHF (*Ultra High Frequency*) qui sont bon marché et relativement simple d'utilisation, les terroristes peuvent communiquer partout dans le monde et de façon très discrète, sans se faire repérer par les services de renseignement.

- Des déficiences dans l'échange du renseignement, que ce soit avec les services étrangers, ou - et surtout - entre les agences américaines elles mêmes.

[33] Comme nous le verrons par la suite, contrairement à la CIA et NSA, le FBI n'est pas un service de renseignement à proprement parler, mais une agence de police dont la tache première est de lutter contre le crime. Cependant son intense activité dans le cadre de la lutte anti-terroriste et de la collecte du renseignement depuis 2001, nous permet de l'incorporer ici au sein des « agences de renseignement » américaines, même s'il ne s'agit donc pas de sa vocation première.

[34] *Nouvelles réalités du renseignement*, Les cahiers du CESA n°16, Décembre 2006, 34p.

Pour preuve de l'effort engagé après le 11 septembre, les dépenses de défense et de sécurité vont augmenter fortement et de façon constante et passer de 16.8 milliards de dollars en 2001 à 55 milliards en 2006.

S'agissant spécifiquement du renseignement, le refinancement débuté avant 2001 fut poursuivi et accru. Les budgets des différentes agences seront ainsi eux aussi largement dotés pour s'élever à 44 milliards de dollars en 2005, contre 27 en 1998, soit une hausse de 65 % en moins de 10 ans. A titre de comparaison, c'est presque autant que la somme allouée annuellement à la Défense française.

Le renseignement américain est assuré principalement par 16 agences, civiles ou militaires. Nous avons choisi de limiter notre étude aux 3 agences les plus importantes et les plus emblématiques (FBI, CIA, NSA) car elles sont bien représentatives de l'évolution observée aux Etats-Unis après le 11 septembre. Mais elles ne sauraient résumer à elles seules la communauté. D'autres agences, telles que la NRO (*National Reconnaissance Office*) ou la DIA (*Defense Intelligence Agency*) y participent activement, notamment dans le cadre de la lutte anti-terroriste.

a) Le *FBI* (*Federal Bureau of Investigation*).

Le FBI est à l'origine un service de police spécialisé dans les enquêtes criminelles. Mais depuis quelques années, il est devenu un véritable instrument œuvrant pour la sécurité nationale, dont les attributions et compétences recouvrent principalement les domaines de l'anti-terrorisme, du contre-espionnage et de la recherche de renseignement à l'intérieur du territoire.

Fondé en 1908 (mais il ne prendra son appellation de «*Federal Bureau of Investigation* » qu'en 1935), il est présent dans plus de 400 villes américaines mais aussi dans une cinquantaine d'ambassades à l'étranger ; il emploie plus de 28 000 personnes dont 12 000 pour l'anti-terrorisme. Son budget oscille à présent entre 7 et 9 milliards de dollars (il n'était que de 4.3 milliards en 2002).

La transformation du FBI fut l'une des grandes décisions prises au lendemain des attentats de 2001 et elle a consisté à recentrer sa mission traditionnelle de lutte contre la criminalité tout particulièrement sur l'anti-terrorisme. Si cette fonction comptait parmi ses priorités depuis le début des années 80, elle devint alors la première : des centaines d'analystes ont été engagés et déployés dans tout le pays et une division anti-terroriste composée de 500 agents (et encore 900 supplémentaires en 2002) a vu le jour avec comme directive principale, la prévention du terrorisme de par l'anticipation de la menace, elle-même dépendante de l'obtention du renseignement et de sa transmission.

Le recrutement d'hommes de terrain au sein du FBI (mais aussi dans d'autres agences) fut largement privilégié afin de remédier à la prédominance du renseignement électronique dont nous avons vu les limites et les risques.

En outre, le partage de l'information est un point capital sur lequel le FBI s'est concentré tout particulièrement. Avant le 11 septembre aucune base de données inter agence sur le thème du terrorisme n'existait, faute d'équipements techniques compatibles, de procédures standardisées et de méthodes de retraçage harmonisées.

Depuis, divers groupes de travail tels que le : « *Joint Terrorisme Task Forces (JTFS)* », le « *National Joint Terrorisme Task Force (National JTTF)* » ou le « *Foreign Terroriste Tracking Task Force (FTTTF)* » ont été créés au sein du FBI dans le but, entre autres, d'obtenir un meilleur renseignement et de faciliter son échange.

Le FBI, comme l'ensemble de la communauté américaine de renseignement, s'est également attaché à la transmission du renseignement avec les services étrangers.

Ainsi le « *Terrorist Threat Integration Center (TTIC)* » est un organe interne au FBI spécialement conçu pour analyser les renseignements réunis aux Etats-Unis et à l'étranger et concernant la menace terroriste. Il fut remplacé par le *National CounterTerrorism Center (NCTC)* en 2004.

Placé sous l'autorité du *Director of National Intelligence (DNI)*, il a pour mission de constituer à partir des informations du FBI, de la CIA, de la NSA et de la DIA principalement, une base de données d'individus dangereux, suspectés d'être en lien avec le terrorisme. En 2006, le *Washington Post* estimait que celle-ci contenait près de 325 000 noms. Au départ elle ne comportait que quatre types de renseignement par personne. Mais elle s'est bien vite améliorée, de telle sorte qu'elle en compte aujourd'hui parfois jusqu'à quarante.

La création d'une base de données de ce type n'était cependant pas une nouveauté. On estime qu'il en existait treize aux Etats-Unis avant 2001. Mais elles étaient totalement indépendantes et incompatibles, et aucun recoupement ou croisement ne pouvait être réalisé entre elles.

C'est pourquoi ce Centre fut créé, pour répondre au besoin de centralisation de l'information.

Cependant, comme nous le verrons par la suite, le FBI est structurellement et culturellement une entité qui recherche avant tout les preuves après un évènement (qu'il s'agisse d'un attentat terroriste ou de tout autre crime ou délit) ce qui restreint de fait son rôle et son apport dans l'anticipation des attentats.

b) La CIA (*Central Intelligence Agency).*

Créée par le *National Security Act* (NSC) en 1949, la CIA a toujours été spécialisée dans la collecte du renseignement à l'extérieur du territoire national, en faisant appel à des méthodes d'espionnage et des opérations clandestines. C'est le service de renseignement par excellence, et l'agence la plus connue des Etats-Unis. Au contraire du FBI, la CIA recherche elle, de

façon prioritaire, les informations avant que l'évènement ne se produise. Ainsi elle participe en première ligne à la prévention contre les attentats terroristes.

Malgré des efforts de « communication » pour améliorer son image, la CIA demeure un organisme très secret. Ainsi la plupart des statistiques relatives à son fonctionnement ne sont pas publiées de façon officielle et les informations à son sujet sont à mettre au conditionnel : elle serait composée de 16 000 employés pour son quartier général (à Langley en Virginie) emploierait ou collaborerait au total avec 100 000 personnes dans le monde et son budget oscillerait entre 3 et 5 milliards de dollars.

Pour les mêmes raisons que celles invoquées pour le FBI, le 11 septembre provoqua une prise de conscience et des changements.

Alors que depuis la fin de la Guerre Froide, leur nombre sur le terrain ne cessait de baisser, elle a connu à partir de 2003, sa plus importante promotion de nouveaux agents. Le recrutement d'opérationnels et d'analystes dévolus au terrorisme et à la dissémination des armes de destruction massive (aux Etats-Unis on a fait à tort l'association entre les deux notions) a doublé en trois ans.

Des coopérations effectives ont été établies avec plus d'une vingtaine de pays.

De plus en 2005, elle a créé *l'Open Source Center* qui est spécialisé dans le recueil de renseignements via des sources ouvertes. Concrètement, il collecte et traduit les informations des radios et journaux du monde entier. Cependant un tel service n'était pas complètement une nouveauté puisqu'il n'a fait que reprendre les moyens du FBIS (*Foreign Broadcat Information Service*) - tout en les augmentant il est vrai.

La CIA surveille également clandestinement la finance internationale sous la supervision de l'Administration Bush et en partenariat avec la *SWIFT (Society for Worldwide Interbank Financial Telecommunication)*, basée près de Bruxelles[35]. Cette société devenue incontournable pour le secteur bancaire mondial, propose un système de messagerie standardisé et ultra sécurisé ainsi qu'un mécanisme de transfert de fichiers à près de 8000 institutions financières dans plus de 200 pays.

Depuis les attentats, le renseignement américain a certes conclu des accords de coopération avec des sociétés de transfert de fonds ou des réseaux de distributeurs automatiques de billets afin de repérer les activités de terroristes avérés ou potentiels. Mais le programme secret en question est d'une toute autre ampleur puisqu'il porte sur les millions de données transitant par la SWIFT.

Les renseignements issus de la surveillance et l'analyse des transactions auraient permis d'arrêter de nombreux terroristes et notamment le cerveau des attentats de Bali en 2002 : Riduan Isamuddin, alias Hambali.

Néanmoins, la divulgation en 2006 par le *New-York Times* d'un tel programme « clandestin » soutenu par l'administration américaine et mettant directement en cause la CIA, a fait grand

[35] Sur ce sujet, lire : *Comment la CIA épie le financement du terrorisme ?*, Le Figaro, 23/6/08, 2p.

bruit. En effet, on se trouve ici, tant au niveau de la loi que du renseignement proprement dit, dans une « zone grise » qui ne peut qu'interroger, notamment sur la confidentialité des transactions financières de millions de clients dans le monde.

c) La NSA (*National Security Agency*).

Mise en place en 1952 (mais elle existait sous une autre forme depuis 1949), c'est l'agence de renseignement la plus importante des Etats-Unis et probablement du monde. Ses activités sont restées quasi secrètes pendant plusieurs décennies et sont encore aujourd'hui mal identifiées. Son existence n'a d'ailleurs été reconnue de façon officielle qu'en 1957.
La NSA est une agence en charge du renseignement électronique dans le but d'assurer la sécurisation des communications officielles américaines et de « *protéger les intérêts vitaux américains par l'écoute et le déchiffrement des communications susceptibles de porter atteinte à la sécurité nationale* »[36].

A la pointe du renseignement d'origine technique, elle a développé au fil des décennies une connaissance et un savoir faire inégalables en la matière, symbolisés par la création de la *National Cryptologic School*, véritable centre de recherche fondamentale, premier employeur de mathématiciens et d'informaticiens des Etats-Unis. Elle disposerait d'ailleurs des ordinateurs les plus puissants du monde.
La NSA s'est appuyée pendant toute la Guerre Froide mais encore aujourd'hui sur le système d'interception des communications mondiales, plus connu sous le nom de système « *Echelon* », qui ne fut révélé qu'en 1999 (même si des rumeurs sur son existence étaient depuis la fin des années 80).

Basée dans le Maryland, à seulement quelques kilomètres au nord-est de Washington, la NSA emploierait 30 000 personnes et aurait à sa disposition un budget de 4.5 milliards de dollars.

Elle fut l'objet de nombreuses critiques, au même titre que le FBI et surtout la CIA, après 2001. En effet, comme mentionné plus haut, la NSA malgré ses moyens colossaux d'interception, malgré ses ordinateurs ultra puissants, etc., n'est pas parvenue à appréhender correctement et dans les temps l'opération en préparation. Des messages des terroristes du 11 septembre n'ont été traduits que le lendemain, tout simplement parce qu'elle ne bénéficiait pas des capacités analytiques suffisantes pour gérer le flot d'informations.
Bien évidemment, la NSA reste une agence de renseignement technique dont les moyens et prérogatives n'ont pas fondamentalement changé depuis cette date. Cependant, et selon le peu d'information disponibles, sa mission principale serait aujourd'hui de constituer la plus grande base de données d'appels au monde, et de l'analyser (du moins en partie) afin de repérer les cellules terroristes.

[36] *Renseignement*, Politique Internationale n°102, 2004, 511p.

Ainsi, ses prérogatives se seraient considérablement étendues, à la limite parfois de la légalité, et le débat la concernant est vif aux Etats-Unis. En effet les marges de manœuvre qui lui sont octroyées par le gouvernement fédéral depuis 2001, sont très mal connues. L'accès direct, semble-t-il sans restriction ni réel contrôle (extérieur) aux réseaux de télécommunications américains pose des questions fondamentales sur la préservation des libertés individuelles.

3) Le « *Director of National Intelligence* » et le « *500 DAY PLAN* ».

Le 11 septembre 2001 a donc été directement à l'origine de la mise en place de deux grandes initiatives « sécuritaires » générales mais étroitement liées au renseignement : le « *Department of Homeland Security* » et le « *Patriot Act* ».

Prises dans les semaines ou mois après les attentats, elles répondaient avant tout à une situation d'urgence et au double impératif de restaurer la sanctuarisation du territoire américain, et d'identifier des « coupables » … parmi lesquels les agences de renseignement

Souvent plus porteuses d'effets d'annonces pour calmer et rassurer l'opinion publique que de réels et profonds changements, elles furent néanmoins suivies, à partir de 2004, d'une réorganisation « globale » de la communauté américaine de renseignement dont les principales étapes sont : la création du poste de *Director of National Intelligence* (DNI) - et de l'*Office of the Director of National Intelligence* pour l'assister - et la rédaction d'un grand programme de réforme appelé *500 Day Plan*, consécutif au *100 Day Plan*.

a) Le *Director of National Intelligence* (DNI).

Cette fonction fut instaurée en 2004 par l'acte de réforme sur le renseignement et la prévention des actes terroristes ou « *Intelligence Reform and Terrorism Prevention Act (IRTPA)* ». Celui qui l'occupe est le chef de la communauté américaine du renseignement (*United States Intelligence Community*) et travaille sous l'autorité et le contrôle direct du Président des Etats-Unis.

Sa mission s'organise autour de 3 objectifs majeurs[37] :

- Il est le conseiller principal du Président, du *National Security Council* (NSC) et du *Homeland Security* pour tout ce qui concerne le renseignement en rapport avec la

[37] Sources : http://www.dni.gouv/mission.htm

sécurité nationale. Il doit remettre un compte rendu quotidien (daily briefing) au président.

- Il est chargé d'organiser, de coordonner les 16 agences de la communauté du renseignement (US *Intelligence Community*).
- Il est à la tête du programme national du renseignement (*National Intelligence Program*).

Contrairement à ce qui était de coutume par le passé, le DNI a l'interdiction pendant la durée de son mandat de diriger une autre agence de renseignement. En effet jusque là, le directeur de la CIA était également le *Director of Central Intelligence*. Un tel cumul est donc désormais impossible.

Dans sa tâche, le DNI est assisté par l'*Office of The Director of National Intelligence* (ODNI). Véritable agence indépendante, l'ODNI est composée d'environ 1500 employés ; il est la « cheville ouvrière » du Directeur.

b) Les « *100&500 Day Plans* ».

Ces deux plans sont l'une des réalisations majeures de l'ODNI depuis sa création en 2005. Publiés en 2007, ils énoncent une série d'initiatives ayant pour but de construire une coopération renforcée dans le domaine du renseignement.

Le *100 Day Plan* a, dans un premier temps, posé les bases de la nouvelle *National Intelligence Strategy* (NIS) et des transformations à entreprendre puis le *500 Day Plan* les a en très grande partie reprises mais cette fois-ci, pour réellement engager et conduire la réforme.

En préambule, il fait le constat suivant :

L'environnement global a changé. Les Etats-Unis doivent faire face à de nouvelles menaces, en premier lieu la menace terroriste, mais aussi celles des armes de destruction massive (ADM), de la prolifération, des trafics illégaux, etc. C'est pourquoi la Communauté du Renseignement (*Intelligence Community*) doit elle aussi évoluer et s'adapter, via une nouvelle stratégie qui privilégie la collaboration entre les agences concernées mais également en intégrant les entreprises susceptibles de contribuer elles aussi à la sécurité nationale.

Le (s) plan(s) distinguent six grands pôles d'actions et d'objectifs :

- **Créer une culture de collaboration** : le reproche a été maintes fois formulé après le 11 septembre : l'échec des autorités américaines tient en premier lieu au manque de

collaboration, de dialogue entre les agences de renseignement. Il s'agit donc de forger en leur sein et bien évidemment entre elles, une véritable culture de collaboration. Pour cela le Plan propose un certain nombre d'initiatives telles que :

- Créer une Université Nationale du Renseignement.
- Mettre en place un Programme de Renseignement à destination des entreprises.
- Améliorer la formation d'employés parlant les langues étrangères.
- Regrouper et connecter les ressources humaines de la communauté du renseignement.

- **Améliorer et accélérer le partage de l'information :** la collecte, l'analyse et la transmission de l'information sont absolument vitales en matière de renseignement. Pourtant les règles, mécanismes et pratiques sont encore trop souvent marqués par la période de la Guerre Froide, et empêchent ou limitent le partage. Il faut redéfinir, ajuster et ce, en trouvant le bon équilibre entre le besoin de produire de l'information nécessaire aux décisionnaires et le risque que celle-ci puisse menacer les sources, les méthodes, les libertés civiles ou encore serve à l'adversaire. Le plan propose donc plusieurs initiatives :

  - Créer un environnement de l'information qui soit unique et commun.
  - Favoriser et mettre en pratique l'accès et l'exploitation des bases de données.
  - Développer une technologie de l'information avec des entités non membres de la communauté.
  - Mettre en place un guide de classification unique pour la communauté.

- **Promouvoir une transformation des stratégies et moyens de collecte et d'analyse de l'information** : la quantité d'information disponible aujourd'hui est telle que les services de renseignement n'ont plus les moyens suffisants pour l'analyser, repérer les éléments clés et dresser des conclusions précises. Il faut donc faire évoluer les stratégies de collecte puis d'analyse à partir de diverses solutions :

  - Développer des standards communs pour la « communauté » dans son ensemble, concernant les activités du renseignement humain.
  - Renforcer les relations avec les services de renseignement étrangers.

- Augmenter les objectifs en matière de stratégies de collecte intégrées.
- Renforcer le savoir faire analytique dans l'ensemble de la communauté.
- Développer l'utilisation du « *National Intelligence Priorities Framework* »[38].
- Créer un Centre de Coordination National du Renseignement (*National Intelligence Coordination Center*).

- **Conserver le leadership technologique** : durant la Guerre Froide, l'avance technologique des Etats-Unis leur a permis de collecter des informations sur l'ennemi d'alors. A présent, les processus d'acquisition de l'information doivent continuer de s'adapter à de nouveaux adversaires, plus nombreux, plus diffus, en perpétuelle et rapide mutation. Il est proposé :

  - La mise en œuvre d'un Plan pour l'amélioration et l'évolution de l'acquisition.
  - La mise en œuvre d'un Plan de transition concernant les moyens technologiques d'acquisition au sein de la communauté du renseignement.
  - La poursuite et la promotion de façon plus complète et approfondie de tous les projets de recherché avancée en matière d'information(s).
  - La réalisation d'une ingénierie - système et d'une architecture de groupe.
  - Le développement de procédures d'acquisition à la fois souples et de qualité.

- **Moderniser les pratiques commerciales et les procédures** : la communauté du renseignement commence à se concevoir comme une réelle entreprise. Mais placer une autre couche de bureaucratie en plus des structures hiérarchiques existantes ne la fera pas fonctionner de façon intégrée et réactive. C'est toute une organisation qu'elle doit trouver et mettre en place, avec comme priorités le développement d'une stratégie globale planifiée et l'efficacité à tous les niveaux, via par exemple, un processus d'autorisation plus rapide, un partage d'information amélioré et une gestion financière consolidée. Cette nouvelle approche nécessite notamment de :

  - Connaître les besoins et les ressources, améliorer les relations entre la communauté et ses clients.

[38] Il s'agit d'un plan publié en 2003, qui établit précisément et formellement les priorités assignées aux différents services de renseignement pour l'année à venir.

- Travailler au respect de la vie privée et des libertés civiques.
- Perfectionner le processus d'accréditation et certification des équipements informatiques.

- **Clarifier et aligner les pouvoirs du DNI** : l'acte de réforme sur le renseignement et la prévention des actes terroristes a défini le rôle du DNI et renforcé ses pouvoirs pour diriger la communauté de renseignement. Mais il reste à dépasser certaines barrières juridiques ou politiques, certains « chevauchements » qui empêchent encore de construire de nouvelles alliances en interne mais aussi entre le renseignement intérieur et extérieur, entre l'analyse et l'opérationnel, entre les fonctions stratégiques et tactiques. Pour une meilleure production et une Nation d'autant plus et mieux sécurisée, il y a donc lieu de :

  - Définir des droits à décision pour tous les points essentiels (certification, classification, partage, etc.).
  - De les formaliser dans des publications, d'élaborer une véritable doctrine et un lexique du renseignement.
  - De travailler étroitement et de façon cohérente avec Conseil de Sécurité Nationale et au-delà, avec l'ensemble des ministères.

Il est mentionné dans la conclusion de ce rapport, qu'une évaluation des progrès sera effectuée tous les 100 jours de façon à pouvoir éventuellement et au plus tôt repréciser ou corriger les approches. Enfin, le *500 Day Plan* se conclut par cette phrase:

« *We know what must be done…NOW is the time to do it* »[39].

Cette formulation volontariste traduit-elle une réelle détermination qui peut laisser espérer des changements et des améliorations notables ou bien relève-t-elle d'avantage de la communication ?

Nous tenterons de nous prononcer dans le chapitre 3.

Au vu des textes, le mot d'ordre après les attentats de New-York et Washington est au partage de l'information tant dans les agences de renseignement qu'au niveau du DNI ou du *500 Day Plan.*

Et il en va ainsi en « interne » mais aussi en « externe », avec les services étrangers.

[39] « *Nous savons ce qu'il doit être fait…maintenant c'est le moment de le faire* ».

c) La coopération avec les services étrangers.

C'est sûrement l'une des leçons tirées après les attentats du 11 septembre et elle s'est imposée aux services de renseignement du monde entier : par manque de communication, ils n'ont pas pu ou su rassembler et exploiter les éléments dont ils disposaient pourtant sur la menace d'attentats…ils ont donc failli. Renforcer les relations entre eux est alors apparu comme une évidence.

Mais le terrorisme transnational d'origine islamique suppose en lui même une étroite coopération internationale entre les services anti-terroristes et de renseignement. La présence d'Al-Qaïda (ou des organisations menant leur combat en son nom) a été recensée dans près de 60 pays, il est donc indispensable que les services compétents puissent s'échanger des informations.

Et depuis 2001, l'Administration Bush, bien consciente de cette nécessité a développé les coopérations avec l'étranger dans le cadre de la « Guerre contre le terrorisme » et plus spécifiquement dans le domaine du renseignement. Mais cette collaboration repose avant tout - et comme dans le reste de la politique étrangère américaine - sur l'établissement de relations bilatérales avec les autres pays.

Au regard du renseignement, quatre « niveaux » de collaboration peuvent être différenciés :

- Le **1er niveau** concerne des services de renseignement avec lesquels les relations sont les sont plus étroites et les plus anciennes. La coopération dépasse dans ce cas le simple cadre de l'échange d'information, et comprend également l'échange d'officiers de liaisons, la création d'organismes communs et parfois même la réalisation d'opérations conjointes. Citons comme exemples le Royaume-Uni, le Canada, l'Australie, la Jordanie, les Philippines, la Thaïlande, Singapour, etc.

- Le **2ème niveau** désigne tout d'abord des « alliés traditionnels » des Etats-Unis (France, Allemagne, Italie, etc.) qui ont développé avec eux de solides relations à partir de la seconde guerre mondiale, mais surtout pendant la Guerre Froide. Mais il compte aussi des « alliés non traditionnels » (Maroc, Algérie, Egypte, Israël, Turquie, Emirats…) auxquels les américains - et plus spécifiquement la CIA - « sous-traitent » une grande partie des responsabilités de collecte au niveau local et/ou régional, particulièrement au Moyen-Orient. L'échange d'information est régulier et bien institutionnalisé mais peut fluctuer grandement en raison de la conjoncture politique (priorités diplomatiques du moment) ou en raison d'incompatibilités techniques des différents systèmes et procédures.

- Le **3ème niveau** vise des Etats qui sont directement liés au terrorisme international, pour en abriter des activistes au sein de la population et même parfois dans l'armée et en particulier dans les services secrets mais qui se sont rangés - du moins officiellement - aux côtés des Etats-Unis (Yémen, Pakistan, Chine, Arabie Saoudite, Indonésie, Kenya, Soudan etc.) et qui collaborent dans la « guerre contre le terrorisme » instituée par ces derniers. Ce type de rapprochement avait commencé dès les années 90 (notamment pour l'Arabie Saoudite), mais le 11 septembre a accéléré les choses.

- **Le 4ème niveau** fait référence aux plaques tournantes du terrorisme sunnite (Syrie, Liban, Libye) avec lesquelles le partage d'informations se révèle crucial et possible de par la bonne qualité de leurs services de renseignement. Cependant, les efforts importants de collaboration entrepris officiellement, par exemple par la Syrie depuis 2001, sont à relativiser en raison même des régimes politiques en question.

En outre, l'échange de renseignement s'est développé à d'autres niveaux, notamment avec des organisations supranationales : des agents d'*Europol* (l'agence européenne de police à laquelle nous nous intéresserons plus en détail par la suite) se sont installés à Washington et inversement pour des agents américains de la *CIA* et du *FBI*.

Des accords d'entraide pénale et douanière ont également été élaborés et poursuivis avec l'*Union Européenne*, etc. Et s'ils ne portent pas sur du renseignement « pur », ils facilitent le transit d'informations diverses à destination des services de renseignement.

Le « *Partenariat nord-américain pour la sécurité et la prospérité* (PSP) » lancé en mars 2005 par les chefs d'État du Mexique, du Canada et des États-Unis a créé un « *Groupe de Travail sur la Coopération en matière de Renseignement* ». Sa mission est de renforcer les efforts visant à accroître la capacité de ces trois Etats à échanger du renseignement pour lutter contre le terrorisme. Elle s'exerce au travers de trois axes principaux[40] :

- Sécuriser l'inter-connectivité et les communications;

- Accroître les échanges de données pour le dépistage des terroristes;

- Renforcer les capacités d'analyse conjointe de l'information.

[40] Source : http://www.spp-psp.gc.ca/overview/intelligence-fr.aspx

4) Le cas particulier du Renseignement Militaire.

Nous avons vu jusqu'ici les évolutions impulsées aux Etats-Unis après le 11 septembre 2001, au niveau des agences de renseignement et sur la réorganisation de l'architecture globale de la « communauté ».

Mais quelles sont celles qui ont touché le renseignement dit « militaire » ?

a) Définition.

Selon la définition donnée par Jacques Baud le renseignement militaire renvoie à « *l'ensemble des renseignements touchant les forces armées* »[41]. Comme nous l'avons mentionné dans l'introduction, il concerne à la fois le temps de paix et le temps de guerre, et dans tous les cas il collecte des renseignement destinés à la planification militaire d'opérations, qu'elles soient en marche (en temps d'opération militaire), ou seulement éventuelles (en temps de paix). Généralement on estime qu'il peut prendre 3 formes :

- Renseignement Tactique.
- Renseignement Opérationnel.
- Renseignement Stratégique.

Les moyens de collecte qu'il utilise sont variés :

- Les moyens de renseignements par sources ouvertes (*Open Source Intelligence OSINT*) fournissent des informations telles que les statistiques sur la population ou bien sur les pratiques culturelles, politiques et sociales d'une société. Toutefois il s'agit là de données souvent basiques qui doivent être complétées à l'aide d'autres techniques de collecte.
- Le renseignement image ou par imagerie (*Imagery Intelligence IMINT*) donne à partir de l'interprétation des clichés, des informations sur les infrastructures, les bases militaires, et les mouvements de troupes.
- Les moyens de renseignements humains (*Human Intelligence HUMINT*), par les signaux (*Signals Intelligence SIGINT*) et le renseignement dit des Signatures (*Measurement and Signature Intelligence MASINT*) sont également employés.

[41] *Ibid.* Jacques Baud Op.cit.p 27.

Le renseignement militaire sert à la collecte puis à l'analyse des informations concernant l'adversaire. Concrètement, il permet l'évaluation de ses moyens et de ses méthodes.

Cependant, il s'inscrit donc dans le domaine militaire, c'est-à-dire les armées et le champ de bataille. Si bien que son usage aux fins de la lutte anti-terroriste semble à première vue limité à certaines circonstances.

b) L'évolution récente du renseignement d'« intérêt » militaire.

L'évolution du renseignement militaire ces dernières années s'explique principalement par :

- L'émergence du nouveau contexte international après la fin de la Guerre Froide.
- L'incorporation du renseignement militaire au cœur de la « *Guerre contre le terrorisme* » menée par les Etats-Unis depuis 2002.

Si le risque d'une confrontation majeure n'est plus ou s'est éloigné, des situations potentiellement conflictuelles sont apparues ou susceptibles de surgir, et ce parfois très violemment.

Le renseignement militaire se doit donc de contribuer à la prévention, c'est-à-dire à la veille stratégique permanente afin d'alerter les autorités politiques ou militaires sur de possibles crises et risques, notamment ceux consistant en des conflits armés puis de fournir un appui renseignement aux forces en action.

Et aujourd'hui sur le terrain, les forces armées ne doivent plus se battre contre un ennemi « conventionnel » mais contre des acteurs « asymétriques ».

L'action terroriste est devenue progressivement la méthode privilégiée de nombreux groupes, lors de guerres d'usure ou de guérilla comme en Irak ou en Afghanistan actuellement.

Et si le renseignement militaire n'est pas d'une grande utilité contre les groupes/réseaux terroristes « traditionnels », il peut en revanche s'avérer très efficace contre un adversaire utilisant les méthodes du terrorisme. Pour parler d'exemples concrets, il n'aurait pas été en mesure de repérer les membres de l'opération du 11 septembre qui n'était pas de nature et/ou d'intérêt militaire.

En revanche, il a permis de localiser les centres d'entrainement d'Al-Qaïda en Afghanistan, et d'estimer le nombre d'activistes, éventuellement leurs ressources en armes, etc.

Il a su parfaitement trouver sa place au sein de la « *Guerre contre le terrorisme* » lancée par les Etats-Unis depuis 2001, qui a tendance à classer tout groupe armé insurrectionnel dans la catégorie du terrorisme. En effet, au-delà du changement de l'environnement global, le renseignement militaire est devenu l'un des éléments centraux, si ce n'est l'élément central de cette politique orchestrée par l'Administration Bush et il a du s'adapter à ce nouvel « emploi ».

Plusieurs facteurs ont obligé les forces militaires à faire évoluer leur système de renseignement sur le terrain :

- **Le degré d'imprévisibilité et de dangerosité terroristes**. Le monde du renseignement s'est trouvé « démuni » face au terrorisme par définition imprévisible, diffus, fragmenté, etc. Les modèles issus de l'affrontement Est-Ouest sont devenus totalement caducs. Si pendant la Guerre Froide le renseignement militaire servait surtout à collecter des informations « quantitatives » sur « l'autre camp » (effectifs de troupes, nombres de chars, bases militaires, etc.), aujourd'hui la plus grande partie de sa mission consiste à « trouver l'ennemi » qui se fond dans un environnement familier, qu'il connait bien et qui le protège en lui permettant d'être discret.

- **La *révolution dans les affaires militaires* (RAM)**. L'apport massif des nouvelles technologies, en matière de vitesse et de capacités de stockage, de transmission, de traitement de l'information, a fondamentalement transformé la pratique du renseignement militaire.

Cette nouvelle donne a mis le renseignement au centre de la manœuvre des forces armées sur le théâtre d'opération et ainsi :

- Le renseignement militaire est devenu déterminant pour, premièrement localiser les cibles ou - comme on dit dans le vocabulaire militaire - communiquer les renseignements « actionnables » (ceux à partir desquels on peut passer à l'action), et deuxièmement assurer la sécurité des forces armées, désormais confrontées à des dangers bien plus imprévisibles et « violents » que dans le cadre d'affrontements conventionnels. Dés lors, le renseignement militaire fait partie intégrante de toute manœuvre militaire, il est nécessaire à tous les stades de l'intervention.

- Le renseignement militaire a du faire preuve d'une plus grande adaptabilité, flexibilité, souplesse, vitesse de réaction pour répondre aux nouveaux besoins. Depuis quelques années, les forces militaires doivent elles mêmes faire face à une importante augmentation de la gamme de leurs interventions puisqu'elles prennent en charge des

taches autrefois en dehors de leurs attributions comme l'aide humanitaire, gèrent des projets civilo-militaires, participent à des actions anti drogues, etc.

En définitive, les forces armées présentes sur le terrain ont à faire à des enjeux multiples. Pour mener à bien leur mission, elles doivent davantage que par le passé avoir une vision, une compréhension globale de la situation. Aussi le renseignement doit être en mesure de leur fournir des éléments politiques, sociaux, économiques, culturels, environnementaux, religieux etc.

C'est pourquoi aujourd'hui on ne parle plus de « renseignement militaire » stricto sensu mais de renseignement d'« intérêt militaire ». Ce changement de vocable traduit bien cette nouvelle réalité et le fait que le renseignement sur le théâtre d'opération ne concerne plus uniquement l'aspect militaire mais qu'il s'étend à tout l'environnement.

Cette évolution est un défi important et exigeant, tant techniquement qu'humainement, mais ce renseignement d'« environnement » est de nos jours vital pour les forces armées et incontournable en matière de défense et de sécurité militaire.

Mais concrètement, quel est le rôle du renseignement militaire dans le cadre de la lutte contre le terrorisme instituée depuis 2001 aux Etats-Unis ?

Prenons l'exemple concret de la *Defense Intelligence Agency* (DIA).

c) Exemple concret avec la : *Defense Intelligence Agency (DIA)*.

Il s'agit de l'agence principale de renseignement militaire aux Etats-Unis.

Créée en 1961 et rattachée au Département de la Défense (son siège central se trouve au Pentagone), elle emploie entre 8000 et 11000 personnes à travers le monde.

Elle a toujours joué un rôle central contre toutes les menaces d'agression dirigées contre l'empire américain : les missiles cubains dans les années 60, la lutte contre l'ennemi soviétique pendant la Guerre Froide, le terrorisme transnational depuis 2001 (mais aussi contre la prolifération des ADM ou le narcotrafic).

Elle fut donc présente à tous les stades de la riposte militaire américaine consécutive aux attentats du 11 septembre :

- En Afghanistan lors de l'opération *Enduring Freedom*.
- Mais aussi dans toutes les régions du monde où la riposte américaine aux attentats prit place. Ce fut le cas par exemple aux Philippines ou dans la Corne de l'Afrique.
- Lors de l'opération *Iraqi Freedom*, qui en mars 2003 sonna le début de la guerre d'Irak : la DIA fournit des renseignements sur l'état des troupes ennemies, sur leur armement, sur les dommages qu'elles subissaient.
- Aujourd'hui les personnels de la DIA sont déployés sur tous les théâtres d'opération à travers le monde, en support des commandements militaires qui luttent contre le terrorisme.

Le renseignement militaire, par l'intermédiaire de la DIA est donc pleinement intégré à l'effort américain de lutte contre le terrorisme.

Il s'insère même en premier lieu dans la vision américaine de lutte « armée » contre le phénomène. En effet, dans d'autres pays - la France en particulier - même si les forces militaires font partie du spectre de la lutte, elles n'interviennent souvent qu'en dernier recours.

En schématisant, la position « européenne » considère que le terrorisme est une lutte globale contre des actions criminelles donnant d'une part la priorité aux actions judicaires, policières et de renseignement, et engageant d'autres part des actions d'aides économiques, de formations, de dialogues culturels, etc.

À l'inverse, les Etats-Unis et Israël ont toujours perçu et organisé cette lutte autour d'un nécessaire recours aux moyens militaires.

C'est l'idée que la conception européenne est basée sur la « protection », la vision américaine sur l'« action-réaction ».

Avant de clôturer cette partie consacrée au renseignement aux Etats-Unis, il nous faut aborder une tendance relativement nouvelle mais pour le moins réelle du renseignement américain : celle de son externalisation ou de sa privatisation.

5) La nouvelle tendance à l'« externalisation »[42].

L'« externalisation » ou la « privatisation » de la sécurité n'est pas un phénomène nouveau, surtout aux Etats-Unis mais il s'est largement développé à l'orée du nouveau millénaire et devint particulièrement visible à partir de 2003 avec la guerre en Irak. Plusieurs « bavures », dont celle concernant la société *Blackwater*[43] permirent d'en mesurer l'ampleur.

Aujourd'hui, on estime qu'entre 20 000 et 30 000 personnels armés sont employés par des sociétés de sécurité privées en Irak, pour le compte du gouvernement américain. Et ce chiffre atteindrait même 180 000 pour l'ensemble des contrats passés par le Pentagone et le Département d'Etat avec ces mêmes entités privées dans le monde.

En revanche, on a découvert beaucoup plus récemment que la tendance touchait les agences de renseignement américaines, notamment pour la CIA et la DIA, et que le cœur de la sécurité nationale n'était donc pas « à l'abri ».

Pourtant, comme le dit Raphael Ramos[44], cette pratique «*…remonte aux origines de la nation américaine […] ainsi durant la Guerre d'Indépendance, le Général Georges Washington eut recours à de nombreux réseaux d'espions civils. De même, au XIXème siècle, la société du célèbre Allan Pinkerton menait des activités d'espionnage pour le compte du gouvernement américain* ».

Mais au cours du 20ème siècle, la professionnalisation du renseignement y avait mis fin.

Et ce n'est seulement à partir des années 90 que l'externalisation du renseignement reprend aux Etats-Unis jusqu'à connaître une véritable explosion depuis le 11 septembre 2001.

a) L'externalisation du renseignement : davantage qu'une simple tendance, une véritable réalité.

Les données chiffrées ne sont pas aisées à obtenir car le sujet prête à polémique et surtout les activités de renseignement sont par essence secrètes.

Cependant, près de 70% du budget de la communauté américaine du renseignement serait consacré à des contrats passés avec des entreprises privées. Si l'évaluation est difficile et le résultat contesté, ce taux ne serait pas inférieur à 50% dans tous les cas.

Cette réalité serait généralisée à l'ensemble des agences américaines, mais affecterait plus celles spécialisées dans le renseignement technique, un domaine d'activité très onéreux, où

[42] Concernant le thème de l'externalisation du renseignement aux Etats-Unis lire : Raphael Ramos, *Externalisation du renseignement : l'exemple des Etats-Unis*, European Strategic Intelligence and Security Center (ESISC), Décembre 2007, 10p.
[43] Société de sécurité, employée par le gouvernement américain en Irak et qui fit 17 morts civils irakiens au cours d'une fusillade dont les circonstances sont restées très vagues.
[44] Chercheur à l'ESISC (voir note 40).

l'intervention d'acteurs privés est en mesure de décharger les gouvernements d'une partie des coûts de fonctionnement :

- Ainsi la NSA aurait signé en 2001 un contrat de plus de 2 milliards de dollars avec des contractants privés et pour une durée de 10 ans, portant sur les technologies de l'information et de communication[45].
- La moitié des 14 000 employés de la *National Geospatial-Intelligence Agency* (NGA) serait issue d'acteurs extérieurs au gouvernement[46].

Mais l'externalisation vise également le renseignement humain. Citons quelques exemples :

- La *Counterintelligence Field Activity* (CIFA) consacrerait de l'aveu même de son directeur, près de 70% de ses crédits à de la sous-traitance[47].
- En Mai 2007, des juristes de la DIA indiquaient que plus de la moitié du personnel de l'agence provenait de sociétés privées[48].
- La CIA est elle aussi largement concernée, puisque 1/3 de ses employés ne proviendrait pas du gouvernement[49], une proportion qui monte à près de 75% pour sa cellule Pakistanaise d'Islamabad.

L'essor est net mais quelles en sont les raisons ?

*L'ensemble des notes 44 à 50 sont tirées de: Raphael Ramos, *Externalisation du renseignement : l'exemple des Etats-Unis*, European Strategic Intelligence and Security Center (ESISC), Décembre 2007, 10p.

[45] Major Glenn J. Voelz, USA, *Managing the Private Spies: The Use of Commercial Augmentation for Intelligence Operations*, Washington D.C., Center for Strategic Intelligence Research, Joint Military Intelligence College, juin 2006, p. 12.

[46] Tim Shorrock, *The corporate takeover of U.S. intelligence*, Salon.com, 1er juin 2007. http://www.salon.com/news/feature/2007/06/01/intel_contractors/

[47] Walter Pincus, *Increase in Contracting Intelligence Jobs Raises Concerns*, The Washington Post, 20 mars 2006 http://www.washingtonpost.com/wp-dyn/content/article/2006/03/19/AR2006031900978.html

[48] R.J. Hillhouse, *Outsourcing Intelligence*, The Nation, 24 juillet 2007. http://www.thenation.com/doc/20070730/hillhouse

[49] Walter Pincus, Stephen Barr, *CIA Plans Cutbacks, Limits on Contractor Staffing*, The Washington Post, 11 juin 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/06/10/AR2007061001180.html

b) L'« explosion » amorcée par le 11 septembre.

L'évolution de l'externalisation est à rattacher à celle du monde après la chute du mur de Berlin. La fin du contexte stratégique issu de la Guerre Froide engendre dans un premier temps un « vide »…une sorte de « pacification globale » est escomptée si bien que les pays réduisent leurs budgets de Défense.

Ainsi aux Etats-Unis, entre 92 et 96, les effectifs du *Département de la Défense* ont diminué de 16%[50] et ceux de la CIA de près de 25% en 10 ans[51], les agences de renseignement étant elles aussi impactées par ses restrictions financières.

Pour autant, elles continuaient d'être sollicitées par le gouvernement américain, mais leur activité quant à elle, ne baissait pas. Au contraire, les demandes en renseignements, de même que les attentes, demeuraient toujours très élevées, notamment pendant la guerre du Golf. Les agences devaient faire donc aussi bien, mais avec moins de moyens.

Pour faire face à cette problématique, les agences américaines se sont tournées pour la première fois vers des acteurs privés

Mais, c'est le 11 septembre qui va transformer ce recours conjoncturel en une réalité bien marquée, en faisant exploser la part des acteurs privés au sein des activités de renseignement pour le gouvernement.

En effet, les américains se lancent après les attentats dans leur « guerre contre le terrorisme ».

Les agences américaines doivent répondre non seulement aux besoins de renseignements pour se prémunir contre une nouvelle attaque sur leur territoire, mais également à ceux des forces militaires actives en Afghanistan, puis en Irak, ou encore dans toutes les régions du monde ou les américains sont militairement engagés (contre le terrorisme islamiste).

Même si le budget de la communauté américaine de renseignement a augmenté à cette époque (de 26 milliards de dollars en 2001 à environ 45 milliards aujourd'hui), c'est très insuffisant compte tenu de la multiplicité et du volume des besoins.

L'externalisation vers le secteur privé s'impose et réalise ainsi de façon quasi-mécanique avant tout pour des aspects et nécessités budgétaires.

Mais il convient de préciser qu'elle fut favorisée par deux autres facteurs :

- **La mutation « technologique » du renseignement** : antérieure à la « guerre contre le terrorisme », elle a généré une augmentation considérable de l'utilité des renseignements électromagnétiques ou d'origine image. Les agences

[50] Major Glenn J. Voelz, USA, *Managing the Private Spies: The Use of Commercial Augmentation for Intelligence Operations*, Washington D.C., Center for Strategic Intelligence Research, Joint Military Intelligence College, Juin 2006, p. 12.
[51] George Tenet, *Written Statement for the Record of the Director of Central Intelligence Before the National Commission on Terrorist Attacks Upon the United State*, 24 mars 2004, p. 24. http://www.9-11commission.gov/hearings/hearing8/tenet_statement.pdf

gouvernementales, en premier lieu la NSA ont du s'adapter à cette mutation technologique, et engager de lourdes dépenses pour acquérir et mettre à jour ces nouveaux systèmes. Mais le développement concomitant des « Start-up », désireuses de passer des contrats avec le gouvernement va faire naître une convergence d'intérêts et leur permettre de mieux supporter cette transition technologique. De même, quelques années plus tard, avec le développement d'Internet et du renseignement issu des « sources ouvertes », des acteurs privés sont venus palier le manque de linguistes ou traducteurs dans les agences gouvernementales de renseignement et ce, d'autant plus que le renseignement de sources ouvertes ne nécessite pas d'habilitation de sécurité, contrairement aux autres types de renseignement.

- **L'absence de réforme :** en effet, faire appel à des acteurs extérieurs qui « composent » les activités des agences gouvernementales, permet premièrement à ces mêmes agences de limiter les mesures de changements et deuxièmement de « compenser » l'activité des agences gouvernementales quand ces dernières ne parviennent pas - même lorsqu'elles le veulent - à faire évoluer leurs pratiques (ou pas assez vite). C'est donc un moyen de contourner la réforme ou d'éviter de faire évoluer trop radicalement un mode de fonctionnement parfois hérité de plusieurs décennies de pratique. Bouger de telles machines bureaucratiques n'est pas chose aisée. En recourant à des entreprises privées, l'Etat s'adapte au nouvel environnement, mais sans passer par des réformes coûteuses et souvent décriées.

II) Refonte au niveau des organisations internationales (ONU, OTAN, UNION EUROPEENNE).

1) L'approche des Nations Unies.

L'ONU ne dispose pas de capacités intrinsèques de collecte ni d'un organe qui serait spécifiquement consacré au renseignement.
Cependant, de par son action ancienne et dynamique dans la lutte anti-terroriste au plan mondial, elle participe à son niveau à l'activité du renseignement.

a) Approche jusqu'au 11 septembre 2001.

Le terrorisme a figuré très tôt à l'ordre du jour des Nations Unies, à une époque où il ne faisait pas encore l'objet de dispositions, de politiques, de stratégies vraiment spécifiques et communes au sein d'organisations internationales et où les législations étatiques lui étant propres n'existaient quasiment pas.

Certaines conventions avaient bien été préalablement signées, comme celle de la *Société des Nations (SDN)* sur la « prévention et répression du terrorisme » adoptée le 6 novembre 1937. Mais la plupart ne furent jamais ratifiées ou furent des échecs. Les années 60 avec la multiplication des actes terroristes vont donner le réel point de départ d'une démarche concertée, pour formaliser l'action et réaliser des avancées concrètes. Des conventions sur la sécurité dans l'aviation sont proposées au niveau de *l'Organisation de l'Aviation Civile Internationale (OACI)* mais également à l'ONU.

Les membres de l'ONU signent le 14 septembre 1963, à Tokyo, celle relative aux « infractions et à certains actes survenant à bord des aéronefs » et le 16 décembre 1970, à la Haye celle pour la « répression de la capture illicite d'aéronefs ».

Mais c'est en 1972 qu'intervient le vrai tournant. Aux Jeux Olympiques de Munich, onze athlètes israéliens sont tués par des terroristes palestiniens. Cet événement marque profondément les esprits et montre que le phénomène terroriste prend de l'ampleur. Il utilise de plus en plus les technologies modernes (notamment les avions pour des prises d'otages). Les Etats n'ont pas les moyens techniques mais surtout juridiques et conceptuels pour le combattre efficacement. Aucune définition officielle ne fait foi et la confusion règne entre le « véritable terrorisme » et les luttes dites ou pouvant apparaître « justes », comme celles de libération(s) nationale(s) ou de libération à un « oppresseur ». De plus, les mesures entreprises ne concernent souvent que des actes terroristes ciblés, comme les détournements d'aéronefs, les enlèvements de diplomates, etc.

C'est pourquoi, le 18 décembre 1972 est adoptée la résolution 3034 des Nations Unies qui débouche sur la constitution d'un comité spécial de trente-cinq membres, chargés d'effectuer un rapport sur le terrorisme international. Pendant la décennie 70, il se réunit à plusieurs

reprises avec comme thèmes majeurs la « *définition du terrorisme international, ses causes sous-jacentes et les mesures à prendre afin de lutter contre ce phénomène* »[52].

Une définition commune n'est cependant toujours pas trouvée.

Durant ces années là, mais également par la suite, les Nations Unies « *entretiennent une relation particulièrement tendue avec le renseignement […] durant la Guerre Froide le terme de « renseignement » donnait à l'organisation un relent de conflit Est-Ouest, au dessus duquel elle voulait se maintenir* »[53]. Pendant longtemps, on ne parlera d'ailleurs pas de « renseignement » mais d'« information » au sein des Nations Unies, pour éviter les amalgames avec les activités douteuses du renseignement qui faisaient alors les gros titres de la presse pendant ces années là.

Mais cette situation n'empêche pas l'ONU de jouer un rôle majeur pendant trois décennies, en recommandant aux pays membres des mesures concrètes à mettre en œuvre pour lutter contre le terrorisme et en adoptant plusieurs conventions : cinq « internationales » et sept « régionales » dédiées elles aussi au terrorisme international.

Elle concentrera son action sur les points spécifiques suivants :

À l'international :

- Elle veut faciliter **l'échange d'informations entre les Etats**.
- Elle entend favoriser la coopération judiciaire entre les Etats.
- Elle invite les Etats à signer et ratifier toutes les conventions internationales et régionales sur le terrorisme.
- Elle les encourage à créer des accords bilatéraux et multilatéraux.

Sur le plan national :

- Elle demande aux Etats d'adapter leur législation nationale aux conventions internationales.
- Elle les appelle à ajuster leur système judiciaire dans le but de pouvoir poursuivre les auteurs d'actes terroristes dans le cadre de tribunaux ordinaires.

[52] Sandrine Santo, *L'ONU face au terrorisme*, Groupe de Recherche et d'Information sur la Paix et la Sécurité (GRIP).
[53] *Ibid.* Jacques Baud Op.cit.p 27.

- Elle incite à combattre le financement et à ne pas accueillir de terroriste sur leur territoire.

L'objectif premier est donc d'élaborer un cadre juridique complet pour combattre et punir les auteurs.

Concernant le renseignement, l'ONU n'a pas de capacités de collecte à proprement parler. Mais d'un point de vue général, l'action pour l'homogénéisation des législations et des systèmes judiciaires des Etats, ainsi que les divers encouragements pour la signature d'accords bilatéraux et multilatéraux entre ces mêmes Etats, etc., ne peuvent que concourir à un meilleur partage du renseignement.

L'ONU œuvre donc pour faciliter l'échange d'information entre les Etats, à défaut de pouvoir en « produire » elle-même. Le *Département des Opérations de Maintien de la Paix (DKPO)* créé en 1993 dispose en effet d'un *Centre de Situation (SitCen)* au sein de son *Office des Opérations,* qui rassemble des spécialistes du renseignement issus des pays membres. Mais il s'agit d'un organe qui met en commun le renseignement issu du terrain où sont déployées les forces lors d'une opération de maintien de la paix et qui est donc dépourvu de moyens de collecte. Donc il n'œuvre pas dans le cadre de la lutte anti-terroriste.

Mais qu'en est-il advenu après le 11 septembre ?

b) L'amorce de règles plus contraignantes après le 11 septembre 2001…mais qui concernent la lutte anti-terroriste en général.

Nous pouvons dire d'emblée que la situation du renseignement spécifiquement, n'a pas beaucoup évolué au sein des Nations Unies.

Deux résolutions majeures et en rapport avec la lutte contre le terrorisme sont pourtant votées après les attentats :

- Dès le 12 septembre, une réunion extraordinaire du Conseil de Sécurité vote la résolution 1368 qui les condamne catégoriquement. Elle appelle à la solidarité de tous les Etats membres et de la communauté internationale, en vue de retrouver et de sanctionner les auteurs. Mais au-delà, elle signifie et retranscrit la volonté de combattre le terrorisme international et rend par ailleurs légitime une éventuelle riposte américaine (qui débouchera sur la guerre d'Afghanistan).

- Mais c'est la résolution 1373 adoptée par le Conseil de Sécurité le 28 septembre 2001, qui bouleverse réellement le cadre jusqu'alors établi en instituant des prérogatives très explicites, avec un caractère d'obligation certain. Des sanctions

peuvent être engagées en cas de refus ou manquement des Etats membres vis-à-vis d'elle.

Cette résolution se concentre sur plusieurs points :

- Les Etats doivent prendre toutes les mesures nécessaires pour priver les groupes terroristes de leurs ressources financières.
- Elle impose d'adapter la législation nationale de chaque Etat afin d'assurer une meilleure répression.
- Elle interdit aux Etats de fournir asile ou quelque appui que se soit, aux terroristes.
- Elle réitère ses demandes **de coopération entre les Etats notamment pour une meilleure circulation du renseignement**.

Un certain nombre de prérogatives et décisions de cette résolution figuraient déjà dans deux conventions importantes négociées à la fin des années 1990 : « *la Convention Internationale pour l'Elimination des Attentats Terroristes (1997)* » et la « *Convention pour la Répression du Financement du Terrorisme (1999)* » mais beaucoup ne furent jamais appliquées.

C'est pourquoi la résolution 1373 lance également la création d'un « *Comité Contre le Terrorisme (CCT)* ». Composé de 15 membres et intégré au Conseil de Sécurité, il est chargé de l'application de ces injonctions. Le caractère « facultatif » qui modérait dans le passé la portée de nombreuses législations votées à l'ONU, disparaît ici, puisque la résolution 1373 est censée engendrer des « sanctions » pour les pays ne la respectant pas.

Il s'agit ici probablement de la plus « grande » avancée concernant le renseignement au sein des Nations Unies bien que ce soit de façon indirecte, via la lutte contre le terrorisme en général et sans que l'ONU ne se dote d'un organe spécifique consacré au renseignement, et encore moins de capacités propres de collecte. Cependant le Comité et sa direction collaborent avec de nombreuses organisations internationales, d'organismes régionaux et locaux, mais aussi avec des services de renseignement.

Les Nations Unies ont donc très largement renforcé leurs prérogatives contre le terrorisme international après le 11 septembre essentiellement par le biais des résolutions 1368 (12 septembre 2001) et surtout 1373 (28 septembre 2001). Si elles ne sont pas foncièrement novatrices ou inédites sur le fond, l'aspect « obligatoire » qui réglemente leur application est lui tout à fait nouveau. Mais l'activité du renseignement n'a pas fait quant à elle l'objet de dispositions particulières.

2) L'approche de l'OTAN.

a) Réorientation vers la lutte anti-terroriste après la chute du Mur.

L'Alliance Atlantique fut créée en 1949 à l'initiative de douze Etats, puis s'est élargie à plusieurs reprises par la suite, pour atteindre aujourd'hui 26 membres. Organisation de défense collective, elle a rempli son rôle contre la menace communiste et des pays du Pacte de Varsovie pendant toute la Guerre Froide.

A l'époque elle n'est pas - ou que très peu - concernée par le terrorisme, lequel n'est alors que marginal et extérieur à l'OTAN, sans caractère transnational. Il se rapporte au conflit israélo palestinien, ou bien à des territoires où le processus de décolonisation se fait dans la violence.

Mais la fin du communisme et par la même occasion de l'affrontement Est-Ouest à partir de 1989, change considérablement l'environnement international. Et se pose alors la question du maintien de l'OTAN dans un monde ou la menace représentée par le communisme et le pacte de Varsovie n'est plus.

Plusieurs options se présentent alors aux membres de l'Alliance Atlantique[54] :

- Laisser l'OTAN en l'état.
- Dissoudre l'Organisation.
- La moderniser.

C'est cette dernière option qui sera finalement retenue. D'importantes réformes militaro-stratégiques vont être entreprises, et l'OTAN accueille d'anciennes Républiques Soviétiques qui viennent de prendre leur indépendance.

Mais surtout, elle va opérer au cours des années 90 une nette réorientation vers la lutte anti-terroriste grâce à laquelle elle trouve une forme de légitimation quant à son existence même (son rôle de « défense militaire » de l'espace européen contre les menaces « classiques » n'est toutefois pas abandonné).

En 1999, elle adopte un nouveau concept stratégique qui reconnaît pour la première fois que le terrorisme représente un danger réel pour la sécurité de l'Alliance et développe son action contre lui.

Mais le 11 septembre 2001 va indubitablement entraîner le renforcement des capacités de renseignement dans ce domaine.

[54] Sur ce thème lire : Daniel Colard, *Le rôle de l'ONU, du G8 et de l'OTAN dans la coopération internationale contre le terrorisme*, Arès N°56, Volume XXII, Décembre 2005, 12p.

b) Augmentation des capacités anti-terroristes et de renseignement après le 11 septembre 2001.

Pour la première fois depuis sa création, l'OTAN invoque après les attentats, l'article 5 du Traité de l'Alliance Atlantique qui déclenche les mécanismes de sécurité collective. Puis, elle s'engage sur le théâtre afghan, notamment en prenant le commandement de la *Force Internationale d'Assistance et de Sécurité (FIAS)* à partir de 2003.

L'après 11 septembre marque une réelle accélération de l'action de l'OTAN dans la lutte contre le terrorisme :

- Le 18 décembre 2001, les ministres de la Défense des pays membres chargent l'autorité militaire (NMA) d'élaborer un nouveau *Concept Militaire* sur la défense contre le terrorisme. Entériné lors du Sommet de Prague en septembre 2002, il édite, entre autres, une vue d'ensemble de l'action anti-terroriste menée au sein de l'OTAN pour les années à venir. Bien qu'étant une organisation militaire, l'Alliance Atlantique conçoit le champ de son intervention au-delà de la simple action armée contre les groupes et réseaux. Afin de renforcer ses capacités, elle entreprend un certain nombre de mesures dont le « *Plan d'action du Partenariat contre le terrorisme* »[55] de 2002 sera le fer de lance et qui vise à la protection des risques, l'aide aux alliées ou aux autres pays sous la menace terroriste, ou encore la **coopération dans le renseignement** et **l'échange d'information** (mesures qui seront renforcées et complétées en 2004 au Sommet d'Istanbul).

Le *Concept Militaire* recense quatre missions distinctes pour l'OTAN : Si deux apparaissent « classiques » en matière de défense contre le terrorisme (anti-terrorisme/contre-terrorisme), les deux autres étendent le spectre de l'intervention à la « coopération civilo-militaire » et à la « gestion des conséquences » :

- L'anti-terrorisme : regroupe les mesures défensives pour permettre de faire baisser la vulnérabilité des biens, des personnes et des infrastructures. Bien qu'il soit du ressort de chaque pays, l'OTAN peut intervenir en soutien pour tout pays qui en ferait la demande. Le **renseignement** et surtout un bon « ***partage des données du renseignement*** »[56] est cité comme l'un des éléments clés pour prévenir les attaques terroristes et s'en protéger.
- Le contre-terrorisme : regroupe les mesures offensives militaires pour réduire et contrer les moyens des terroristes. Ces opérations sont essentiellement interarmées,

[55] Elaboré par les membres du *Conseil de partenariat euro-atlantique (CPEA),* un organisme de l'OTAN.
[56] Extrait du rapport sur le : *Concept militaire de l'OTAN relatif à la défense contre le terrorisme*, consultable à cette adresse : http://www.nato.int/docu/terrorisme-f.htm

conduites par des unités spécialisées et peuvent être menées sous l'égide de l'OTAN ou avec son soutien. Et là encore il est fait mention de l'importance de disposer de **structures de renseignements adéquates** pour parvenir à une efficacité maximale.

- La gestion des conséquences : concerne toutes les mesures de réaction pour atténuer les effets d'une attaque.

- La coopération civilo-militaire : le rapport constate qu'une opération militaire seule ne suffit pas ou ne suffit plus à annihiler le terrorisme et éviter qu'il ne renaisse. Il faut aujourd'hui coupler les interventions armées, avec des initiatives économiques, sociales, juridiques, diplomatiques, etc. Et les forces armées de l'OTAN doivent jouer un rôle de soutien auprès des autorités civiles (services de police, des douanes, de l'immigration, **services de renseignement** et de sécurité, etc.) pour optimiser les actions contre le terrorisme.

- Auparavant, le 20 septembre 2001 avait été instaurée au sein de l'Etat-major de l'OTAN, une cellule de réflexion sur la menace terroriste. Et de manière plus globale, l'idée selon laquelle le terrorisme représente désormais la menace la plus sérieuse contre les membres de l'Alliance Atlantique et qu'il faut en conséquence développer des stratégies, systèmes, moyens, etc., pour le combattre, fait l'objet d'un large consensus.

- L'OTAN mène également son action au sein du *Conseil OTAN-Russie* et du *Conseil de partenariat euro-atlantique*. Tous deux ont élaboré un plan d'action contre le terrorisme. L'alliance a développé également des coopérations avec des pays du « Moyen-Orient élargi » tels que l'Algérie, l'Egypte, la Jordanie, la Mauritanie, la Tunisie, le Maroc et Israël. En octobre 2001, elle lança l'opération militaire « *Active Endeavour* » pour combattre le terrorisme en Méditerranée tant sur la mer qu'en provenance de la mer laissant une large place (et de plus en plus) à l'échange de renseignement pour cibler les navires suspects ou présentant un intérêt particulier. Ainsi « *l'opération Active Endeavour s'est de plus en plus transformée en une opération axée sur l'information et le renseignement* »[57].

- Elle a aussi davantage coopéré avec d'autres organisations internationales :

  - Avec l'ONU, en contribuant aux travaux du *Comité contre le Terrorisme* mais aussi avec d'autres agences Onusiennes, notamment pour la réaction en cas de catastrophe internationale et la gestion des conséquences.

  - Avec l'Union européenne via *Eurocontrol*[58], ainsi qu'avec l'*Organisation de l'aviation civile internationale (OACI)*, l'*Association du transport aérien international*

[57] Brochure de l'OTAN : *Combattre le terrorisme en mer*.
[58] Organisation créée en 1963 dans le cadre européen, pour la sécurité de la navigation aérienne.

(IATA), l'Office *contre la drogue et le crime (UNODC)*, l'*Alliance pour la sécurité et coopération en Europe (OSCE)*, etc.

Parallèlement, les capacités de renseignement vont être sensiblement rehaussées et réorientées pour lutter contre le terrorisme.

L'Alliance Atlantique ne dispose pas de services de collecte de renseignement à proprement parler. Mais son rôle dans ce domaine est cependant plus important que celui des Nations Unies, même s'il s'exerce non pas de façon directe mais seulement par le biais des Etats membres et de leurs services spécialisés.

Concrètement le renseignement au sein de l'OTAN s'organise autour de plusieurs entités et initiatives[59] :

- Tout d'abord, l'*Etat-major International (EMI)* au sein duquel la *Division du Renseignement* (*Intelligence Division*) informe quotidiennement le *Conseil de l'Atlantique Nord*, le *Comité Militaire*, le *Conseil et Comité des Plans de Défense* et les autres organismes de l'organisation tels que le *Comité Politique* et le *Centre sur les Armes de Destruction Massive*. Cette division comporte elle-même deux branches : l'une dévolue au *Renseignement de Base (Basic Branch)* et l'autre au *Renseignement de Situation (Warning-Branch)*. Elle reçoit exclusivement les contributions des Etats membres et joue donc le rôle de coordination centrale du renseignement au sein de l'OTAN. Elle élabore également des documents sur la politique de renseignement globale de l'organisation, alimente des bases de données, administre des fonctions liées aux alertes et aux gestions de crises et organise la liaison avec des pays qui exécutent des fonctions de renseignement spécialisés. En résumé « *la division renseignement, appuyée par les pays et commandement de l'OTAN, informe en permanence les organismes principaux de l'Alliance, aide le Comité Militaire à formuler des avis militaires à l'intention des autorités politiques, fournit le fondement en matière de renseignement qui permet d'orienter la composition, l'organisation et les opérations des forces de l'OTAN, et accomplit un vaste éventail de tâches à l'appui des rôles politiques et de défense de l'OTAN* »[60].

- Le *Comité Spécial* a vu ses attributions étendues et renforcées après le 11 septembre. C'est un « *organe consultatif du Conseil de l'Atlantique Nord pour les questions*

[59] Pour plus d'informations sur l'organisation du renseignement au sein de l'OTAN :

- *Le renseignement et la lutte contre le terrorisme*, Jacques Baud, Lavauzelle, 2005, 413p.
- Marc Francina, *Rapport au nom de la commission de la Défense Nationale et des forces armées sur le projet de loi (n°2277 rectifié) modifiant les articles **414-8** et **414-9** du **code pénal***, Assemblée Nationale, Janvier 2007, consultable à l'adresse suivante : http://www.assemblee-nationale.fr/12/rapports/r3648.asp

[60] *Ibid.* Brochure OTAN Op.cit. p 65.

d'espionnage et de menaces terroristes ou connexes qui pourraient affecter l'Alliance »[61]. Composé des chefs des services de renseignement et de sécurité de tous les Etats membres, sa mission principale est la production de documents analytiques sur la menace terroriste qui pourrait s'abattre sur les membres de l'Alliance.

- En octobre 2001, et suite à la demande des américains, l'OTAN a adopté une série de mesures (au nombre de huit) concernant la lutte contre le terrorisme, parmi lesquelles figurait une intensification des échanges de renseignements au sein de l'Alliance.

- Par la suite, cette volonté, cette détermination des membres de l'organisation pour un meilleur partage du renseignement ne s'est pas démentie. A titre d'exemple, lors de la Déclaration du Sommet de Riga (28-29 novembre 2006), il est souligné à plusieurs reprises par les Chefs d'Etat et de gouvernement, l'importance d'une bonne coordination dans ce domaine :

  - « *Nous appelons les Alliés à continuer de développer et à mettre pleinement en œuvre leurs capacités nationales dans ce domaine important, et à renforcer l'aptitude de l'Alliance à* ***partager les informations et les données du renseignement sur le terrorisme****, en particulier à l'appui des opérations de l'OTAN* »[62].

  - « *L'adaptation de nos forces doit se poursuivre. Nous avons entériné une série d'initiatives visant à accroître l'aptitude de nos forces à répondre aux menaces et défis de notre époque. Il s'agit notamment de s'employer à* ***développer une capacité en réseau de l'OTAN pour partager les informations, les données et les éléments du renseignement d'une façon fiable et sûre****, qui ne retarde pas les opérations de l'Alliance, tout en améliorant la protection de nos systèmes informatiques clés contre les cyber attaques. Il s'agit* ***d'activer un centre de fusion des données du renseignement pour améliorer le partage des informations et des données du renseignement*** *dans le cadre des opérations de l'Alliance* »[63].

- Ce centre avait vu le jour un mois plus tôt, en octobre 2006 sous l'acronyme : *IFC* pour *Intelligence Fusion Center*. Il octroie véritablement pour la première fois, une capacité opérationnelle de renseignement au sein de l'Alliance Atlantique puisqu'il est spécialisé dans la collecte et la distribution du renseignement, surtout celui à vocation militaire à destination des forces Otaniennes. Les Etats-Unis font office de nation cadre au sein de cette entité, mais tous les membres de l'organisation sont invités à y participer.

[61] Source : http://www.nato.int/issues/special_committee/index-f.html
[62] Déclaration du Sommet de Riga, 28 et 29 novembre 2006, consultable à l'adresse suivante : http://www.nato.int/docu/pr/2006/p06-150f.htm
[63] *Ibid*.

- L'OTAN a également effectué en 2006, un essai grandeur nature de nouvelles technologies pour le renseignement. Plus de 2000 hommes des forces aériennes, navales et terrestres se sont retrouvés en Grèce du 2 au 16 novembre pour participer à cet exercice nommé *Trial Spartan Hammer* (une première série d'essais avait eu lieu en avril 2005) faisant de ce dernier « *le plus important essai interarmées de l'histoire de l'Alliance mené dans le domaine du renseignement d'origine électromagnétique et des mesures de soutien électronique* »[64]. Il a permis de tester avec succès de nouvelles méthodes en matière de renseignement pour lutter contre le terrorisme.

- Dans ce même secteur du renseignement électronique, l'OTAN a créé un *Groupe de travail sur le renseignement d'origine électromagnétique et les mesures de soutien électroniques*. Composé d'experts et représentants de l'industrie ainsi que de personnels de l'OTAN chargés des opérations, il fut d'ailleurs chargé de l'organisation du *Trial Spartan Hammer* de 2006.

- Enfin, l'Alliance a lancé en 2008, la construction de six centres de coordination et d'échange du renseignement. Le premier d'entre eux : le centre anti-terroriste Pakistan-Afghanistan-OTAN a été inauguré à Turkham à la frontière afghano-pakistanaise.

L'OTAN s'est engagée dans l'action anti-terroriste de façon assez « tardive » par rapport à des organisations comme l'ONU ou l'Union Européenne (voir le point 3 ci après) mais elle a développé très rapidement - surtout après le 11 septembre 2001 - de réelles capacités opérationnelles pour lutter contre le terrorisme.

Son rôle en matière de renseignement a suivi la même évolution et la création de l'IFC laisse supposer qu'il deviendra de plus en plus important.

3) L'approche de l'Union Européenne (UE).

L'un des principaux enseignements du 11 septembre est donc la défaillance du renseignement. Les services américains n'ont pas su clairement appréhender une menace pourtant réelle en raison d'une communication déficiente tant en interne qu'en externe, puisque les informations apportées par leurs homologues européens n'ont pas pu ou su être analysées correctement.

Cependant, les informations transmises par ces derniers sont demeurées bien floues et disparates. Il est bien évidemment plus aisé de faire ce genre de constat et de tirer des conclusions après coup, mais toujours est-il que c'est l'ensemble du réseau mondial du renseignement qui a montré ses limites en n'ayant pas pu anticiper, et encore moins empêcher cette opération.

[64] *Grèce : essai d'une nouvelle technologie OTAN pour le renseignement*, consultable : http://www.nato.int/docu/update/2006/11-novembre/f1102c.htm

Les attentats furent d'ailleurs en grande partie planifiée en Europe (Allemagne, Italie, Espagne, Belgique), l'échec est donc aussi celui des européens.

Après ces évènements, les Etats de l'Union vont repenser et véritablement intensifier leur politique de coopération en matière de renseignement.

Cet effort s'est produit essentiellement, à deux « niveaux » :

- Au niveau de l'Union Européenne, via ses institutions, systèmes, entités, etc.,
- Au niveau bilatéral ou multilatéral, c'est-à-dire lorsque deux ou plusieurs Etats décident de mener une politique commune et spécifique, détachée des institutions ou entités de l'Union. Ce type de collaboration peut se faire entre pays européens, mais aussi avec des pays extérieurs (en premier lieu avec les Etats-Unis).

a) Les initiatives du renseignement au niveau de l'Union.

- **Les entités pour l'échange d'informations :**

Dès les années 70, des commissariats communs dans les zones frontalières nommés « *Centre de coopération policière et douanière (CCPD)* » furent créés.

Les groupes *TREVI (Terrorisme, Radicalisme, Extrémisme et Violence Internationale* vérifier*),* ou le « *Club de Berne* »[65] répondaient également à un besoin de coopération interétatique pour le renseignement.

Cependant les échanges restaient soumis au bon vouloir de chaque Etat de transmettre, ou non, les informations en sa possession.

Aussi les choses ont été remaniées après le 11 septembre 2001 et davantage encore après les attentats de Madrid en 2004 qui frappèrent directement le sol européen.

- **Le Coordinateur de la lutte anti-terroriste.**

En mars 2004, Gijs de Vries (ancien homme politique néerlandais) est devenu le premier *Coordinateur antiterroriste de l'Union Européenne*. Sous la direction du *Haut représentant de l'Union Européenne* Javier Solana, il travaille à la rationalisation, à l'organisation et à la coordination de la lutte contre le terrorisme, en attachant une attention particulière à l'échange de renseignement entre Etats membres.

[65] Créée en 1968, cette structure informelle réunie les chefs des services de sécurité intérieure de 20 pays de l'Union (plus la Suisse et la Norvège) pour échanger de l'information dans les domaines du contre-espionnage, de la criminalité organisée et du terrorisme.

- **Le « *Club de Berne* »**.

Il fut réagencé et a constitué le « *Groupe anti-terroriste (GAT)* », qui réunit les responsables des unités anti-terroristes des pays de l'Union, ainsi que des experts spécialisés sur le renseignement lié au terrorisme islamiste et aux réseaux Al-Qaïda.

- **Le groupe *TREVI (Terrorisme, Radicalisme, Extrémisme et Violence Internationale).***

Il œuvre principalement pour la lutte contre le terrorisme mais aussi contre la criminalité organisée et le trafic de stupéfiants. Il est constitué de six groupes d'experts qui travaillent sur des thèmes particuliers et qui tentent d'organiser les échanges de renseignements et d'harmoniser les législations européennes[66].

- **La *cellule d'analyse de la menace terroriste* au sein du *centre de situation (SITCEN)*.**

Créée après les attentats de Madrid en 2004, elle fut placée sous l'autorité du Secrétaire Général du *Conseil Européen* et du Haut Représentant pour la *Politique Etrangère de Sécurité Commune (PESC).* Elle tente d'élaborer une perception commune de la menace terroriste à partir des ressources fournies par les services de renseignement, les militaires, les diplomates et les services de police des pays de l'Union.

- ***L'Etat Major de L'Union Européenne* (EMUE).**

Après 2001, il s'est doté d'une division « renseignement » consacrée à l'évaluation de la situation, à la veille stratégique et, plus généralement à l'échange de renseignement. Elle est composée d'une trentaine d'experts issus de chaque pays membre de l'Union, qui sont en relation permanente avec leur service national de renseignement.

A ces entités spécialisées, on peut ajouter d'autres outils, cellules, moyens, etc., non spécifiques au renseignement dans la lutte contre le terrorisme, mais qui y participent directement ou indirectement d'une façon plus ou moins prononcée. C'est d'ailleurs tout le sens d'une série de mesures adoptées le 20 septembre 2001, par le *Conseil Justice et affaire intérieurs de l'Union* (JAI) dont l'un des chapitre s'intitulait : « *coopération policière/services*

[66] *Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil*, Commission de défense, M. Lemoine (rapporteur), Juin 2002, 25p.

de renseignements », pour renforcer la coopération entre ces deux types d'entités. Un certain nombre d'initiatives vont donc suivre cette voie :

- ***Europol* : L'office européen de police.**

Constitué le 26 juillet 1995, il avait pour objectif initial d'établir une meilleure coopération entre les services compétents des Etats membres dans le domaine de la lutte contre le terrorisme, mais aussi du trafic de drogue et de la traite d'êtres humains (il a remplacé le groupe *TREVI*). Mais jusqu'à 2001, il se chargeait presque uniquement des bases de données sur les personnes suspectées, données alimentées par les différentes « unités nationales » de l'office.

De plus, ses responsabilités opérationnelles étaient inexistantes et ses membres très peu nombreux pour un organisme avec une telle vocation (350 membres tous services confondus).

C'est pourquoi le *Conseil Européen* a entériné après le 11 septembre, l'augmentation significative des moyens humains et matériels à sa disposition. De plus, sa dimension opérationnelle put enfin prendre forme avec la constitution d'équipes d'enquêtes communes ainsi que la mise en place d'une cellule réunissant les directeurs européens au siège d'*Europol* à partir de décembre 2001.

- **Les équipes d'enquêtes communes.**

Instaurées le 29 juin 2000 par la convention sur l'entraide pénale (permettant la création d'équipes d'enquête commune entre les Etats de l'Union Européenne) ces équipes n'ont réellement vu le jour et fonctionné qu'après le 11 septembre.

Si là encore, l'initiative va au-delà du simple renseignement, et même de la lutte anti-terroriste, elles peuvent cependant œuvrer de façon efficace dans ce domaine et permettre un meilleur échange d'information.

- ***Eurojust* : l'Office Européen de Justice.**

Il a suivi une évolution similaire à celle des équipes d'enquêtes communes. En place à partir de 1999, il ne devient opérationnel que le 28 février 2002. Sa mission première est de faciliter, soutenir et coordonner les enquêtes pénales transfrontalières. Il est constitué de procureurs, de magistrats et d'officiers de polices. Sa compétence n'est pas spécifiquement centrée sur le terrorisme et le renseignement mais s'étend à l'ensemble de la criminalité transnationale organisée.

- **La « *Task Force* » des directeurs de polices.**

La *Counter Terrorism Task Force* a été créée en 2000 (mais n'est devenue effective qu'en 2001). Elle contribue à une amélioration de la transmission du renseignement, en favorisant les échanges d'informations entre les Etats membres et organes du contre-terrorisme et en tenant un fichier « anti-terroriste » regroupant les analyses dans ce domaine.

- **Le *Système d'Information Schengen (SIS)*.**

Il s'agit d'un système de coopération policière via la mise en commun de bases de données informatiques. Il permet l'échange d'informations entre les services de polices des Etats membres, concernant des biens et des personnes pouvant menacer l'ordre public (le SIS s'intéresse donc aux terroristes et réseaux terroristes). Il est censé compenser l'arrêt des contrôles aux frontières au sein de l'espace Schengen.

Précisons pour finir qu'un certain nombre d'autres groupes ou de forums d'échanges existent mais ne sont pas connus du grand public.

Mais la coopération au sein de l'Union Européenne ne repose pas uniquement sur des entités ou des groupes d'échange de l'information, elle se fait également au niveau « technique » pour la collecte de cette dernière :

- **Les systèmes « techniques » de collecte :**

- Le Programme européen *MUSIS (Multiuser Satellite Imagery System)*, est supposé lancer en 2009, toute une série de nouveaux capteurs spatiaux de nature à augmenter les capacités de renseignement d'origine image dans le cadre de la lutte anti-terroriste.

- La station satellitaire à Torrejon en Espagne permet l'interprétation d'images spatiales au profit du *Centre de situation* et de *l'Etat Major de l'Union Européenne*. C'est la *division Renseignemen*t de l'EMUE qui est en charge d'orienter les recherches du Centre.

- L'Union a également mis à niveau ses capacités en imagerie aérienne via les contributions des armées de ses pays membres (surtout la France et la Grande-Bretagne) en aéronefs et drones.

- Idem pour les interceptions électromagnétiques, l'Union dispose de capacités uniquement à partir des contributions nationales (mais ici, il est davantage question de construction européenne, de souveraineté nationale, de volonté de

constitution d'une Europe politique etc., que de renseignement spécifiquement). Soulignons tout de même le lancement en 2004 de la constellation de quatre satellites « *Essaim* » spécialisée dans l'interception des signaux électro magnétiques.

- **La coopération avec l'« international » :**

  Après le 11 septembre, la préoccupation principale de l'Union Européenne est de développer une stratégie globale de sécurité portant non seulement sur son territoire, mais aussi à l'extérieur, stratégie dans laquelle la collecte et l'analyse du renseignement tiennent une place centrale.

  Immédiatement après les attentats, un souhait intense de rapprochement et de renforcement de la coopération transatlantique émerge. Georges W Bush exprime très rapidement l'urgence pour les européens de déclarer immédiatement quarante priorités contre le terrorisme. Une session extraordinaire des Etats membres le 21 septembre et une réunion anticipée du *Conseil Européen* le 8 octobre, produisent un florilège de mesures anti-terroristes, notamment sur la sécurité aérienne civile.

  - Le 30 août 2002, *Europol* ouvre dans les locaux de la *Commission Européenne* un bureau de liaison à Washington dans lequel plusieurs officiers dits « de liaison » travaillent à la simplification des échanges d'informations avec les agences de sécurité et de renseignement américaines. Cette collaboration est renforcée par un accord complémentaire le 20 décembre 2002. *Eurojust* suit le même schéma avec l'élaboration de plans de travail avec les Etats-Unis.

  - Le 23 avril 2004, un accord portant sur la sécurité des informations classifiées (dans le cadre de la lutte contre le terrorisme) était signé entre les Etats-Unis et l'Union Européenne.

  - La collaboration UE/OTAN revêt un caractère particulier. En effet, l'OTAN n'est pas un fournisseur de renseignement, ou du moins pas directement. Comme nous l'avons vu précédemment, elle dispose de capacités dans ce domaine mais seulement grâce aux contributions de ses Etats membres, parmi lesquels plusieurs pays européens. Malgré tout, la collaboration spécifique Alliance Atlantique/Union Européenne est assez peu développée. On peut remarquer toutefois qu'après 2001, l'OTAN a autorisé l'Union Européenne à accéder à son réseau informatisé d'informations confidentielles nommée : le *BICES (Battlefield Information Collection and Exploitation System).*

  - Des collaborations existent entre l'UE et l'UEO (*Union de l'Europe Occidentale*), notamment sur la transmission de renseignement par réseau informatique.

Nous venons donc de voir que l'Union Européenne dispose de divers outils, systèmes, entités, etc., pour la collecte et l'échange du renseignement dans le cadre de la lutte contre le terrorisme.

Cependant, il ne faut pas sous estimer les échanges bi ou multilatéraux des pays membres entre eux, mais aussi avec l'extérieur, qui ne s'inscrivent donc pas dans le cadre des institutions ou entités de l'Union Européenne. Cette forme de coopération « en dehors » de l'Union est en effet très importante.

b) Les initiatives du renseignement au niveau « bilatéral » et « multilatéral » (en dehors du cadre de l'UE).

Les Etats européens développent ainsi des partenariats détachés du cadre de l'Union, la plupart du temps parce qu'ils entendent préserver leur souveraineté nationale qu'ils considèrent menacée au sein des instances européennes. Les coopérations bi ou multilatérales « parallèles » leur donnent plus de liberté, plus de souplesse pour prendre les décisions qu'ils jugent appropriées. Mais des éléments historiques ou de proximité géographique peuvent également justifier qu'il en soit ainsi.

- C'est le cas par exemple avec la coopération anti-terroriste entre l'Espagne et la France notamment à propos d'ETA. Le service espagnol qui conduit les enquêtes sur le territoire (qu'il s'agisse de terrorisme, de délinquance, de trafic de drogue, etc.) - le CGI (Centre Général d'Informations) - dispose aussi d'une cellule de renseignement extérieur qui surveille les groupes et réseaux terroristes en dehors des frontières nationales et collabore avec les services français particulièrement en ce qui concerne l'organisation séparatiste basque, dont les activistes se trouvent des deux côtés des Pyrénées.

- La coopération Espagne/Maroc s'est largement intensifiée après les attentats de Madrid en 2004. En effet les deux pays sont géographiquement très proches, les relations historiques entre eux sont anciennes, une importante communauté marocaine est installée en Espagne, mais surtout la plupart des terroristes des attentats de Madrid étaient marocains...de quoi faire de l'Espagne une cible de choix. La coopération entre les services anti-terroristes et de renseignement de ces deux Etats est donc indispensable et les services de renseignements espagnols ont ainsi renforcé leurs effectifs d'agents au Maroc. Mais cela va même plus loin, car selon certains

observateurs « *les principales unités de contre-espionnage ibériques ont été d'ailleurs formées pour travailler spécialement sur le Maroc* »[67].

- Mais globalement, de nombreux pays européens ont engagé des partenariats spécifiques avec des services anti-terroristes et de renseignement des pays du Maghreb ou pays à forte majorité musulmane. D'une part, le caractère aujourd'hui transnational du terrorisme fait qu'il est nécessaire de lutter contre le phénomène à l'extérieur des frontières nationales. Si les pays européens (mais c'est valable partout dans le monde) veulent se prémunir des attentats, ils ne peuvent se contenter de le faire uniquement au sein de leur propre territoire. D'autre part, développer des partenariats avec ces services étrangers permet de contourner la quasi impossibilité d'infiltrer les réseaux lorsque l'on est un agent d'un service occidental. De plus, et au-delà même de cette difficulté « physique » d'infiltration, les services des pays concernés sont les plus à même de lutter efficacement contre le terrorisme, dans un environnement, une société dans lesquels ils sont parfaitement adaptés, ancrés (ou du moins qu'ils connaissent mieux que leurs homologues européens).

  On citera par exemple :

  - La coopération France-Algérie qui passe par l'échange d'informations sur les activités des groupes terroristes, ainsi que par la mise en commun de techniques et des équipements utiles dans la traque des terroristes.

  - La conférence des ministres de l'Intérieur de la Méditerranée occidentale (France, Espagne, Tunisie, Algérie, Maroc) qui depuis sa création en 1982, travaille à lutter contre le fondamentalisme islamique et le crime organisé.

  - Les coopérations pour un meilleur échange du renseignement ont également été très largement renforcées après le 11 septembre, entre les pays européens eux-mêmes, mais aussi avec l'étranger (en dehors des pays à majorité musulmane dont nous venons de parler). Ainsi, de nombreux services de renseignement européens ont entériné des partenariats spécifiques avec leurs homologues américains, sous forme de détachement, d'échange de renseignements, etc.

  - La France abrite depuis 2002 une cellule commune d'agents des services secrets issus d'agences de renseignement américaines, canadiennes, australiennes, anglaises, et françaises. Nommée « *Alliance Base* », elle a pour mission de combattre l'islamisme radical : « *c'est un dispositif opérationnel d'échanges et de*

[67] *Renseignement : L'Espagne met le paquet sur le Maroc*, 12 décembre 2006 :

http://www.spyworld-actu.com/spip.php?article3220

mise en commun d'un certain nombre d'éléments, qui permettent d'améliorer l'efficacité des services qui y participent »[68].

- Un partenariat spécifique existe entre la DGSE et la CIA. Outre l'échange de renseignement, des agents des deux agences sont détachés spécialement au sein des locaux de l'autre entité.

Enfin les capacités de collecte du renseignement donnent aussi lieu à des partenariats technologiques (bien que la lutte antiterroriste ne soit pas forcément la motivation première dans l'élaboration de tous ces programmes) :

- Avec la station franco-allemande d'écoute, installée à Kourou en Guyane.
- Français, Espagnols et Italiens ont développé le projet de satellites d'observations *Hélios 1* (premier lancement en 1995), qui fournit des images de très haute résolution dans le domaine visible, mais aussi en infra rouge et dont le budget conséquent s'élève à plus d'un milliard et demi d'euros. L'exploitation des images recueillies est bien évidemment commune et la composante « sol » du système repose sur plusieurs centres : à Creil et Colmar pour la France, à Patricia di Mare (aux environs de Rome) et Lecce pour l'Italie, et à Torrejon (près de Madrid) et Maspalomas pour l'Espagne. En 2004, fut lancé le programme Hélios 2 améliorant les capacités de son prédécesseur.
- D'autres programmes d'échanges d'images existent également entre les trois pays précédemment cités : comme le système spatial *SAR-Lupe* mis en service en 2007 pour l'Allemagne, le programme *Ishtar* pour l'Espagne et *Cosmo-Skymed* qui devrait être opérationnel en 2009 pour l'Italie. Cependant, la coopération est ici moins « intégrée » qu'elle ne l'était dans le cadre du programme Hélios 1, car il ne s'agit que d'échanges d'images et non d'une véritable mise en commun des moyens.

Après avoir étudié les évolutions impulsées au sein du renseignement depuis 2001 aux Etats-Unis, à l'ONU et à l'OTAN, intéressons nous maintenant à la réponse française.

[68] Christophe Chaboud (UCLAT), tiré d'Eric Lecluyse, *Antiterrorisme : "Alliance base" existe bien,* L'express avec Reuters, 12 septembre 2006 : http://www.lexpress.fr/actualite/politique/alliance-base-existe-bien_460124.html

III) La réponse française.

1) Présentation générale de la « communauté française » du renseignement.

En France, le renseignement dans le cadre de la lutte contre le terrorisme s'organise comme dans tous les pays du monde, autour de services ou agences civils et/ou militaires dont les compétences sont censées se compléter, s'imbriquer pour assurer la sécurité et la défense du territoire. Plusieurs services œuvrent donc dans le renseignement français[69] :

a) Les services spécialisés.

- Les services du Ministère de la Défense :

  - La **DGSE (*Direction Générale de la Sécurité Extérieure*)** : Dans l'imaginaire collectif français, il s'agit du service de renseignement par excellence, au même titre que la CIA aux Etats-Unis. Elle est en charge de la collecte et de l'exploitation du renseignement à l'extérieur du territoire national, et utilise des moyens tant humains que techniques. Mais elle remplit également de façon non officielle des missions « actions » à l'étranger.

  - La **DPSD (*Direction de la Protection et de la Sécurité de la Défense*)** : Elle assure la protection et la sécurité des personnels, informations, matériels, et installations sensibles dépendant du Ministère de la Défense. C'est un organisme de surveillance.

  - La **DRM (*Direction du Renseignement Militaire*)** : Equivalent de la DIA aux Etats-Unis, cet organisme interarmées collecte, analyse puis diffuse les renseignement d'intérêt militaire à l'ensemble des forces armées françaises.

- Les services du Ministère de l'Intérieur :

  - La **DST (*Direction de la Surveillance du Territoire*)** : Elle était avec la DGSE l'autre « grand » service de renseignement. Chargée historiquement du contre-espionnage sur le territoire français, elle se consacrait largement depuis plusieurs années à la lutte anti-terroriste. Cette structure particulièrement discrète était l'un des rares services au monde à disposer d'une capacité à la fois de police/renseignement et judiciaire. Elle pouvait donc suivre les enquêtes ou

[69] Sur l'organisation des services de renseignement en France, lire :

- Charlotte Lepri, *Quelle réforme pour quels services de renseignement ?*, IRIS, 2007, 13p.

dossiers d'un bout à l'autre de la procédure. Cependant, depuis le début de l'année 2008, la DST n'existe plus en tant que telle puisqu'elle a fusionné au sein d'une nouvelle direction qui a pris le nom de *Direction Centrale pour le Renseignement Intérieur* (DCRI)[70].

- La **DCRG ou « RG » (*Direction Centrale des Renseignement Généraux*)** : Tout comme la DST, elle a récemment disparu pour être à présent incorporée à la DCRI. Sa mission avait trait à la recherche des informations relatives à la sécurité intérieure, puis à leur transmission au gouvernement.

A ces quatre services, s'en ajoutent deux autres spécialisés :

- La **DNRED** (***Direction Nationale du Renseignement et des Enquêtes Douanières***) : Elle dépend du Ministère de l'Economie et bien que son rôle soit souvent minimisé, elle est très active dans la lutte contre la fraude financière et les trafics illicites qui peuvent procurer des fonds aux terroristes.
- **TRACFIN** ou ***cellule de Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins*** : Sous la tutelle des ministres de l'Economie, des Finances et de l'Emploi, c'est la cellule française de lutte anti-blanchiment. Mais elle a intégré dès l'origine le groupe *Egmont*. Créé en 1995, ce dernier fédère au niveau mondial des Cellules de Renseignement Financier (101 unités au 31 décembre 2006).

b) Les autres entités participant au renseignement.

Aux services spécialisés dans le renseignement, on pourra ajouter plusieurs entités qui certes ne sont pas des services de renseignement à proprement parler, mais qui y participent indirectement de par leurs activités et leurs attributions :

- La **DAS (*Direction aux affaires stratégiques*)** : Rattachée au Ministère de la Défense, elle ne dispose d'aucune capacité de collecte, mais en revanche elle élabore à partir des informations fournies par les services de renseignement (en grande partie) des analyses et notes à caractère politique, stratégique et prospectif à destination du Ministre de la Défense et d'un certain nombre de services Etatiques.

[70] Voir la réforme des services de renseignement français dans la suite de ce travail.

- La **SDAT (*Sous Direction Anti Terroriste*, ancienne *DNAT*) :** Ce service de police judiciaire dépendant du Ministère de l'Intérieur est comme son nom l'indique un organisme de lutte anti terroriste, mais qui produit du renseignement dans le cadre de ses activités.

- La ***Gendarmerie Nationale*** : Son rôle est souvent minimisé, à tort. Bien qu'elle ne soit pas spécialisée dans la lutte contre le terrorisme, sa mission de surveillance du territoire au quotidien, et surtout son organisation formant un véritable maillage font d'elle un pourvoyeur important de renseignement.

- La ***Police Judiciaire*** **(PJ)** : Sa contribution dans le renseignement provient des enquêtes qu'elle mène en rapport avec des affaires criminelles.

- Les ***Unités militaires spécialisées*** : Elle sont dépendantes soit de la Police (**RAID**), soit de la Gendarmerie (**GIGN**) ou des forces militaires de l'armée (regroupées depuis 92 auprès du *Commandement des opérations spéciales*).

Au total, la communauté française du renseignement emploie environ 16 000 personnes dont 4000 hommes spécifiquement pour le renseignement militaire et dispose d'un budget d'environ 800 millions d'euros par an.

Jusqu'à présent, le *Secrétariat Général à la Défense Nationale* servait d'agent de liaison interministériel entre les différentes entités françaises du renseignement, mais sa fonction était purement administrative, limitée à l'organisation des Comités et Conseils de Défense dont celui du CIR (*Conseil Interministériel sur le Renseignement*).

Nous verrons par la suite que certaines des décisions récentes et notamment la publication du nouveau Livre Blanc en 2008 vont modifier l'architecture de la communauté française du renseignement.

Mais avant arrêtons-nous sur les changements que celle-ci a connu après le 11 septembre.

2) Les initiatives de l'après 11 septembre 2001.

Nous avons vu que les évolutions dans le renseignement ont été rapides et assez « spectaculaires » du côté américain, tout de même assez significatives pour l'OTAN et l'Union Européenne, mais qu'en est-il pour la France ?

a) Les conclusions françaises concernant les attentats sont les mêmes que dans le reste du monde…mais n'engendrent aucun changements profonds dans le renseignement.

Les conclusions tirées des attentats du 11 septembre furent globalement les mêmes en France que dans le reste du monde. Dans un rapport d'avril 2006 du Ministère de la Défense[71], Michelle Alliot-Marie parlait en introduction de : « *L'évolution de la menace depuis les attentats du 11 septembre 2001* » en qualifiant cette dernière de « *plus en plus transnationale* » et liée au « *développement de zones instables dans le monde* ».

On prend conscience que le terrorisme est devenu transnational et que son développement en « franchise » et en réseaux le rend plus difficile à combattre…et ces constats ne diffèrent là en rien de ceux des américains, de l'Union Européenne, des Nations Unies ou de l'OTAN.

Nous ne détaillerons pas l'ensemble des initiatives anti-terroristes entreprises par la France dans ce domaine après 2001, mais préciserons néanmoins qu'à partir de cette nouvelle perception de la menace, elle décide de participer à l'élaboration d'une réponse « globale », « internationale », soudée et coordonnée avec tous les acteurs mondiaux. Il est procédé à un renforcement de la protection de sa population (notamment pour les ressortissants français à l'étranger), de son territoire et à une amélioration et une adaptation des plans de protection et de vigilance. Les armées et la gendarmerie sont amenées à réexaminer leur contribution dans cet « effort national ».

Mais aucune rupture avec la stratégie antérieure n'est à relever et la base structurelle de la lutte contre le terrorisme reste inchangée. Les cinq organes principaux (DST, RG, DNAT, DGSE, Gendarmerie) gardent une importance comparable.

Les différentes dispositions ou lois votées après le 11 septembre ne remettent pas en cause le socle édicté par la loi du 9 septembre 1986 (qui est la référence en matière de lutte anti-terroriste en France).

Les trois grands principes du contre-terrorisme français : « Prévenir, Protéger, Agir » perdurent, malgré des ajustements et nouveautés.

Et concernant le renseignement, nous pouvons dire dès à présent qu'il ne connaît pas de « révolution » majeure.

Il est plus que jamais confirmé comme un aspect essentiel de la prévention contre le terrorisme. Justifiées ou non, les critiques envers la trop grande place dédiée aux moyens « technologiques » de collecte du renseignement dans le monde anglo-saxon (avant le 11

[71] *La Défense contre le terrorisme : une priorité du ministère de la Défense*, Rapport du Ministère de la Défense, avril 2006, 48p.

septembre) encouragent la France à maintenir son système fondé sur l'équilibre entre le renseignement « technologique » et le renseignement « humain ».

Les services n'enregistrent donc pas d'avancées notables si ce n'est une augmentation de leurs crédits mais qui s'avère moins marquée que celle observée dans les pays d'importance et de puissance comparables. Sur ce plan, le différentiel existant avant le 11 septembre se confirme donc, au désavantage de la France :

- Au niveau des effectifs, les services français sont toujours à la traîne puisqu'ils comptent (hors renseignement militaire) 12 000 personnes, les services britanniques 14 000, les allemands presque 17 000. La communauté américaine emploie elle plus de 100 000 personnes, mais elle est « hors catégorie », et ce nombre est de toute façon en adéquation avec la puissance (économique, démographique, etc.) des Etats-Unis.
- Budgétairement, la France consacre annuellement entre 750 et 800 millions d'euros au renseignement contre plus de 3 milliards pour la Grande Bretagne, de plus la hausse est chez eux en moyenne de 10% par an depuis le 11 septembre, ce qui est loin d'être le cas en France.

Mais ces données quantitatives ne suffisent pas à appréhender l'état d'un système de défense – ni du renseignement - et en l'occurrence l'absence d'attentat terroriste majeur dans l'hexagone depuis 1996 témoigne très nettement en faveur de la qualité et de l'efficacité française.

Selon beaucoup de spécialistes, la France est en effet devenue au fil du temps la seule nation de l'Union Européenne à disposer d'une autonomie complète en matière de renseignement et la seule en mesure d'apporter, lorsque c'est nécessaire, des éclairages sur ceux fournis par les Etats-Unis[72].

Mais pour autant, la culture du renseignement y est quasiment inexistante tant auprès des instances dirigeantes que dans l'opinion publique. Alors que dans les pays anglo-saxons le renseignement est une activité honorable, son image de marque reste dans le notre très fortement connotée négativement : pour des raisons historiques, il est demeuré d'une part synonyme d'espionnage, de viol des libertés et de la vie privée et d'autre part, relativement exclu du processus de décision des politiques. Jusqu'ici le renseignement n'a jamais fait l'objet en France d'une réflexion ou d'une réorganisation de fond, ni même d'une attention particulière de nature à lui accorder les moyens nécessaires à son action et le reconnaître à sa juste valeur.

[72] Selon Eric Denécé dans : Le *renseignement français au milieu du gué*, Centre Français de Recherche sur le Renseignement (CF2R), décembre 2005. Disponible à l'adresse suivante : http://www.cf2r.org/fr/article/article-le-renseignement-francais-au-milieu-du-gue-1-2.php

Si le 11 septembre n'engendre pas dans un premier temps en France, de remise en cause profonde du renseignement comme ce fut le cas dans certains pays (notamment aux Etats-Unis), l'idée qu'il faut s'adapter en permanence aux nouvelles menaces présentes mais surtout futures va pousser les autorités à augmenter les budgets des services concernés. Ainsi entre 2001 et 2003, le budget de la DGSE a été augmenté de 9,9%, celui de la DPSD de 17,7%, celui de la DRM de 7,5%[73].

Cependant, ces chiffres doivent être relativisés car une hausse des budgets s'était déjà produite à la fin des années 90 : en 1999 le budget de la DGSE avait connu une hausse de 11,4%, celui de la DRM de 25% (surtout à cause de la guerre au Kosovo).

C'est seulement dans un second temps, que les autorités vont se lancer dans une vaste « réforme » de la communauté du renseignement. Les prémices ont lieu en 2006, avec le vote de la loi du 23 janvier relative à la lutte contre le terrorisme puis en 2007, avec celle du 9 octobre sur la création d'une délégation parlementaire pour le renseignement.

b) Les prémices d'une évolution, avec les lois du 23 janvier 2006 et du 9 octobre 2007.

- **Loi du 23 janvier 2006**[74] :

  Elle avait l'ambition d'adapter la lutte anti-terroriste aux impératifs posés par le « nouveau » terrorisme et les nouvelles menaces. Un certain nombre de directives concernent directement le renseignement. Plusieurs axes sont développés[75] :

  - **Améliorer la surveillance des communications électroniques** : la loi élabore une procédure administrative, contrôlée par une autorité indépendante, pour l'accès aux données de connexions auprès des opérateurs Internet (numéros d'abonnement ou de connexion d'une personne désignée, localisation des équipements utilisés, liste des numéros appelés et appelants, durée et date des communications).

  - **Autoriser l'accès des services de renseignement et de sécurité à certains fichiers administratifs « de droit commun »** : la consultation de certains fichiers administratifs détenus par le Ministère de l'Intérieur (immatriculations, cartes d'identité et passeports, permis de conduire, titres de transport et visas) devient possible pour les agents des services de renseignement. Auparavant et contrairement à la plupart de leurs homologues étrangers, ils n'avaient pas le droit

[73] *Ibid.* Eric Denécé op.cit p 79.
[74] *LOI n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, consultable à cette adresse : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124&dateTexte=
[75] A ce sujet voir : *La France face au terrorisme – Livre Blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La documentation française, 2006, 135p.

d'accéder à ces données alors que c'était là le seul moyen de vérifier certaines informations et d'identifier préventivement des jeunes recrues terroristes très souvent inconnues des services de police.

- **Mieux identifier les voyageurs dangereux** : elle modernise le « *Fichier National Transfrontière (FNT)* » relatif aux documents de voyage et visa, qui était devenu inefficace et obsolète. Cela permet aux services d'obtenir des informations sur les individus se rendant de façon régulière dans des régions du monde connues pour abriter des lieux de radicalisation, des camps d'entrainement terroristes, etc. Jusque là le FNT était alimenté seulement à partir des cartes d'embarquement et de débarquement remplies par les passagers, documents qui ne peuvent être systématiquement vérifiés dans le détail et qui n'ont qu'une valeur relative. La loi du 23 janvier permet, entre autre, d'alimenter automatiquement le fichier à partir de la lecture optique des documents. De plus, elle prévoit que les régimes de surveillance en place dans le transport aérien (le fichier PNR[76] notamment) puissent être généralisés aux déplacements ferroviaires et maritimes dès lors que les frontières de l'Europe sont franchies.

- **Loi du 9 octobre 2007**[77] :

A première vue, la promulgation d'une loi portant création d'une délégation parlementaire au renseignement paraît être bien loin des réalités du terrain et donc moins importante que des réformes relatives par exemple à l'augmentation des budgets des services de renseignement, ou à la refonte de la communauté.

Néanmoins, cette délégation constitue pour le renseignement un réel progrès et symbolise la nouvelle place accordée à cette activité dans le dispositif de défense et de sécurité, et en particulier dans le domaine anti-terroriste.

Elle met aussi fin à une singularité française puisque la France était le dernier pays, (excepté le Portugal), à ne pas s'être doté d'un tel organe parlementaire dédié au suivi et au contrôle des services de renseignement.

Elle n'avait pas non plus de juge spécialisé, de sorte que la seule forme d'encadrement s'effectuait uniquement par le vote des budgets par les différents Ministères et par l'action

[76] Les fichiers PNR ou *Passenger Name Record* sont, à l'origine, des informations commerciales déclarées par le voyageur au moment de la réservation. Ils peuvent contenir des données comme le numéro de carte bleue, le prix du billet, les références de passeport ou l'adresse à destination. Depuis le 11 septembre 2001, les Etats-Unis ont exigé d'accéder à ces fichiers pour les comparer avec leurs propres listes de suspects, puis pour établir des évaluations de risques dites « profilages ». Mais l'Union Européenne et la France se sont lancées depuis dans cette entreprise.

Source : http://mcsinfo.u-strasbg.fr/article.php?cPath=17_53&article_id=9296

[77] LOI *n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement*, consultable à cette adresse :

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000252177&dateTexte=

toute relative de l'*Inspection Générale de la Police Nationale* (IGPN). Mais l'Etat n'avait aucun moyen de s'assurer que les activités des services respectaient les orientations politiques décidées par le gouvernement, ou de connaître leurs moyens.

A titre d'exemple, il a fallu attendre 2004 pour que l'Assemblée Nationale puisse enfin avoir accès aux données concernant les effectifs exacts d'employés travaillant à la DST.

Pourtant le contrôle parlementaire du renseignement est absolument essentiel, et ce à plusieurs niveaux :

- Premièrement - et il s'agit sûrement du point le plus fondamental - il garantit le respect des principes démocratiques dans l'activité des services. C'est d'autant plus justifié et indispensable dans un domaine ou l'on se trouve parfois dans des « zones grises », aux limites de ce qu'un Etat démocratique peut accepter et tolérer.

Mais au-delà de cet aspect lié à la « surveillance », le contrôle parlementaire du renseignement permet :

- « *D'accroître l'importance du renseignement dans le processus de décision politique, à condition qu'il puisse s'exercer à l'abri des querelles politiciennes* »[78].

- D'améliorer le fonctionnement et l'efficacité générale de la communauté du renseignement, dès lors qu'il s'exerce de façon intelligente. Ainsi, cette délégation est destinée non seulement à éviter les dérives, à contrôler l'utilisation des budgets etc., mais aussi à instaurer de meilleures relations entre la représentation nationale et les services de renseignement. Il n'est ici pas inutile de rappeler qu'en France, les hommes politiques ont toujours montré une grande méfiance envers les services de renseignement. Comme le dit Pascal Junghans[79] dans un article de la revue *Sécurité Globale*[80] : « *L'efficacité d'un service de renseignement ne relève pas seulement de la bonne qualité de son système de production des données, mais aussi, sinon surtout, de la manière dont les décideurs politiques reçoivent et utilisent ces mêmes données* ». Cette délégation devrait donc être « *un lieu d'éducation des dirigeants politiques aux subtilités et aux nécessités du renseignement* »[81].

[78] *Ibid.* Jacques Baud Op.cit. p 27.
[79] Journaliste français, auteur de plusieurs ouvrages sur le renseignement.
[80] Pascal Junghans, *La nouvelle délégation parlementaire au renseignement va-terrorisme-elle améliorer l'efficacité des services ?*, Sécurité Globale, Eté 2008, 12p.
[81] *Ibid.*

- D'harmoniser et de mieux structurer l'organisation globale de la communauté. Il s'agira d'éviter ou de limiter « *l'éparpillement ou une répartition anarchique des compétences et un imbroglio hiérarchique* »[82].

- De mettre les services en face de leur responsabilité et par la même, de les responsabiliser puisqu'ils auront à rendre des comptes à une « entité supérieure ».

- De donner au renseignement une nouvelle légitimité aux yeux de nos concitoyens. Une plus grande « transparence » devrait revaloriser le rôle et l'image des services de renseignement au sein de la population et favoriser l'émergence d'une réelle culture du renseignement dans notre pays.

L'idée de créer cette délégation pour le renseignement est en fait déjà ancienne. En 1999, deux propositions de loi avaient été déposées, sans être inscrites à l'ordre du jour et ensuite, elle a reçu de nombreux et réguliers soutiens.

Mais il aura donc fallu attendre 2007 pour que les textes soient votés.

L'exposé des motifs de la loi mentionne que :

« Les services de renseignement de l'Etat contribuent à assurer la sécurité de nos concitoyens dans un contexte caractérisé par l'existence de nouvelles menaces. Les domaines particulièrement sensibles dans lesquels ils interviennent, qu'il s'agisse de la lutte contre le terrorisme, la prolifération des armes de destruction massive, le suivi des capacités militaires d'Etats étrangers ou l'anticipation des crises internationales, justifient pleinement le caractère secret de leur activité qui doit être préservé et protégé.

Cet impératif de discrétion doit cependant se concilier avec l'exigence d'une information du Parlement sur l'activité générale et les moyens des services spécialisés à laquelle doit répondre tout Etat démocratique.

Le présent projet de loi y pourvoit en créant au sein du Parlement une délégation pour le renseignement »[83].

L'importance du renseignement au regard des nouvelles menaces et notamment du terrorisme figure donc clairement dans la présentation de la loi. Pourtant, ce même constat était acquis et formulé dès 2001, et beaucoup d'autres pays n'ont d'ailleurs pas

[82] *Ibid.* Charlotte Lepri Op.cit. p 78.
[83] Exposé des motifs concernant le projet de loi portant création d'une délégation parlementaire au renseignement, consultable sur :

http://www.legifrance.gouv.fr/html/actualite/actualite_legislative/exp_delegation_parlementaire_renseignement.htm

attendu les attentats de New-York et Washington pour encadrer le renseignement : le contrôle parlementaire existe en Italie depuis 1977 et au Royaume-Uni depuis 1994.

Mais en France, la mise en place d'un tel système s'était jusque là toujours heurtée aux réticences liées notamment à l'association entre « renseignement » et « action ». En effet, selon Jacques Baud : « *En France, où le renseignement est très rapidement associé à l'« action », le rôle d'une surveillance est considéré comme un obstacle au renseignement* »[84]. En revanche « *la culture politique anglo-saxonne – marquée par un consensus sur le respect des institutions sécuritaires – est mieux armée pour mettre en place des mécanismes de surveillance des services de renseignement* »[85].

Le pas est désormais franchi et la délégation parlementaire mise en place. Ses six membres (trois parlementaires et trois sénateurs) sont astreints au secret Défense. S'ils reçoivent des informations sur le budget, l'activité générale et l'organisation des services de renseignement, s'ils peuvent également auditionner les Ministres de tutelle de ces mêmes services ainsi que leurs directeurs, en revanche les informations à leur disposition « *ne peuvent ni porter sur les activités opérationnelles de ces services, les instructions données par les pouvoirs publics à cet égard et le financement de ces activités, ni sur les échanges avec des services étrangers ou avec des organismes internationaux compétent dans le domaines du renseignement* »[86].

Ils pourront avoir accès aux informations classifiées, sauf celles concernant « *des données dont la communication pourrait mettre en péril l'anonymat, la sécurité ou la vie d'une personne relevant ou non des services intéressés, ainsi que les modes opératoires propre à l'acquisition du renseignement* »[87].

Ces deux lois du 23 janvier 2006 et du 9 octobre 2007 n'impulsent aucune « révolution » ni dans le renseignement ni dans la lutte anti-terroriste.

Elles peuvent toutefois être considérées comme représentatives de la période de l'après 11 septembre en France, pour deux raisons principales :

- Le renseignement est véritablement perçu, et de plus en plus, comme un élément clé du dispositif de lutte contre le terrorisme.
- Cependant, bien que faisant l'objet « d'améliorations », de « renforcements », aucune mesure réellement novatrice n'est à relever. Le contrôle parlementaire du renseignement est certes un point positif, mais d'une portée relative, dans la mesure où la France n'a fait que rattraper un « retard » par rapport aux autres pays. On peut parler ici davantage d'une « remise à niveau » que d'une véritable « révolution ».

[84] *Ibid.* Jacques Baud Op.cit. p 27.
[85] *Ibid.*
[86] *Ibid.* Pascal Junghans Op.cit. p 85.
[87] *Ibid.*

De plus, en dehors de ces deux lois, le gouvernement publiait en 2006 un *Livre Blanc sur la Sécurité Intérieure face au Terrorisme* fixant les axes et priorités de la réponse française à la menace terrorisme. A ce titre, il rappelait que le renseignement était la première clé du dispositif de lutte contre le terrorisme, tant en matière d'anticipation que d'analyse et de compréhension du phénomène terroriste, d'où le besoin constant de renforcer les capacité des services de renseignement et de sécurité et d'assurer la coordination de ces derniers. Pour autant aucune décision d'envergure n'était à retenir

Mais l'arrivée au pouvoir de Nicolas Sarkozy au printemps 2007 va accélérer grandement les choses. En effet, comme nous venons de le dire, si la période 2001/2007 n'est marquée par aucune avancée fondamentale dans le renseignement - en dépit d'améliorations certaines - 2008, avec la création de la Direction *Centrale du Renseignement Intérieure* (DCRI), et surtout la publication du nouveau *Livre Blanc sur la Sécurité et la Défense,* semblent poser de nouvelles bases.

3) Les nouveautés impulsées par le Livre Blanc 2008.

Le *Livre Blanc sur la Défense et la Sécurité Nationale* a été publié au printemps 2008 et fait suite au dernier en date, publié en 1994.

Par son intermédiaire, le renseignement devient véritablement le cœur des nouvelles orientations stratégiques de la France pour les 10 ou 15 années à venir. En effet, pour la première fois la fonction « *connaissance et anticipation* » (à laquelle le renseignement participe largement) est érigée au rang de fonction stratégique majeure pour le pays. Le renseignement devient le pivot de la défense et de la sécurité nationale.

Concrètement, le Livre Blanc comporte des décisions qui devraient modifier significativement la pratique du renseignement et que l'on peut classer en deux catégories :

- Evolutions au niveau de l'organisation et de la coordination.
- Evolutions au niveau des ressources humaines et des moyens.

a) L'organisation et la coordination.

Le Livre Blanc entérine la *Direction Centrale du Renseignement Intérieur* (DCRI) (mais ce n'est pas une création directe de ce dernier). Voulue par Nicolas Sarkozy, elle est issue de la fusion des *Renseignements Généraux (RG*) et de la *Direction de la Sûreté du Territoire (DST)*. Elle a pris ses quartiers au début de l'année 2008 dans le « Pole de Levallois-Perret ». Cette nouvelle structure est constituée de 5000 fonctionnaires de police et divisée en quatre sections principales dévolues à : la protection des institutions, au contre-espionnage, à la surveillance des mouvements sociaux et faits de société et enfin à la lutte anti-terroriste qui occupera la part la plus importante de l'activité de la *DCRI*.
Dans les dernières décennies, la *DST* et les *RG* se sont imposés comme les deux grands piliers du renseignement en France et de la lutte contre le terrorisme.

En réunissant la *DST* et les *RG*, les bénéfices affichés et attendus sont multiples :

- Tout d'abord la présence d'un seul (grand) interlocuteur dédié au renseignement intérieur devrait permettre une amélioration du traitement des informations et de la fluidité de l'échange de ces dernières, que ce soit au niveau national ou international.
  Le « dialogue » avec nos partenaires étrangers devrait être clarifié par la présence désormais de cette nouvelle entité dominante. De plus, avec la DCRI nous nous alignons sur le mode de fonctionnement de la plupart de nos homologues (Allemagne, Grande-Bretagne, Etats-Unis…) qui privilégient tous un seul grand organisme de renseignement intérieur (même si d'autres entités comme la Gendarmerie en France, y participent également).
  Dans le même temps, la frontière avec la *Direction Générale pour la Sécurité Extérieure (DGSE)* sera également bien mieux définie qu'elle ne l'est actuellement. La *DST* empiète trop souvent, selon certains, sur l'extérieur et donc sur les prérogatives de la *DGSE*. La hiérarchie des services de renseignement français devrait donc se simplifier.

- Les chevauchements et redondances entre la *DST* et les *RG*, concernant notamment les informations utiles à l'anti-terrorisme seront de fait supprimés. L'objectif est d'assurer une « *communication sans faille entre tous les acteurs* » d'après les propres mots de la Ministre de l'Intérieur.

- Il est également de pouvoir concilier le savoir faire « local » des *Renseignements Généraux* à travers son système de maillage du territoire très serré et la dimension centrale de la *DST*. Et c'est dans cet esprit que l'on parle officiellement d'une « mise en commun des moyens » plutôt que d'une véritable « fusion » au sens premier du terme. Conserver les spécificités des deux sections sera vraisemblablement l'un des facteurs majeurs de réussite ou de faillite du projet.

- La présence d'un directeur unique devrait permettre également une prise de décision (notamment sur le plan « opérationnel ») plus rapide et harmonisée.

- Enfin, l'attrait de cette fusion tient également à des aspects plus pragmatiques relevant d'une logique économique notamment pour la partie logistique. En effet, la mise en commun des moyens, qu'il s'agisse de l'informatisation, des locaux, ou même du parc automobile permettra de réaliser des économies non négligeables sur tous les frais de fonctionnement.

En dehors de la DCRI qui n'est donc qu'un « regroupement » optimisé de services, on retrouve toujours l'organisation classique que nous avons précédemment décrite.

En revanche, la coordination globale de la communauté de renseignement est redéfinie. C'était l'une des faiblesses majeures en France. En effet, malgré l'existence d'un plan de renseignement gouvernemental et d'un *Comité Interministériel du Renseignement (CIR)*, aucune stratégie claire au niveau national n'instaurait jusque là une véritable « communauté française du renseignement » qui serait concertée et coordonnée.
De plus, l'absence d'une stratégie « nationale » du renseignement avait empêché les différents acteurs du secteur de s'adapter correctement entre eux aux nouvelles menaces, de telle sorte qu'il existait parfois (et il en est encore ainsi aujourd'hui) un chevauchement entre les attributions et les prérogatives des différents organismes.

C'est pourquoi le Livre Blanc crée plusieurs initiatives pour tenter d'y remédier, et plus généralement pour permettre une plus grande fluidité dans la circulation des renseignements au sein de la communauté[88] :

- Le ***Conseil National du Renseignement*** **(CNR)** : cette nouvelle entité sera le cœur de la communauté française du renseignement et aura pour mission de fixer les grandes orientations du renseignement (stratégies, priorités), de répartir les objectifs et de rendre ses arbitrages juridiques si nécessaire. Présidé par le Président de la République, il sera en mesure de réunir à tout moment, une assemblée constituée par :

  - Le Premier ministre ;

  - Les représentants des ministères de l'Intérieur, de la Défense, des Affaires Etrangères, de l'Economie et du Budget, et le cas échéant, d'autres ministères selon les sujets abordés ;

  - Les directeurs de tous les services de renseignement ;

[88] Voir : Défense *et Sécurité nationale – Le libre blanc*, Odile Jacob, 2008, 350p.

- Le *Coordonateur National du Renseignement*.

- Le ***Coordonateur National du Renseignement*** : placé sous l'autorité directe du Président de la République, il sera chargé grâce à une structure d'appuis légère, de préparer les décisions du CNR et d'en suivre l'exécution. Il sera l'interlocuteur majeur pour les services de renseignement et servira de relais entre ces derniers et le Président de la République. De plus, il présidera des séances périodiques réunissant les directeurs des services ainsi que le cabinet du Premier ministre, pour hiérarchiser les priorités de recherche.

On peut distinguer ici très clairement une organisation similaire à celle existante aux Etats-Unis avec *Director of National Intelligence* (DNI), sorte de grand ordonnateur de la communauté du renseignement américaine, qui exerce sa mission sous l'autorité directe du Président, et qui est épaulé dans sa tâche par l'*Office of the Director of National Intelligence*.

- Le SGDN ne disparaît pas pour autant, puisqu'il supportera l'action du coordonateur du renseignement et animera des groupes de travail sur des sujets définis en fonction des priorités posées par le CNR.

- La Délégation Parlementaire au renseignement dont nous venons de parler, était déjà en place avant le Livre Blanc de 2008, mais elle viendra parfaitement s'insérer dans ce système et sera chargée de l'information relative aux activités des services.

- Un nouveau dispositif législatif relatif aux activités et missions des services de renseignement, mais aussi à la protection du secret de la défense nationale ainsi qu'à celle des personnels, sera élaboré.

b) Ressources humaines et moyens techniques.

C'est le second « grand chantier » du Livre Blanc en matière de renseignement. Il devrait permettre premièrement à ce dernier de devenir le pilier des nouvelles orientations stratégiques françaises en matière de sécurité et de défense, et deuxièmement, d'opérer une remise à niveau des services français par rapport à leurs homologues étrangers.
La réputation de la France en matière de renseignement a toujours été - du moins celle qui ressort de ces dernières années - de « faire bien mais avec peu de moyens ».

En effet, quantitativement les moyens des services de renseignement français sont tant sur le plan technique qu'humain, inférieurs à ceux de puissances comparables, telles que la Grande-Bretagne ou l'Allemagne (voir chiffres donnés précédemment**)**.

Le Livre Blanc s'attache donc à rehausser :

- Les **ressources humaines** : même si la France a semble-t-il toujours respecté un équilibre entre les moyens de collectes humains et les moyens de collectes techniques, l'effort concernant les ressources humaines correspond bien aux leçons tirées après le 11 septembre. C'est-à-dire que le renseignement repose d'abord et avant tout sur des hommes et des femmes qui le recueillent mais qui surtout l'exploitent et l'analysent. Développer les capacités techniques de collecte est indispensable, mais c'est inutile si la capacité humaine d'analyse ne suit pas ensuite.
  De plus, les personnels du renseignement sont amenés à exercer leur mission dans des conditions souvent dangereuses.

  Pour toutes ces raisons, le Livre Blanc 2008 porte une attention toute particulière sur :

  - Le **recrutement** : le niveau des effectifs sera tout d'abord renforcé et en premier lieu dans le cadre de la lutte anti-terroriste. Cette augmentation concernera à la fois les personnels dévolus à la collecte du renseignement sur le terrain, mais aussi les personnels « techniques », c'est-à-dire les techniciens, ingénieurs, linguistes, interprètes-images, spécialistes en programmation informatique, etc.

  - La **formation** : une académie du renseignement devrait voir le jour, et proposera une formation de haut niveau (sanctionnée par un Brevet) planifiée et hébergée par les services. Mais d'autres filières spécialisées dans cette activité devraient se créer. L'objectif est à terme de pouvoir favoriser un recrutement plus ouvert, à partir d'universités, de grandes écoles, de contractuels, etc.

- Les **moyens techniques** : les ambitions dans ce domaine visent les 15 ans à venir. Le Livre Blanc, document officiel généralement caractérisé par une « neutralité » et une « réserve » prononcée, fait lui-même le constat d'une déficience des moyens technologiques de renseignement français. Il est ainsi mentionné :

  « *Les évolutions technologiques rapides justifient l'accroissement de nos moyens techniques pour mieux assurer la sécurité du pays. Un saut qualitatif et quantitatif est d'autant plus nécessaire que nous devons conserver un bon niveau pour pouvoir dialoguer avec les quelques pays qui sont nos interlocuteurs majeurs, présent et à venir, dans le domaine du renseignement.*
  Or les moyens de ces pays connaissent un fort accroissement de puis 2001, ***dont nos services n'ont pas bénéficié à la même échelle*** »[89].

[89] *Défense et Sécurité nationale – Le libre blanc*, Odile Jacob, 2008, 350p.

C’est pourquoi des efforts seront portés tout particulièrement sur :

- Le renseignement spécialisé sur le réseau Internet, déjà intensifié par les dispositions de la loi du 23 janvier 2006, verra ses capacités encore accrues.

- Le domaine spatial qui est absolument indispensable pour l’autonomie stratégique d’un Etat, mais qui est tout aussi nécessaire au renseignement dans le cadre de la lutte anti-terroriste, sera l’objet d’un effort significatif. La France dont les besoins dans ce domaine sont couverts - en partie - par le programme *Hélios* collaborera davantage avec ses partenaires dans le cadre des systèmes spatiaux *SAR-Lupe* (avec l’Allemagne), *Cosmo-Skymed* (avec l’Italie), ou *MUSIS* (Europe).

- Le domaine aéroporté devrait voir ses capacités d’acquisition augmentées via les aéronefs, les systèmes embarqués sur les avions de combat mais aussi les drones avec pour ces derniers le système MALE (moyenne altitude longue endurance) qui entrera en service au cours de la prochaine décennie.

- Le renseignement d’origine électromagnétique sera de fait favorisé et sa composante spatiale amplifiée par le programme européen CERES (*capacité européenne de renseignement électromagnétique spatiale*) qui sera opérationnel au cours des années à venir. Les moyens terrestres (en premier lieu les détachements avancés de transmissions) et navals (bâtiments d’écoute et sous-marins nucléaires d’attaques) seront également consolidés.

Le Livre Blanc de 2008 sur la Défense et la Sécurité Nationale prépare ainsi un certain nombre d’évolutions ayant trait à la fois à l’organisation et surtout à la coordination entre les services (création du CNR et du poste de coordonateur notamment), mais aussi à une réelle augmentation des moyens, qu’ils soient humains ou techniques.

Nous tenterons de voir dans le Chapitre 3, si ces annonces politiques sont crédibles et susceptibles d’instaurer des changements profonds au sein de la communauté française du renseignement, notamment dans le cadre de la lutte anti-terroriste.

Conclusion Chapitre 2 :

Précisons que ce Chapitre 2 a eu pour but de montrer les types de « réponses » ou les évolutions du renseignement dans le cadre de la lutte anti-terroriste depuis le 11 septembre 2001, d'une façon descriptive, objective et neutre.

Nous avons souhaité donner une image la plus fidèle possible à partir des exemples des Etats-Unis, de l'Union Européenne, des Nations Unies, de l'Alliance Atlantique et de la France, car ils sont chacun, à leur niveau et à leur échelle, des acteurs majeurs et incontournables de la lutte contre le terrorisme dans le monde, et des entités au sein desquelles le renseignement joue et jouera un grand rôle.

D'une manière générale, les changements intervenus dans le monde du renseignement depuis les attentats de New-York et Washington se sont organisés en tout premier lieu autour du constat selon lequel les menaces et notamment le terrorisme, avait pris de nouvelles « formes », une nouvelle « dimension ». Ils ont été entrepris non seulement après des réflexions, des études, des rapports, etc., sur les défaillances du renseignement - et spécifiquement son incapacité à anticiper et empêcher le 11 septembre - mais surtout à partir de considérations plus globales relatives aux impératifs du contexte post-Guerre Froide en matière de sécurité et de défense.

Les Etats Unis ont effectué un remaniement à grande échelle (surtout par le biais du *Homeland Security* et du *Patriot Act*) de leur stratégie de défense et de sécurité, dont le renseignement est l'un des pivots.

L'ONU a marqué l'idée que le renseignement devait devenir le cœur de la lutte contre le terrorisme, mais à ce jour, le renseignement n'a pas fait l'objet de dispositions concrètes particulières.

L'OTAN s'est, quant à elle, montrée bien plus active puisque la place du renseignement a été considérablement renforcée au sein de l'organisation ainsi que dans les actions militaires contre terroristes qu'elle mène sur le terrain.

L'Union Européenne a, elle aussi, revu et rehaussé ses moyens du renseignement, mais très souvent par le biais d'entités, d'organes ou de dispositifs etc., déjà existants.

Enfin, la France même si elle ne l'a pas fondamentalement bousculé, a redéfini - plus tardivement que les autres - son système de renseignement. La création de la DCRI, les lois du 26 janvier 2006 et du 9 octobre 2007, puis les nouveautés apportées par le Livre Blanc en 2008 (notamment la création du CNR et du Coordonateur du Renseignement, les efforts concernant les moyens humains et techniques de collecte, etc.) représentent des évolutions certaines.

Introduction Chapitre 3 :

Le 11 septembre 2001 a donc eu des conséquences non négligeables sur les stratégies contre-terroristes dans le monde et en particulier sur la place qu'y occupe le renseignement.

Des lois ont été votées, des plans entérinés, certaines mesures renforcées et d'autres redéfinies, des coopérations envisagées puis mises en place, des services et agences ont été réformés, réorientés, etc.

Aujourd'hui, en 2008, sept années après les attentats, il semble possible et opportun de dresser un premier bilan, avec le recul nécessaire. Au-delà des discours et des annonces politiques, au-delà des descriptions officielles et des objectifs affichés, qu'a réellement changé le 11 septembre dans le domaine du renseignement ?

Les décisions prises et mises en œuvre dans la foulée ont souvent été qualifiées de novatrices mais l'étaient elles vraiment ? Se sont-elles révélées efficaces ? En d'autres termes, quelles conclusions peut-on tirer ?

Ces interrogations seront le fil conducteur de ce dernier chapitre, avant d'aborder, pour terminer, les perspectives pour le renseignement dans les années à venir. Il s'agira d'apporter une vision plus « globale » sur le futur du renseignement appliqué à la lutte anti-terroriste en tentant de répondre aux questions suivantes :

Quelles sont les voies envisagées et envisageables pour en améliorer l'efficacité ?

Quels dangers, présents ou à venir faudra-t-il éviter ?

Chapitre 3 : Bilan, et perspectives futures pour le renseignement.

I) Bilan de la refonte de la communauté américaine de renseignement.

1) Les initiatives sécuritaires.

À première vue, les initiatives concernant la lutte contre le terrorisme et plus généralement la sécurité à l'intérieur du territoire américain semblent colossales.

L'élaboration du *Patriot Act* et plus encore celle du *Department of Homeland Security* apparaissent, à elles seules, comme une véritable « révolution » de la pratique du contre-terrorisme aux Etats-Unis. Aux 40 milliards de dollars alloués en 2002 au seul DHS sont venus s'ajouter par exemple : 150 milliards de rallonges en 2003 pour la sécurité intérieure. Et depuis cette même année, le Pentagone fonctionne avec 378 milliards de dollars de budget annuel, soit plus d'un par jour.

Bien que centré sur l'aspect « sécuritaire » en général, le renseignement fait partie intégrante de ces initiatives, et on pouvait donc s'attendre, aux Etat-Unis, à de réelles améliorations dans ce domaine. Mais quel est le bilan sept ans après leurs mises en place ?

a) Homeland Security :

Comme le disait Olivier Palluault en décembre 2005[90] : « *ce ministère [le DHS] ne reflète qu'une réforme institutionnelle et le signal d'une accélération des capacités budgétaires et matérielles de l'anti-terrorisme. De même sa structure organisationnelle ne repose que sur l'agrégation d'agences ayant quitté leurs ministères d'affectation et les missions du DHS ne sont que la somme de missions préexistantes auparavant effectuées par d'autres administrations* ». Et il énonce la principale critique envers ce « *Département* », à savoir : l'inexistence d'une capacité opérationnelle propre.

En effet, s'il coordonne les initiatives entre les différents acteurs du système, donne une impulsion générale et facilite l'échange des renseignements ce qui est certes (déjà) important, il est complètement dépendant des différentes agences et de leur bonne collaboration. L'absence de capacité de collecte de l'information limite de fait son apport car les dissensions entre les agences de renseignements sont toujours bien présentes, ce qui nuit au partage optimal du renseignement.

[90] Olivier Palluault, *Le 11 septembre 2001, une rupture dans la pratique de l'anti-terrorisme*, Technologie et Armement, Octobre 2005.

De plus, on peut constater que l'« élan » post 11 septembre qui a permis et accompagné sa construction émanait en réalité de décisions et de dynamiques antérieures.

Dès le début de l'année 2001, des parlementaires américains avaient appelé à la constitution d'un outil similaire au *Department of Homeland Security*, car selon eux, le coordinateur national intégré au *National Security Council* depuis 1995 ne bénéficiait pas d'une autorité suffisante et s'appliquant directement sur les agences de renseignement et de sécurité.

De même, l'augmentation de budget allouée à ces dernières et affectée à leur activité de contre terrorisme est antérieure au 11 septembre, même s'il est indéniable que cette date marque une réelle explosion en la matière : par exemple, celui de la section anti-terroriste du FBI enregistra un bond de 280 % entre 1995 et 2000 et son effectif passa de 550 à 1400 personnes compétentes au cours de cette période.

Quant au budget national du contre-terrorisme de 5.7 milliards de dollars en 1996, il atteignait les 12 milliards au début de l'année 2001 (il est vrai cependant que le budget de la communauté du renseignement n'avait pas connu d'augmentation jusqu'à 2001, après la baisse du milieu des années 90).

A cette époque, les autorités américaines étaient déjà convaincues de la nécessité de protéger le territoire, notamment par une amélioration des capacités et de l'échange du renseignement.

Quoi qu'il en soit, bien qu'en gestation depuis une décennie, le « *Homeland Security* » n'a vu le jour et ne s'est rapidement mis en place qu'après les attentats, dans l'état d'urgence et l'onde de choc (émotionnelle et politique) qu'ils ont suscités. A défaut de disposer d'une capacité opérationnelle en tant que telle, et au-delà des réticences toujours présentes, cette entité permet désormais la collaboration concrète, entre les différentes agences de renseignements américaines qui n'avaient jusque là pas ou peu l'habitude de travailler ensemble. En mesurer les effets de façon réelle, exhaustive et spécifique s'avère difficile puisque ce *Département* est une partie indissociable d'un système plus global, mais force est de reconnaître qu'aucun acte terroriste ne s'est déroulé aux Etats-Unis depuis 2001 et que par conséquent, l'objectif initial et essentiel est respecté.

Néanmoins, derrière cet apparent succès de la refonte « administrative » et « institutionnelle » - la plus importante depuis la création de la CIA et du « *National Security Council* » en 1947 - se cachent des constats et des résultats plus nuancés.

Le pilotage de l'ensemble est intrinsèquement une tâche ardue et intimement liée à l'effort consenti par chacun des organismes participants.

On estime qu'environ 56 agences et administrations américaines participent à la lutte contre le terrorisme (services de police, services d'immigration, douanes, etc.), et 16 sont spécialement dévolues au renseignement. Des autorités locales ainsi que le secteur privé y participent parfois activement.

Cette imbrication architecturale comporte un autre handicap : la très grande diversité des activités rassemblées au sein d'une unique entité.

Le trop large spectre de sa mission de sécurité intérieure a valu au DHS de fréquentes réserves ou désapprobations. Avant même sa mise en place, un rapport de la « *Brooking Institution* » de juillet 2002 concluait qu'il « *fusionne trop d'activités, dont plusieurs ont peu de rapport entre elles, dans un seul Département* ».

Ses auteurs abordaient aussi l'opportunité de différencier la gestion des situations d'urgence des opérations courantes liées à la sécurité (celle des frontières, des transports et des infrastructures) ou au renseignement (sa collecte et son exploitation) et jugeaient que les deux domaines se devaient de rester distincts et autonomes, au moins dans un premier temps.

De plus, la question de la pertinence d'instaurer le *Homeland Security Council* tout en maintenant le *National Security Council* s'est assez rapidement fait entendre.

En schématisant, ils rassemblent tous deux autour du Président un certain nombre d'experts chargés de prendre des décisions en matière de sécurité intérieure, notamment coordonner l'action des différentes agences. Leurs champs d'action sont connexes et les objectifs sont comparables. Cette similitude tant de structures, de moyens que d'attributions a soulevé et soulève encore des interrogations et elle n'est pas sans incidence ou problème sur le terrain.

Comme nous l'avons dit, le *Homeland Security* fut créé avec l'intention louable de devenir l'entité de base, de référence du système. Mais pour ce qui est du renseignement, à quelle entité les agences doivent-elles se référer ? Au NSC ? Au *Homeland Security Council* ? Ou bien au *Director of National Intelligence* (DNI)?

On voit bien à travers cet exemple, que le DHS a davantage compliqué les choses qu'il ne les a simplifiées.

Dans la pratique, les services secrets sont demeurés sous l'autorité du NSC (le DNI intervenant lui essentiellement au niveau du renseignement seul). Le simple renforcement des prérogatives de ce dernier n'aurait-il pas été plus judicieux après le 11 septembre ? Si l'argument se défend au plan strictement fonctionnel et utilitaire, il paraît clair que le besoin de sécurité exprimé par le peuple américain a prévalu dans la décision : le gouvernement a opté pour un choix immédiatement visible et psychologiquement fort en termes d'annonces.

De même, la légitimité législative du *Department of Homeland Security* est inexistante car il a été promulgué par décret, contrairement au *National Security Council* crée par un acte du Congrès et dont la nomination des membres est soumise à l'approbation du Sénat, tout comme ses activités sont soumises à des contrôles parlementaires réguliers. Le DHS manque d'une assise légale et donc d'autorité ce qui se ressent sur l'ensemble de son activité, et sur le renseignement en particulier.

Le bilan du DHS dans ce domaine est donc très mitigé.

b) Le *Patriot Act*.

Il a instauré une plus grande liberté aux agences fédérales de sécurité, et aux agences de renseignements dans le cadre de la lutte contre-terroriste décrétée après les attentats. C'est

ainsi qu'elles ont disposé de nouveaux pouvoirs en matière de renseignement, de détention de suspects, de surveillance des communications, de contrôle aux frontières, etc.

Cependant, les organisations de défense des droits de l'homme et plus généralement des millions d'américains jugent cette loi contraire aux principes de la démocratie et de la liberté des citoyens (voir pour plus d'informations la Partie IV de ce chapitre). Au lendemain du 11 septembre, elle a pourtant été adoptée sans trop de difficultés par le Congrès alors que le rapport de force entre Démocrates et Républicains n'augurait pourtant pas d'un combat aisé pour ces derniers qui disposaient d'une courte majorité. Mais le choc du 11 septembre a mis fin provisoirement aux oppositions sénatoriales entre les deux parties et a rassemblé tout le monde autour du président et des initiatives de la Maison-Blanche.

En retrait de ce consensus politique, les organisations de défense des droits de l'homme se montrent actives dès le départ et appellent à la vigilance et à la résistance.

Parmi elles, l'*American Civil Liberty Union* (ACLU) affirme que : « *les libertés civiles et la sécurité n'ont pas à être mises en conflit* » et que le pays possède déjà tout un corpus de textes et de mesures anti-terroristes dont il convient de revoir simplement l'application et non le contenu.

En d'autres termes, l'effort doit consister à réduire le manque de coordination et non pas les libertés, à renforcer la collecte et le traitement de l'information et non pas la répression policière.

La liste des attributions et des prérogatives précédemment énoncées peut objectivement mener à des dérives. La diminution des droits de la défense, la violation de la vie privée, l'atteinte du droit à la liberté d'expression et l'absence d'un véritable contrôle parlementaire, sont les points critiques qui font débat aux Etats-Unis et plus de 360 villes et comtés ont d'ailleurs déclaré refuser d'appliquer cette loi.

Beaucoup se demandent si la lutte contre le terrorisme vaut que l'on réduise les libertés individuelles, que l'on entrave les droits de l'homme et du citoyen, que l'on altère des valeurs démocratiques.

A long terme, le *Patriot Act* pourrait se révéler contre-productif.

Mais surtout au-delà de ces aspects éthiques, son utilité réelle dans le cadre de la collecte du renseignement puis de son exploitation pour lutter contre le terrorisme, est contestée (comme les plans d'écoutes des communications de la CIA et de la NSA).

Certes, il a directement permis l'arrestation puis la condamnation de plus de 200 personnes impliquées dans le terrorisme.

Et c'est au total près de 450 personnes qui ont été inculpées aux Etats-Unis en six années de lutte.

Mais par rapport aux effets négatifs engendrés (notamment une frustration - voire davantage - de toute une frange de la population, la frange Musulmane, et la « mauvaise » publicité à

l'étranger), on peut se demander si le *Patriot Act* est d'un apport bénéfique pour la lutte contre le terrorisme.

Concernant les autres initiatives « sécuritaires », telles que la biométrie incorporée dans les passeports, les différentes initiatives de contrôle et de sécurité du transport aérien, le renforcement de la cyber-surveillance, et plus globalement toutes les mesures pour la sécurité « globale », on se trouve dans une configuration similaire à celle du *Patriot Act*.

En effet, beaucoup de ces mesures s'imposaient, la majorité d'entre elles améliorent le niveau de sécurité générale et représentent autant d'obstacles supplémentaires pour des terroristes qui voudraient perpétrer une action.

Mais encore une fois, certaines d'entre elles posent également des questions relatives au respect des libertés publiques et à l'équilibre au sein d'une société entre le besoin de sécurité et respects des droits fondamentaux des personnes. C'est particulièrement valable pour les nouvelles mesures ayant trait aux enquêtes « informatiques » ou de cyber-surveillances (notamment de la finance internationale) et les législations en œuvre dans ce domaine qui se sont durcis depuis le 11 septembre.

La traque des terroristes bien évidemment voulue par l'ensemble de la population doit-elle être cependant une justification pour la mise en place de systèmes, règles, législations susceptibles de réduire l'espace de liberté ?

Il s'agit de question que nous aborderons spécifiquement dans la suite de ce travail.

2) Bilan de la refonte des agences : des progrès, mais encore insuffisants.

a) Le FBI.

Le 11 septembre a engagé le *Federal Bureau of Investigation (FBI)* dans une profonde restructuration même s'il convient de préciser qu'il avait entrepris avant, certaines transformations ou améliorations. L'augmentation de ses fonds, ainsi que la hausse des effectifs spécialisés dans tous les aspects du contre-terrorisme (financement et cyber terrorisme surtout), en sont des signes majeurs. Mais le glissement de sa mission première représente encore la plus grande évolution : depuis 2001, l'agence n'est plus exclusivement chargée de l'application de la loi et de la répression des actes criminels, elle se doit d'œuvrer pour la sécurité nationale et la prévention des actes terroristes. Le FBI a du se restructurer en interne et se doter de réelles capacités de collecte et d'analyse du renseignement. Rappelons rapidement les évolutions majeures :

- Création d'une division anti-terroriste spécifique doté de près de 1500 employés, et laissant une large place au renseignement.

- Recrutement de centaines d'hommes de terrain pour la collecte.
- Mise en place de systèmes de communications standardisés en interne, mais aussi en externe avec les autres agences américaines.
- Création de divers groupes de travail tels que le : *Joint Terrorisme Task Forces (JTFS),* le *National Joint Terrorisme Task Force (National JTTF)* ou le *Foreign Terrorist Tracking Task Force (FTTTF),* ou le *National Counterterrorism Center (NCTC),* pour obtenir un meilleur renseignement et de faciliter son échange.
- Les sections antiterroristes et contre-espionnage du FBI sont passées sous la supervision du directeur national du renseignement, tandis que la lutte contre le crime «ordinaire» reste sous la tutelle du département de la Justice.
- Environ 60% du personnel a été réaffecté à la lutte contre le terrorisme et le nombre d'analystes a été multiplié par quatre.
- Cinquante-six «cellules de renseignements» (*Field Intelligence Groups*) ont été créées à travers le pays.
- Pour éviter l'éparpillement, toutes les enquêtes concernant des menaces d'attentats sont dirigées depuis le quartier général de Washington.

Mais si les moyens financiers du contre-terrorisme et du renseignement ont été considérablement renforcés depuis 2001, ces deux activités ne représentent qu'entre 400 et 600 millions de dollars, c'est-à-dire moins de 10% du budget annuel total du FBI (soit entre 7 et 9 milliards de dollars).

Ainsi, le FBI reste prioritairement un organisme de surveillance et de répression de la criminalité « ordinaire » même s'il devient de plus en plus, du fait de son implication croissante dans la lutte contre le terrorisme, un instrument de la politique étrangère américaine.

En Mai 2008, un rapport de la *Commission du Renseignement* du Sénat mettait en lumière les insuffisances du FBI en matière de lutte contre le terrorisme et de renseignement et pointait les aspects suivants :

- Le déploiement d'agents et d'analystes de terrain engagés après le 11 septembre n'a pas été à la hauteur des attentes par manque de formation et d'encadrement.
- Les *Field Intelligence Groups* manquent cruellement de moyens et leurs demandes passent souvent après les autres priorités du FBI.
- Au quartier général de l'agence, 20% des postes de la section en charge des activités d'Al-Qaïda seraient vacants.

- Le FBI ne dispose toujours pas d'un réel programme de formation pour les analystes du renseignement.
- Beaucoup de ces analystes sont supervisés par des agents spéciaux qui ont peu, ou pas du tout d'expérience dans ce domaine.
- Malgré les progrès « techniques » réalisés depuis 2001, seulement 1/3 des agents et analystes de renseignement ont un accès Internet depuis leur bureau. Et plus généralement, les capacités techniques des connexions ne permettent pas aux employés de télécharger les images, vidéos et documents audio parfois nécessaires aux investigations.

De plus, même si une volonté de meilleure coordination organisationnelle a vu le jour entre les agences compétentes de la sécurité nationale, des obstacles d'ordre technique, antérieurs au 11 septembre, sont toujours d'actualité. La mise en commun des bases de données, la standardisation des procédures, les règles de classifications, etc., sont toujours des problèmes récurrents. La mise en place de la *Foreign Terrorist Track List* (coordination entre le FBI, le Service d'Immigration et Services de Douanes) ou de l'*Office of Intelligence* du FBI (pour l'amélioration des capacités d'analyses, de partage, de rassemblement de l'information concernant la sécurité nationale) sont une voie d'amélioration mais pas encore une solution.

Au vu de ces différents éléments, le rapport de la Commission du Sénat sur le renseignement recommandait que l'*Office of the Director of National Intelligence* (ODNI) soit chargé de rédiger un rapport semi annuel au Congrès pour l'informer des progrès du FBI dans le cadre de ses programmes liés à la sécurité nationale et au renseignement. Elle souhaitait en outre qu'un calendrier précis soit mis en place pour combler au plus vite les lacunes constatées.

On mesure ici l'écart qui peut exister entre les discours officiels, les annonces politiques, et la réalité sur le terrain, même lorsque la volonté de changement est avérée, ce qui semble être le cas ici.

Mais réformer une bureaucratie telle que le FBI requiert, outre les conséquentes enveloppes budgétaires, du temps, notamment pour changer des mentalités issues de décennies d'un fonctionnement quasi autarcique dans lequel la préservation des intérêts domine non seulement en interne mais aussi en externe, face à la concurrence des autres agences.

Pour une administration de cette dimension, il n'est ni aisé ni instantané de s'adapter à la redéfinition de son cœur de métier et plus encore de modifier sa culture.

Mais de façon globale, les progrès impulsés au sein du FBI depuis 2001, pour en faire une agence leader dans la lutte anti-terroriste et dans le renseignement, sont réels, même s'ils sont encore très insuffisants. C'est pourquoi certains spécialistes émettent l'idée qu'il faudrait démembrer le FBI et créer une véritable agence de contre-espionnage indépendante, sur le modèle du MI 5 britannique ou de l'ancienne DST française.

b) La CIA.

Les problèmes de la *Central Investigation Agency (CIA)* sont relativement les mêmes que ceux du FBI. Elle aussi a considérablement intensifié sa force de lutte contre le terrorisme, par l'augmentation des budgets, l'arrivée massive de nouveau personnel et la réorientation globale de sa mission. Elle ne se contente plus de son rôle « traditionnel » d'agence d'analyse et d'exécution mais s'intègre à l'effort de défense du territoire, participe à des missions de planification et de surveillance des opérations militaires extérieures et agit clandestinement dans les milieux terroristes. Plus généralement, elle se concentre sur l'élimination des réseaux notamment via l'espionnage des flux bancaires. Désavouée pour son incapacité à prévoir les attaques et sommée de parvenir à un partage absolu et complémentaire des idées et des capacités, la CIA s'accommode de ses nouvelles prérogatives mais avec lenteur.

Après le 11 septembre, elle a établi des centres de coopération dans plus d'une vingtaine de pays.

Mais la médiatisation de ses programmes de surveillance de la finance internationale ou de ses méthodes de détention et d'interrogatoire de suspects bannies par le droit international, a engendré d'importantes critiques sur le plan international. La période de l'après 11 septembre n'aura en tout cas pas marqué une amélioration de l'image de cette agence.

De surcroît, elle est victime d'un déficit structurel de cadres expérimentés d'âge moyen, du fait de son évolution au « second plan » au cours d'une longue période précédant le 11 septembre. Après cette date, elle a largement incorporé de jeunes recrues disposant de solides connaissances en informatique et en langues étrangères (40% des effectifs « post 11 septembre »). Mais il existe un déficit important entre cette « nouvelle » génération et l'« ancienne » (20% des effectifs) composée de membres qui partiront à la retraite dans les toutes prochaines années. La pyramide de l'âge et de l'ancienneté du personnel démontre un besoin évident en agents et analystes exercés. Cette carence à la fois qualitative et quantitative en expérience et en savoir-faire, d'ores et déjà très sensible, s'annonce encore plus préjudiciable à l'avenir.

c) La NSA.

La *National Security Agency (NSA)* est au cœur d'un vaste programme de contrôle des réseaux et communications électroniques américains, mais aussi étrangers, puisque l'administration a encouragé les compagnies nationales de télécommunications à attirer le trafic international vers leurs commutateurs. Ainsi un pourcentage élevé d'appels téléphoniques qui ne concernent pas les Etats-Unis (ni par l'émetteur ni par la destination finale) transitent tout de même par eux.

Comme nous le savons, la NSA est la plus importante des agences de renseignement des Etats-Unis. Pendant la Guerre Froide, elle était chargée d'intercepter les communications et messages de l'« ennemi » communiste et plus généralement tous les renseignements jugés

« vitaux » pour la défense et la sécurité nationale. Après la chute du mur, ses prérogatives sont devenues plus floues et ont secrètement dérivé vers l'interception d'informations ne concernant plus seulement la sécurité et la défense, mais aussi des secteurs relatifs à l'intelligence économique.

Depuis 2001, ses missions principales se sont intensifiées dans le cadre de la lutte contre le terrorisme, le plus souvent à l'encontre ou à la limite du 4ème amendement de la constitution relatif aux libertés individuelles.

Son objectif affiché dépasse la « simple » écoute et vise à utiliser les données pour analyser les relations sociales des individus et déterminer ainsi leur implication dans des cellules terroristes.

Mais un vif débat a pris place outre-Atlantique, depuis la divulgation de toute la portée de ce programme tenu secret par l'administration en raison, selon elle, de son rôle considérable pour la sécurité du territoire, pour la lutte contre le terrorisme et encore plus directement dans le démantèlement du réseau Al-Qaïda. D'un côté, les instigateurs et responsables de ce projet affirment que les données enregistrées, stockées et analysées dans ce cadre restent cantonnées exclusivement à cette tâche et démentent toute possibilité de dérives. D'un autre côté, ses détracteurs, emmenés par les organisations de défense des droits civiques, de plus en plus nombreuses et influentes aux Etats-Unis, pointent le manque de contrôle et de transparence de cette gigantesque entreprise.

Fin 2005, le *New York Times* dévoilait que la NSA intercepte les communications entre les Etats-Unis et l'étranger à partir d'une suspicion de liens ou d'appartenance à Al-Qaïda et sans mandat d'un juge. Elle détermine seule les numéros et les adresses Internet à observer sans qu'aucune autorisation ne lui soit nécessaire ou imposée.

En mai 2006, le *USA Today* révélait qu'elle collecte des dizaines de millions de relevés téléphoniques de citoyens américains « ordinaires » et d'entreprises.

Si la détection des comportements suspects et plus globalement la chasse aux terroristes sont officiellement les raisons avancées pour justifier cette surveillance domestique organisée et à grande échelle, nul doute que les écoutes ont dépassé et dépassent de simples listes de présumés ou potentiels terroristes. Une telle masse d'informations pourrait inciter à une exploitation « sauvage », à des fins commerciales par exemple pour tracer des profils de consommations et trouver par ailleurs d'autres applications progouvernementales.

Concernant son efficacité, nous ne pouvons assurément pas la cerner du fait de l'extraordinaire flou qui entoure tant les méthodes que les prérogatives de cette démarche aux allures d'espionnage.

Dans un souci d'évaluation strictement utilitaire et s'agissant du repérage et de l'anéantissement de diverses structures (qu'elles soient terroristes ou qu'elles aient trait à la criminalité organisée ou au grand banditisme), nous émettrons l'hypothèse que ces programmes ont un intérêt certain mais cependant restreint puisqu'elles font preuve d'une extrême précaution, en limitant au maximum leurs communications par des moyens

« technologiques » et en revenant à l'utilisation de moyens de communications « basiques », délaissés ou sous-estimés depuis des années par les services de renseignements occidentaux.

Ainsi, Ben Laden n'est il toujours pas en liberté ? Cependant il faut tout de même préciser sur cette question spécifique, que de plus en plus de spécialistes émettent l'hypothèse que Ben Laden est tout à fait localisé par les américains, mais n'est pas arrêté pour des raisons politiques.

Mais au-delà de l'activité réelle, supposée ou fantasmée de telles entreprises, des questions plus générales, plus symboliques voire même philosophiques se posent. La lutte contre le terrorisme, même après le traumatisme du 11 septembre, vaut-elle que l'on remette en cause les règles fondamentales des démocraties, que l'on tende vers la réduction des libertés individuelles et tout simplement que l'on en fasse trop ? Jusqu'où un gouvernement peut-il aller pour assurer la sécurité de sa population qui par ailleurs en est demandeuse ? Ces interrogations trouvent un lien direct avec la question du *Patriot Act* et seront abordées dans la Partie IV de ce travail.

Mais plus globalement, et malgré tous les efforts liés notamment à un meilleure partage de l'information, à une simplification et une harmonisation des procédures inter-agences, etc. les relations restent assez difficiles, notamment entre le FBI et la CIA. Il est indéniable que depuis le 11 septembre, de nombreux progrès ont été effectués et les différences tendent à s'aplanir, mais structurellement et culturellement parlant, les deux services poursuivent des logiques opposées et parfois difficilement compatibles.

De plus et en rappelant une nouvelle fois les progrès effectués ces dernières années, les communications entre les agences (et même à l'intérieur de ces agences) sont obsolètes. Les ordinateurs sont présents en trop faibles quantités, ne sont bien souvent pas reliés à Internet et disposent d'une mémoire insuffisante. Il existe plusieurs dizaines de réseaux de mails, qui ne sont pas compatibles entre eux et rendent donc la communication entre les agences par ce biais, quasi inopérante.

3) Bilan de la mise en place du DNI, du 500 Day Plan et des initiatives relatives à la coopération internationale.

a) DNI et le *500 Day Plan* : des avancées à confirmer.

Longtemps souhaitée mais jamais concrétisée, la création d'un poste de Directeur de la communauté nationale du renseignement américaine (ou DNI) voyait le jour en 2004 avec l'acte de réforme sur le renseignement et la prévention des actes terroristes ou « *Intelligence Reform and Terrorism Prevention Act (IRTPA)* ».

Chargé de coordonner les activités des agences de renseignement, il publiait en 2007 avec l'aide de l'ODNI (*Office of Director of National Intelligence*) les *100 et 500 Day Plans*, documents qui devaient lancer des mesures effectives pour bâtir cette coopération renforcée au sein du renseignement.

Si un bilan du *500 Day Plan* est encore prématuré puisque l'essentiel des mesures n'ont pas été encore traduites dans la réalité, ou qu'elles le sont mais depuis trop peu de temps, nous pouvons en revanche parler du DNI - en fonction depuis 4 ans - en nous référant au témoignage et à l'avis fournis par Mr Tim Roemer[91] devant le *Sous-comité de Gestion de la Communauté du renseignement* du 7 décembre 2007[92] :

Selon cet homme d'expérience, le DNI a permis ou favorisé un certain nombre de progrès significatifs dans le domaine du renseignement américain, qui remplissent les principaux objectifs assignés à sa fonction. Cependant, bien que les débuts soient encourageants, il convient de noter que ces avancées devront être pérennisées et renforcées dans le temps et que l'action reste donc insuffisante pour le moment. En analysant l'intervention de Roemer on distingue :

⇨ **Les progrès avérés :**

- Un des points positifs tient au fait que tous les agents ou officiers du renseignement qui cherchent à atteindre des postes hauts placés dans la communauté, doivent obligatoirement effectuer une expérience dans un autre service de renseignement pour être promus. Ces « rotations » visent à ce que ces futurs « dirigeants » aient une idée de la communauté dans son ensemble, et non pas une vision fragmentée.

- Les relations entre le DNI et le *Département de la Défense* se sont améliorées de façon significative. Pendant des décennies, 85% du budget de la communauté du

[91] Président du *Centre de Politique Nationale* (CNP), ex membre du *Comité Permanent sur le Renseignement*, ex membre de la *Commission d'enquête sur les attentats du 11 septembre* ayant soutenu la création du DNI.

[92] *The Director of National Intelligence's 500 Day Plan - Testimony of the Honorable Tim Roemer before the Subcommittee on Intelligence Community Management*, 6 Décembre 2007, consultable sur : http://www.cnponline.org/ht/display/ContentDetails/i/2418

renseignement relevait du *Département de la Défense*, et était donc en dehors du contrôle du Directeur de la CIA, alors chargé de coordonner le renseignement américain. Cette nouvelle coopération peut être considérée comme de bon augure pour assurer le développement d'une communauté unifiée.

⇨ **Les progrès à confirmer…ou à « surveiller » :**

- La commission sur les attentats du 11 septembre qui a recommandé la création d'un Directeur National du Renseignement avait estimé les effectifs de l'ODNI à « plusieurs centaines » mais sans fixer ou imaginer une limite. Mais depuis, ils s'avèrent bien plus élevés et en constante augmentation. C'est là un fait qui tend à attester des efforts entrepris en termes de moyens. Cependant Tim Roemer évoque l'hypothèse selon laquelle cette croissance pourrait saper les objectifs initiaux en instaurant des redondances, des chevauchements, du gaspillage, etc., ce qui altèrerait par voie de conséquence la qualité du renseignement, de sa collecte à sa distribution.

- Le nombre de personnel sous contrat est en forte hausse dans la communauté du renseignement. Ce phénomène n'est en lui-même pas un mauvais indicateur[93]. Lorsqu'ils sont utilisés correctement, ces « sous traitants » peuvent accroître l'efficacité dans les fonctions de nature non gouvernementales et donc être une bonne contrepartie pour l'argent des contribuables. Cependant, un seuil a été franchi, tant au sein de la communauté du renseignement que de l'ODNI lui-même, et il est à craindre qu'un recours excessif ou mal maîtrisé à ces contractants privés conduise à des dysfonctionnements dans la pratique ainsi qu'à des déséquilibres budgétaires. Et le DNI n'a pour le moment pas été en mesure d'inverser ou du moins de contrôler cette tendance.

⇨ **Les insuffisances :**

- La diversité « ethnique » du personnel était une priorité de l'ODNI et des *100 et 500 Day Plan*. Au-delà de l'aspect purement moral qui veut qu'une administration nationale soit le reflet des spécificités de la société dans laquelle elle opère (qu'il s'agisse du sexe, de l'ethnie, de la provenance sociale, etc.), rassembler un personnel aux origines ethniques diverses permet notamment d'augmenter la capacité linguistique. Si les choses évoluent favorablement sur ce point, les a priori restent marqués et beaucoup de personnes « étrangères » se voient exclues du monde du renseignement en raison de leur milieu ou de leur origine. Faire confiance à de nouvelles recrues et leur donner accès à des informations touchant la sécurité nationale peut comporter certains risques mais se priver de compétences notamment en langues étrangères n'en comporte t-il pas de plus grands ?

[93] Sur ce thème lire : **5) L'externalisation du renseignement, p115**.

- La communauté du renseignement est relativement jeune, voire trop jeune. 70% des analystes ont moins de cinq ans d'expérience.

- Enfin, et c'est surement le problème le plus important, le partage de renseignements entre l'échelon fédéral et local est encore trop souvent entravé par des questions d'incompatibilité technique mais aussi par des réticences « culturelles » tenaces.

Pour tenter de parer à ces déficiences, Georges Bush annonçait le 31 juillet 2008, la révision de l'*Ordre exécutif 12333*[94]. De nouvelles dispositions augmenteraient les pouvoirs du DNI en matière de partage de l'information et elles prévoiraient l'élaboration de lignes directrices pour régir l'accès aux informations entre les différents organismes de renseignement.

Ces conclusions générales sur la création du DNI de l'ODNI et sur les changements amorcés par le *500 Day Plan* dans les mois et années à venir, ne sont pas mauvaises.

Des avancées ont été réalisées, d'autres sont en marche, des insuffisances perdurent, sachant qu'il s'agit là d'un bilan dans une période de « formation » de « mise en place » et que les résultats ne pourront donc être réellement appréhendés et évalués que dans quelques années.

b) La coopération Internationale.

Enormément de progrès ont été effectués dans ce domaine depuis les attentats du 11 septembre 2001. Pleinement conscients que leur incapacité à empêcher les attentats avait été due en partie à un manque de communication avec les services étrangers, les américains ont fait de ce volet international l'un des axes majeurs de leur « guerre contre le terrorisme ».

La satisfaction première concerne le net rapprochement impulsé depuis 2001 entre les Etats-Unis et un certain nombre de pays du Moyen-Orient au sens large, au sein desquels les activistes islamistes radicaux sont largement implantés et actifs. Des gouvernements d'Etats traditionnellement hostiles aux américains ont rejoint la lutte, du moins de manière officielle. C'est le cas notamment de l'Arabie Saoudite et du Pakistan. Non seulement ces pays luttent directement contre les groupes terroristes implantés sur leur territoire, mais ils transmettent également à leurs homologues américains des informations sur certains de leurs ressortissants implantés à l'étranger et susceptibles de fomenter des actions terroristes.

Et plus globalement la coopération entre les services américains de renseignement et les services étrangers s'est intensifiée et améliorée depuis quelques années. La CIA a par exemple ouvert des cellules ou centres dans plus d'une vingtaine de pays et dispose depuis 2002 d'un centre d'échange international de renseignement basé à Paris (*Alliance Base*). De

[94] L'Ordre exécutif 12333 est un document qui fut signé le 4 décembre 1981, sous l'administration Reagan et qui précise les objectifs, les taches et les responsabilités des activités de renseignement aux Etats-Unis, pour que celles-ci s'exercent de manière efficace et dans le respect des droits constitutionnels.

plus les services de renseignements américains ont tous établis des coopérations, qu'elles soient institutionnalisées ou non, avec de nombreux services de renseignement étrangers.

Cependant, la coopération américaine en matière de renseignement avec le reste du monde, se heurte toujours aux obstacles « traditionnels » de l'échange d'information, c'est-à-dire une collaboration qui dans les faits se trouve très largement affaiblie soit par le manque de volonté « politique », soit par des obstacles liés principalement à des procédures techniques et juridiques différentes ne permettant toujours pas un échange optimal des informations.

Mais ces déficiences ne constituent pas une surprise. Entre les Etats-Unis et l'Europe par exemple, des avancées positives se sont amorcées pour la coopération judiciaire, la transmission de données informatiques, etc., et cependant globalement le bilan est mitigé. Mais comment pourrait-il en être autrement alors que la transmission du renseignement s'avère elle-même déjà très souvent chaotique à l'intérieur même de l'Union Européenne, tant au niveau étatique qu'inter étatique ?

Ainsi la coopération USA/UE pâtit obligatoirement des déficiences existant à une plus petite échelle. Il ne faut jamais oublier en effet, qu'une coopération, et quelque soit le domaine, doit d'abord se révéler efficiente au « bas de la pyramide » avant de prétendre fonctionner aux échelons supérieurs.

4) Bilan au niveau du renseignement militaire.

a) Une adaptation cohérente aux nouveaux enjeux du terrorisme…

L'après 11 septembre a confirmé l'importance du « militaire » et plus particulièrement celle du renseignement militaire au sein de l'arsenal américain de lutte contre le terrorisme.

Cette vision organisée autour de la place prépondérante des forces armées pour contrer les réseaux et les activistes n'est pas nouvelle, mais elle s'est très largement accentuée à partir de 2001, avec le lancement de la « guerre contre le terrorisme » menée par les américains dans de nombreuses régions du monde.

La place de la *Defense Intelligence Agency* (DIA) au sein de l'arsenal anti-terroriste américain n'a cessé de grandir durant les années de l'après 11 septembre et ce, sur tous les théâtres d'opération concernés par la « *War on Terror* » que se soit en Irak, en Afghanistan, dans la Corne de l'Afrique, etc.

Et globalement, les structures du renseignement militaire aux Etats-Unis se sont correctement adaptées à ce contexte de lutte contre le terrorisme, et plus généralement à ce contexte stratégique post-Guerre Froide caractérisé par l'évolution des menaces et l'arrivée de nouveaux acteurs non étatiques.

Ainsi le renseignement d'« environnement » s'est développé, de telle sorte qu'on parle aujourd'hui davantage de renseignement d'« intérêt » militaire. Au-delà du renseignement centré purement sur les réseaux, des cellules de collecte ayant trait aux conditions sociales, politiques, économiques, religieuses, culturelles d'un pays ou d'une région, ont vu le jour, tout comme d'autres spécialisées dans la collecte d'informations liées aux trafics en tous genres ou aux engins explosifs improvisés (*Improvised Explosives Devices* ou *IED*), etc.

Les capacités techniques de collecte ont été rehaussées, notamment pour ce qui est de l'interception électromagnétique, mais aussi et surtout celles concernant les sources ouvertes, en premier lieu Internet.

Les Etats-Unis ont récemment créé une organisation du renseignement « toutes sources », nommé *Centre de renseignement conjoint*, sorte d'organe interarmées de collecte et de mise en commun des informations (mais les services civils de renseignement et services de sécurité peuvent y participer). Mais l'organisation s'avère lourde et la coordination et planification compliquées.

Sans détailler l'ensemble des évolutions techniques et pratiques du renseignement militaire, nous pouvons dire que les forces américaines se sont d'autant mieux et vite adaptées, qu'elles opèrent dans un domaine ou tout retard se traduit directement en vies humaines. Il ne s'agit donc pas d'amorcer des évolutions sur un trop long terme, ou d'amorcer de « fausses » évolutions comme c'est parfois le cas pour les agences « classiques ».

Cependant, au-delà de la place et du rôle du renseignement militaire au sein de la lutte contre le terrorisme, les forces militaires sont-elles une solution efficace et viable pour annihiler les activistes et les réseaux ?

b) …mais qui n'occulte pas le débat plus général sur le rôle et la place des forces armées dans le cadre de la lutte contre le terrorisme.

Même si l'on s'éloigne quelque peu du cœur du sujet, c'est une question fondamentale qui est posée ici. La place des forces armées dans ce domaine a toujours été un sujet de débat, mais encore plus depuis 2001.

En effet, sur ce plan, l'exemple du conflit « afghan » et encore plus celui de la guerre d'Irak sont édifiants. L'absence d'une vision globale et à long terme a renforcé ce que les américains voulaient contrer, c'est-à-dire le terrorisme.

Leur véritable erreur (mais elle est généralisée à une bonne partie de la communauté internationale), c'est de s'attaquer aux seules manifestations du terrorisme (et en plus par des moyens armées) et très peu à ses centres de gravité et racines.

Les Etats-Unis ont donc continué après le 11 septembre de développer, comme ils le faisaient auparavant, une stratégie finalement « symétrique » afin d'éliminer des individus de toute

façon prêts à mourir, avec une probabilité d'effet dissuasif par conséquent très faible mais avec, en revanche, un risque très élevé voire certain d'accroître la motivation des combattants.

Cette stratégie très « spectaculaire » et « démonstrative » a peut-être soulagé et rassuré l'opinion américaine après le choc du 11 septembre mais force est de constater que les résultats sont extrêmement discutables sept ans après l'événement et les impératifs fixés au départ loin d'être remplis.

Aujourd'hui l'Afghanistan est redevenu un axe majeur de développement du terrorisme, les Talibans reviennent au pouvoir et l'Irak est devenu une « école » de guérilla, l'un des terrains de recrutement et d'entraînement de terroristes le plus important dans le monde ainsi que le symbole « numéro 1 » de l'impérialisme américain inlassablement brandi par les terroristes.

La structure « historique » d'Al-Qaïda a certes été très durement touchée. Pour une majorité, ses dirigeants les plus importants ont été arrêtés ou sont aujourd'hui décédés et presque tous les instigateurs du 11 septembre ont connu le même sort. « Seulement » quinze attentats formellement montés par Al-Qaïda ont eu lieu dans le monde depuis 2001 provoquant cinq fois moins de morts que le 11 septembre.

Mais cet affaiblissement propre au « siège social » est trompeur, car partout dans le monde (au Maroc, en Algérie, aux Philippines ou en Turquie, etc.), les franchises ou les mouvements affiliés à Al-Qaïda ont repris le « combat ».

Les américains se sont donc non seulement trompés de cible, ils ont aussi et surtout installé un désordre plus grand qu'il ne l'était avant l'intervention.

Leur stratégie « armée » de lutte, n'a pas du tout engendré une « pacification » ou du moins une « stabilisation » du Moyen-Orient.

En Europe et en France particulièrement, on s'oppose à l'emploi récurrent ou trop important des forces armées dans la lutte contre le terrorisme. On refuse tout d'abord d'envisager des opérations miliaires sans la légitimité de l'ONU et de la même façon, on ne conçoit pas des opérations militaires indépendantes.

Pourtant, personne ne remet en cause le fait que l'emploi des armées pour contrer les terroristes est un outil indispensable. Mais alors comment concilier les deux approches, à savoir la « nécessité » et les « réserves ».

- Une voie de résolution pourrait tenir à la définition d'un « cadre légal » partagé par tous, sur les principes, les conditions, les modalités et les limites de l'intervention des forces armées. En effet, si les européens acceptent les forces armées en tant que moyen de lutte contre le terrorisme, ils restent cependant méfiants sur l'emploi qui peut en être fait.
  L'intervention militaire en Irak des américains contre l'avis du conseil de sécurité et de la majorité de la communauté internationale, bien que menée « contre le terrorisme » était elle justifiée ? Où se situe la frontière entre la « préemption » qui répond à une intention et la « prévention » qui répond, elle, à des capacités ?

Ces questions doivent être débattues et tranchées au travers de règles claires, dont le respect puisse être imposé et contrôlé. La décision d'intervenir militairement (ou pas) doit reposer sur l'examen de critères précis et strictement énoncés tant en ce qui concerne les situations que les objectifs.

L'ONU dispose de la légitimité « juridique » pour représenter ce cadre. Cependant, comme nous l'avons déjà mentionné, elle manque aujourd'hui d'une autorité suffisante sur les plus grandes nations (surtout les Etats-Unis) pour imposer ses décisions (comme en a témoigné la guerre en Irak de 2003).

- De plus, d'un point de vue opérationnel, il existe généralement toujours un « vide » pour les opérations de traque prolongée et d'élimination des réseaux sur le long terme. En effet, la plupart des pays disposent soit de petites unités anti-terroristes spécialisées dans des opérations très spécifiques comme la libération d'otages ou les détournements d'avions, soit d'unités militaires « conventionnelles » de plus grande importance. Et lors d'opérations comme *Enduring Freedom*, ces deux types d'unités sont inadaptés. L'Allemagne a par exemple envoyé les KSK (« *Kommando Kräfte* »), des unités anti-terroristes spécialisées dans la libération d'otages, mais pas formées pour la traque de longue haleine contre les Talibans. Il manque encore dans la plupart des Etats, des unités pour assurer des missions « contre-terroristes » au premier sens du terme et capables d'opérer en dehors du territoire national.

Donc, plus que l'emploi des forces armées dans la lutte contre le terrorisme, et davantage que la place occupée par le renseignement dans cette activité - qui ne sont pas remis en cause - c'est la « façon de faire » qui donne lieu à débat.

On se rend compte qu'une stratégie de lutte peut donc paradoxalement renforcer le phénomène, si elle est mauvaise ou mal utilisée.

5) L’externalisation du renseignement : conséquences à « double tranchant ».

L’externalisation du renseignement aux Etats-Unis dans le cadre de la lutte anti-terroriste, longtemps envisagée comme une simple « tendance » est en fait une réalité. Pour ne (re)donner qu’un chiffre, on estime qu’entre 50 et 70% du budget de la communauté américaine du renseignement en 2007, était affecté à des entités privées.

Ce phénomène, déjà mesurable dans les années 90, a véritablement explosé après le 11 septembre 2001. Les besoins étaient alors tels, et la hausse des budgets si insuffisante pour les couvrir, que l'externalisation fut pour les agences gouvernementales le moyen de « gestion » leur permettant de répondre à la demande tout en limitant les coûts. Aujourd’hui, il faut constater que les acteurs privés offrent des services de qualité et en adéquation avec les activités du renseignement. « Ré-internaliser » le renseignement semble désormais inenvisageable et n’est d’ailleurs pas souhaitable face à la surabondance de données à collecter et exploiter via les sources ouvertes. Les entreprises extérieures sont un complément très utile pour les agences et la grande diversité des moyens et des sources qu'elles offrent ne peut à priori qu'être profitable.

Cependant divers éléments viennent relativiser ce constat :

- L’apport de ces acteurs privés dissuade les agences gouvernementales de se réformer, ou du moins empêche que ces réformes se fassent en profondeur. En effet, l’externalisation est désormais une alternative pouvant pallier les insuffisances des agences. En ce sens elle devient une solution de facilité qui masque la nécessité de bousculer certaines habitudes, un frein à la volonté.

- Les employés de ces sociétés, contrairement aux fonctionnaires des agences étatiques, ne sont pas tenus de rendre des comptes et on peut craindre, pour cette raison, que le gouvernement leur confie des missions « sensibles » telles que l’interrogatoire de prisonniers. D’ailleurs c’est déjà une réalité, puisque nombre de ceux menés en Afghanistan et en Irak ont été externalisés. Le risque qu'ils donnent lieu à des pratiques et dérives douteuses, voire davantage, ne peut être écarté.

- Si ces sociétés sont de bons sous-traitants pour les agences, elles peuvent devenir également de sérieuses concurrentes. En effet, de plus en plus de membres expérimentés de la communauté du renseignement quittent les agences étatiques telles que la CIA pour rejoindre le secteur privé ou les rémunérations sont beaucoup plus avantageuses. C’est ce que l’on nomme désormais la « fuite des espions » et elle est importante car l’effectif de certains acteurs privés est composé quasi exclusivement d’anciens membres des agences gouvernementales. Et c’est d’ailleurs pour la contrer « *que la CIA interdit depuis peu aux entreprises avec*

lesquelles elle est en contrat de lui proposer des personnels ayant quitté la CIA depuis moins de dix-huit mois »[95].

- Ce différentiel de rémunération peut également avoir un effet négatif sur le moral des employés des agences qui constatent que ceux du secteur privé gagnent davantage alors qu'ils effectuent le même type de tâches.

- Mais se pose également la question du coût réel pour le gouvernement de cette externalisation. Certes, par ce biais l'Etat fait d'importantes économies surtout parce qu'il n'a pas à payer les pensions de retraites des employés du privé. Cependant la *Commission du Sénat sur le Renseignement* a démontré qu'un fonctionnaire revenait à 126 000 dollars par an à l'Etat, contre 256 000 dollars pour un employé extérieur[96].

L'externalisation du renseignement aux Etats-Unis s'avère donc à « double tranchant ».

Ce bon complément aux activités des agences gouvernementales, peut indéniablement constituer aussi un « danger » pour leurs(s) activité(s).

Néanmoins, aujourd'hui la privatisation du renseignement est une réalité, un retour en arrière n'est plus envisageable et il s'agit donc de trouver les bonnes conditions pour que cette participation s'avère bénéfique pour tous.

[95] Walter Pincus, Stephen Barr, *CIA Plans Cutbacks, Limits on Contractor Staffing*, tiré de Raphael Ramos.Op.cit p53.
[96] John D. Rockefeller, *Report 110-75*, Senate Select Committee on Intelligence, 31 Mai 2007, p. 11, tiré de Raphael Ramos.Op.cit p53.
http://intelligence.senate.gov/11075.pdf

II) Bilan des évolutions du renseignement au niveau des organisations internationales (ONU, OTAN, UE).

1) Les Nations Unies (ONU).

a) Son rôle dans le renseignement ne peut être appréhendé qu'au regard de son rôle dans la lutte contre le terrorisme.

Comme nous l'avons dit précédemment, les Nations Unies ne tiennent aucun rôle particulier, ou ne disposent d'aucune capacité spécifique en matière de renseignement.
Pourtant, il serait erroné de ne pas lui accorder tout de même un certain crédit dans ce domaine. En effet, grâce aux activités de certaines de ses entités, l'AIEA par exemple (*Agence Internationale de l'Energie Atomique*), l'organisation dispose de nombreuses informations et brasse une quantité importante de renseignements. Ainsi, en 2003, avant le déclenchement de la guerre en Irak, les experts mandatés par l'ONU, furent en mesure de contredire les américains concernant la présence supposée d'armes de destruction massive dans ce pays.
Cependant, encore une fois l'ONU ne dispose d'aucune structure ou d'aucun système spécifique, qui serait consacré au partage de ces renseignements entre tous les membres. De plus, lorsque l'organisation appelle à favoriser l'échange de renseignement, elle le fait majoritairement par le biais d'orientations, de législations, de résolutions, etc., qui concernent la lutte anti-terroriste en général. Précisons d'ailleurs que n'ayant pas non plus de moyens opérationnels dans ce domaine, elle vise à établir les grands principes juridiques et non pas à « agir » en tant que tel.

Appréhender l'apport des Nations Unies pour le renseignement est toutefois possible mais il faut le faire au travers de leur rôle dans la lutte contre le terrorisme et de la refonte profonde qu'elles ont connue avec le 11 septembre.

Les résolutions 1368 du 12 septembre 2001, et encore plus la 1373 du 28 septembre 2001 en furent les clés de voûtes et énoncèrent des décisions inédites.

Pour rappel, la première laissait le champ libre à une riposte armée de la part de l'entité agressée (en l'occurrence les USA), en réponse à un acte terroriste.
La seconde imposait véritablement aux Etats une obligation de mettre en place les clauses qu'elle édictait. Les mesures intérieures, législatives et exécutives, dépassaient pour la première fois le simple cadre de la « recommandation » ou du « conseil » et afin d'en contrôler la mise en œuvre, un *Comité Contre le Terrorisme* (CCT) était créé.

Ces deux résolutions furent ensuite complétées par d'autres, mais ensemble elles constituent pour le droit pénal international une véritable révolution et plus largement, elles installent la problématique du terrorisme international comme l'une des premières préoccupations et priorités du Conseil de Sécurité et de l'ONU.

Concernant le cas spécifique du renseignement, l'ONU s'était toujours attelée à faciliter l'échange d'informations entre les Etats dans le cadre de la lutte contre le terrorisme. Cependant cette résolution 1373 ne se contentait plus cette fois-ci de simplement recommander ou de conseiller, elle imposait **une coopération entre les Etats notamment pour une meilleure circulation du renseignement**. Et avec la création de ce CCT, on était en droit d'attendre une application forte et généralisée de ces prérogatives.

Mais des éléments viennent relativiser le véritable effet de ces deux textes et au-delà l'efficacité globale de la stratégie de lutte contre-terroriste de l'ONU.

b) Les prérogatives ne sont toujours pas assez respectées, et le rôle des Nations Unies reste donc toujours relatif.

L'aspect obligatoire de la résolution 1373 n'est pas toujours respecté.

En dépit de la création du CCT et des menaces de sanctions, un certain nombre d'Etats ne peuvent, ou ne veulent pas suivre la résolution 1373. Son interprétation est également très souvent divergente selon les Etats :

- Beaucoup d'Etats entendent par : « *financement des activités et des groupes terroristes* » uniquement le blanchiment d'argent. Or le terrorisme se finance souvent aux moyens d'activités tout à fait légales et légitimes qui peuvent aller du simple commerce de proximité jusqu'à des sociétés au poids économique important, ou des ONG, etc. Des confusions sur le gel, la saisie ou la suspension des comptes sont également à signaler[97].

- De même, certains pays traitent les actes terroristes sur leur propre sol, mais omettent de coopérer avec d'autres Etats sur des actes terroristes perpétrés par certains de leurs ressortissants à l'étranger.

- La coopération internationale n'est pas formalisée dans le cadre de la résolution 1373, elle reste cantonnée à la simple coopération judiciaire par le biais des extraditions. Le renseignement n'est l'objet d'aucune mesure concrète. On demande vivement aux Etats de coopérer, mais rien de plus n'est engagé ou proposé.

- Mais le bémol principal à propos de cette résolution réside dans le fait que beaucoup d'Etats désireux de la mettre en place n'en ont pas les moyens législatifs, administratifs et financiers. C'est d'ailleurs pour pallier à cette impossibilité que l'Union Européenne, notamment, apporte une aide de plusieurs centaines de millions

[97] Chantal De Jonge Oudraat, *Le conseil de sécurité de l'ONU et la lutte contre le terrorisme*, 2005, 14p.

d'euros par an aux pays tiers qui se trouvent dans cette situation (environ 400 millions d'euros par an depuis 2004). À ce titre : « *Une analyse informelle du respect de la résolution 1373, conduite à l'automne 2003, a révélé que soixante-dix Etats souhaitaient la mettre en œuvre, mais n'en étaient pas capables, tandis que quelques soixante Etats s'y conformaient peu à peu et que, parmi les trente Etats considérés comme ayant atteint « un degré de respect considérable » quelques blancs persistaient, particulièrement sur la question des transferts financiers illégaux. Enfin les besoins d'aide dépassaient de loin les moyens du CCT* »[98].

Le rôle et le poids des Nations Unies restent donc toujours relatifs.

Son rôle de coordinateur ou plutôt d'établissement des grands principes juridiques de la lutte contre-terroriste au niveau mondial, est accepté « symboliquement » par tous les Etats membres et de fait par la très grande majorité des pays du monde, mais il ne se vérifie pas complètement dans la réalité.
En effet, la seule définition entérinée par l'organisation concerne des actes précis « dits » terroristes, mais elle ne qualifie même pas ce qu'est un « acte terroriste » en général.
En l'absence d'une description claire et consensuelle de ce qu'elle entend combattre (ou aider à combattre), l'ONU perd en efficacité et malgré sa légitimité à intervenir dans une lutte se voulant internationale, elle est reléguée à un rang de pouvoir et d'action secondaire.

De plus, la résolution 1373, même si elle rompt avec le caractère « facultatif » des précédentes résolutions, ne formalise pas pour autant les sanctions en cas de non-respect ni l'autorité compétente qui serait chargée de les appliquer.

En effet, le *Comité Contre le Terrorisme* ne bénéficie pas des fonds et des personnels suffisants pour apporter l'aide nécessaire aux pays incapables de mettre en œuvre les résolutions onusiennes ou réticentes à les appliquer. C'est pourquoi des coopérations bilatérales se sont mises en place, notamment entre l'Union Européenne et des pays Tiers.
Par ailleurs, l'ONU ne parvient guère à s'opposer le cas échéant à de grandes puissances comme le sont les Etats-Unis mais aussi les états européens les plus influents.

Dans ces conditions, l'apport des Nations Unies dans le renseignement reste très limité, voire inexistant.

[98] *Ibid*. Chantal De Jonge Oudraat Op.cit. p 119.

2) L'Alliance Atlantique (OTAN).

a) Le caractère « multilatéral » du renseignement, encore difficile à concilier.

Depuis 2001, les progrès de l'OTAN en matière de renseignement appliqué à la lutte contre le terrorisme ont été nombreux.

Rappelons les principales étapes et avancées :

- L'élaboration du *Plan d'action du Partenariat contre le terrorisme* qui a fait du renseignement l'un des éléments centraux.
- La définition d'un nouveau *Concept Militaire* dans le domaine de la défense contre le terrorisme dans lequel le renseignement occupe aussi une part importante.
- La création d'une cellule de réflexion sur la menace terroriste dans l'Etat-major de l'OTAN.
- Le renforcement des activités contre terroristes et d'échange de l'information menées par le *Conseil OTAN-Russie* et le *Conseil de partenariat euro-atlantique.*
- La consolidation de l'activité de l'*Etat-major International (EMI)* au sein duquel la *Division du Renseignement* (*Intelligence Division*) joue un rôle d'information pour les autres entités de l'organisation.
- L'extension des attributions du *Comité Spécial*.
- La tenue d'un essai grandeur nature de nouvelles technologies pour le renseignement, nommé *Trial Spartan Hammer*.
- La constitution d'un *Groupe de travail sur le renseignement d'origine électromagnétique et les mesures de soutien électronique*.
- La construction de six centres de coordination et d'échange du renseignement, dont le premier a ouvert à la frontière afghano-pakistanaise en 2008.
- Enfin la création en octobre 2006 de l'IFC : *Intelligence Fusion Center*.

L'action otanienne depuis les attentats de New-York et Washington a donc été importante et l'Alliance dispose aujourd'hui d'outils, de moyens, de systèmes lui permettant d'organiser et d'appuyer la lutte contre le terrorisme.

Cependant, des carences perdurent et en premier lieu celle tenant à l'absence d'un service propre de collecte du renseignement. La création de l'IFC en 2006 est un pas en avant pour la construction d'une telle structure dans le futur, car il s'agit bien d'un centre de collecte du

renseignement, mais de renseignement militaire qui plus est, de caractère général. Il n'est donc pas spécialisé dans la lutte contre le terrorisme.

L'OTAN joue un rôle certain de coordination et de diffusion des renseignements issus des services nationaux des pays membres avec l'avantage supposé et attendu de fournir un renseignement multi-sources et donc de pouvoir confronter plusieurs points de vue. C'est logiquement un vecteur « d'enrichissement » pour le renseignement.

Mais hélas, il reste « théorique » car cette dépendance de l'Alliance vis-à-vis des pays membres, représente également son principal point faible[99] :

- En effet ces contributions sont extrêmement variables que se soit en volume ou en régularité. De plus la multiplicité des sources n'est en fait que très relative puisque dans la réalité, seuls quelques pays alimentent l'échange : Etats-Unis, à l'Allemagne, Royaume-Uni, Italie, Danemark et France essentiellement.

- Même si, même si la langue officielle de l'organisation est le Français, c'est l'Anglais qui est la langue de travail et toute contribution de renseignement rédigée dans une autre langue est presque immédiatement laissée de côté.

- Cette origine « nationale » du renseignement pose également un certain nombre de problèmes en ce qui concerne les échanges de l'Alliance avec des pays extérieurs ou avec d'autres organisations internationales. En effet, avant d'envisager une collaboration avec une entité étrangère, il faut obligatoirement passer par l'assentiment de l'ensemble des membres de l'OTAN, une unanimité qui ne s'obtient que très difficilement et rarement. Bien que la confidentialité soit garantie et qu'il s'agisse de documents produits au sein même de l'OTAN, des oppositions sont présentes car dans tous les cas l'origine du renseignement reste nationale.

- Enfin, le renseignement produit à l'OTAN doit être validé par consensus, avec les conséquences suivantes :

  - Lorsque les contributions se résument à quelques pays, le consensus est plus facile à trouver, mais la qualité du produit fini s'en trouve réduite.

  - A l'inverse, lorsqu'elles sont plus nombreuses, le renseignement n'en serait que meilleur mais alors le consensus est pratiquement impossible à établir entre tous les contributeurs. Pour que le document soit agréé, il faut donc « lisser » les aspects les plus marqués, et l'on perd donc en intérêt et en pertinence. Les spécialistes qui exploitent ensuite ces documents savent généralement « lire entre les lignes » et décoder les passages où l'information a été volontairement édulcorée, néanmoins tout le processus d'élaboration du renseignement se trouve alourdi.

[99] A ce sujet, lire : Michel Choux, *Sécurité et Défense en Europe – Le renseignement stratégique de l'OTAN*, Défense Nationale, 2001.

Ces faiblesses existaient avant 2001 mais force est de constater qu'elles demeurent d'actualité aujourd'hui et qu'elles entravent ou limitent les progrès réalisés.

Mais surtout, au-delà des imperfections liées directement au renseignement, c'est la « crise » traversée au sein de l'OTAN, en interne qui se révèle le plus préjudiciable non seulement pour le renseignement, mais plus généralement pour l'efficacité de la lutte contre le terrorisme.

b) Le consensus sur la lutte contre le terrorisme dissimule mal les difficultés structurelles de l'organisation.

Si un consensus général existe au sein de l'OTAN - particulièrement depuis 2001 - concernant la lutte contre le terrorisme et plus spécifiquement sur la place que doit y occuper le renseignement, il ne peut cacher les difficultés structurelles, voire la véritable crise à laquelle doit faire face l'Alliance depuis quelques années.

Le refus de plusieurs pays européens membres de l'OTAN (la France en premier lieu) de participer à la guerre en Irak en 2003 a largement détérioré les relations au sein de l'organisation.

Mais le thème de l'engagement en Irak n'est pas le seul responsable de cette situation.

Le développement de la *Politique Européenne de Sécurité et de Défense* (PESD/PESC) mais aussi l'écart grandissant entre les conceptions européenne et américaine de la sécurité ont alimenté la crise.

Les Etats-Unis sont plus que jamais contestés sur le plan diplomatique et politique, principalement par des Etats de forte tradition atlantiste (Turquie, Allemagne, Espagne, etc.). Les intérêts économiques entre les américains et les européens entrent de plus en plus en concurrence, et surtout la « fracture » intellectuelle et culturelle sur la façon de concevoir les relations internationales n'a jamais été aussi accentuée.

La « cassure » ne semble pas être circonscrite à une conjoncture politique défavorable, mais de nature plus profonde et durable.

L'année 2008, marquée notamment par le rapprochement français impulsé par Nicolas Sarkozy, laisse augurer d'un retour à de meilleures relations. Mais il est encore trop tôt pour en tirer de véritables conclusions.

Et dans les conditions actuelles et en dépit de la convergence officielle des opinions en matière de lutte contre le terrorisme, on peut difficilement envisager que la transmission du renseignement – activité demandant de fait une grande « confiance » entre les membres – puisse être exploitée au maximum de ses possibilités dans le cadre de l'OTAN.

3) L'Union Européenne.

a) Des efforts conséquents amorcés au niveau de la lutte contre le terrorisme et du renseignement…

Le 11 septembre a marqué pour l'Union Européenne le point de départ d'une véritable mise en place d'une stratégie contre-terroriste commune. La préparation de l'opération en partie sur son sol, ainsi que la « faillite » des services de renseignement l'ont alertée sur sa vulnérabilité importante face à ce terrorisme d'un nouveau genre.

Précisons tout de même à titre purement indicatif que pour l'Europe, beaucoup d'évolutions, d'avancées, de changements dans le cadre de la lutte anti terroriste et du renseignement ont été davantage impulsés après les attentats de Madrid en 2004 et de Londres en 2005. Le choc avait été immense en 2001, mais c'est véritablement ces attentats perpétrés sur le sol européen qui ont dans beaucoup de cas fait avancer significativement les choses.

Trois grandes mesures phare ont cependant découlé directement des enseignements du 11 septembre 2001 :

- La mise en place du mandat d'arrêt européen.
- L'accord sur une définition concertée et commune du terrorisme : une concrétisation préalable, nécessaire à toutes les autres et à forte portée fonctionnelle et symbolique puisque, à partir d'elle, les Etats membres appréhendent le phénomène d'une façon similaire et cohérente.
- Mais surtout pour ce qui nous intéresse ici : le renforcement certain des coopérations entre services de renseignement européens que ce soit au sein des institutions de l'Union, ou bien par l'élaboration de coopérations bi ou multilatérales développées en parallèle.

De plus, même s'il s'agit de la lutte contre le terrorisme d'un point de vue général – et pas seulement de renseignement - le budget de la « lutte » au niveau de l'Union a été considérablement augmenté, de 30 millions d'euros en 2001 à 600 millions d'euros aujourd'hui (on reste cependant encore bien loin des américains), auxquels il faut ajouter les crédits pour la sécurité globale. De même, l'aide fournie par l'Europe à des pays tiers pour la bonne application de la résolution 1373 de l'ONU est passée de 250 à 410 millions d'euros entre 2004 et 2006[100].

[100] M. Lahetjuzan, *La lutte anti-terroriste enjeu de puissance pour l'Europe*, CID, 2006, 37p.

Le Conseil européen a également créé un poste de *Coordinateur de la lutte contre le terrorisme*. C'est M.Gijs de Vries qui a hérité de cette place avec pour mission principale la rédaction de rapports réguliers au *Conseil*, concernant le suivi de ces mesures.

La *Politique Européenne de Sécurité Commune (PESC)* et son utilité ont été réévaluées par ce même *Conseil Européen* qui a adopté une déclaration contre le terrorisme[101].

Des clauses relatives au contre-terrorisme ont été également introduites dans tous les nouveaux accords de coopération et de développement avec des pays tiers.

Ces décisions (entre autres) ont permis aux membres d'affirmer de façon théorique une volonté commune de dépasser la souveraineté nationale, de réduire ou solutionner les obstacles juridiques pour la réalisation d'une espace commun de sécurité et de justice.

Voilà pour l'aspect « positif » et déclaré de la lutte au niveau de l'Europe après le 11 septembre. Cependant un certain nombre d'obstacles et de points noirs persistent, en particulier au niveau du renseignement.

b) …mais des efforts insuffisants.

- **L'échange d'informations et de renseignement : manque de volonté politique.**

  - Le projet d'une « CIA » européenne n'est pas encore à l'ordre du jour et c'est très significatif de la place et du rôle du renseignement au sein de l'Union.

    En 2004, la Suède a déposé en ce sens un projet de décision cadre sur la simplification de l'échange de renseignement, mais la plupart des « grands » pays tels que la France s'y sont opposés parce qu'ils ne sont pas prêts à abandonner les principes du droit national selon lesquels des informations détenues par les autorités judiciaires ne doivent pas être transmises par le biais de la coopération policière. Ils avaient de la même façon rejeté la demande de l'Autriche et de la Belgique pour la création d'une agence européenne de renseignement.

    Les coopérations sur le renseignement ont bien progressé après le 11 septembre, mais l'Union se heurte toujours à cette question fondamentale inhérente à la mise en place d'une « CIA » européenne : le veut-elle vraiment ?

    Car derrière cette « non » décision se pose toute la problématique de la souveraineté des Etats et de leur degré d'autonomie les uns vis-à-vis des autres et vis-à-vis de l'Union.

[101] Constance Chevallier-Goven, L*a lutte contre le terrorisme au sein de l'Union européenne*, Arès n°56, Volume XXII, décembre 2005.

Elle n'est d'ailleurs pas exclusive à la lutte contre-terroriste, elle a trait au statut même de l'Europe. Tant qu'une réelle volonté de créer une Europe politique proprement dite ne sera pas entreprise par les Etats membres, le projet d'une mise en commun quasi-totale et permanente du renseignement demeurera illusoire.

À l'heure qu'il est, les modes de partage des informations dans le cadre de l'Union Européenne sont satisfaisants mais reposent toujours sur le bon vouloir des Etats et des services concernés à transmettre ou non les informations en leur possession. C'est la faiblesse première dans ce secteur.

- Si la coopération policière a mené à la création du troisième pilier et des institutions *Europol* et *Eurojust*, le renseignement n'a lui en revanche pas donné lieu à la constitution pourtant espérée par beaucoup d'*EuroRens* qui pourrait devenir l'équivalent des deux entités précédemment citées, dans le domaine du partage d'information.

  Globalement, la coopération est très bien installée entre services de renseignements autant sur des points généraux que spécifiques. Le problème tient à la constance de cette coopération qui est très fluctuante dans le temps.

- De même, aucune définition du renseignement n'existe à l'échelle européenne, ni même une liste des services de renseignements européens comme c'est le cas pour les services de polices[102]. Beaucoup de pays ne reconnaissent d'ailleurs toujours pas certains de leurs services de renseignement. C'est assez symbolique du flou qui entoure encore cette activité au sein de pays membres de l'Union.

- **Les obstacles techniques et juridiques:**

  De plus, au-delà du manque de volonté, ou des réticences liées aux questions de souveraineté, la coopération européenne sur le renseignement se heurte souvent à des obstacles techniques et juridiques qui empêchent une transmission optimale des informations :

  - Des obstacles techniques, non seulement entre services étrangers, mais aussi et souvent entre services d'un même pays, rendent la transmission des données incompatibles. C'est en partie à cause où grâce à cela (mais pas seulement) que les Etats européens préfèrent souvent développer des collaborations bi ou multilatérales en dehors des institutions de l'Union, pour pouvoir travailler avec plus de « souplesse ». Il est en effet plus simple d'échanger des informations avec seulement un ou quelques pays, plutôt qu'avec une multitude d'Etats aux pratiques et systèmes différents.

[102] *Ibid.* Didier Bigo Op.cit.p 35.

- Les obstacles juridiques ont les mêmes effets. L'effort d'harmonisation des législations nationales, tout comme la mise en oeuvre du mandat européen s'avèrent insuffisants. Malgré une « adhésion intellectuelle » des Etats, les différences entre le droit Romain, anglo-saxon et scandinave rendent la coopération judiciaire lente.

  En Allemagne Mounir al Motassadeq impliqué dans les attentats du 11 septembre puis dans ceux de Djerba a vu son jugement annulé par la cour fédérale parce qu'il n'aurait pas bénéficié de conditions de défense équitables.

  La France a toujours refusé d'extrader Cesare Battisti, ancien membre des *Brigades Rouges* lorsque ce dernier était détenu sur le territoire.

  Le 1er juin 2004, l'extradition de trois membres d'un groupe indépendantiste Basque a été rejetée par le tribunal de Pau au motif qu'une partie des infractions avait été commise en France, alors que le mandat d'arrêt européen aurait dû logiquement le permettre.

  Mais surtout, il existe encore des différences marquées dans l'obtention, la détention puis éventuellement la transmission de données relatives aux individus. Par exemple, les règles en matière de rétention des données varient complètement d'un Etat à l'autre. En France, la « *Commission Nationale de l'Informatique et des Libertés* (CNIL)» considère que la rétention des données pendant plus d'un an dans le cadre du terrorisme serait disproportionnée, alors que l'Irlande les conserve pendant trois ans, l'Italie pendant deux ans (renouvelable) et l'Allemagne, à l'inverse seulement six mois. Cette disparité empêche la bonne transmission du renseignement et représente parfois une entrave aux investigations.

  Ces quelques exemples montrent qu'il existe, malgré des intentions sincères, des divergences au sein même de l'Union. Le pas vers une substitution des droits nationaux par le droit européen n'a pas encore été franchi et le renseignement en pâtit.

- **Pas de position commune :**

  Plus globalement, l'UE donne parfois une image totalement divisée concernant le traitement accordé au renseignement. C'est particulièrement vrai à la lumière de la collaboration qu'entretiennent certains services nationaux avec la CIA. Les transferts illégaux sur le sol de pays européens de suspects détenus sans procès ou bien les programmes de « surveillance » initiés par les autorités américaines, qu'ils concernent la finance ou les registres des voyageurs sont parlants. En effet il n'existe aucun consensus entre les Etats européens sur ces dossiers. Certains collaborent, d'autres s'y opposent fortement, aucune ligne directrice n'émerge. Il s'agit d'ailleurs ici d'un problème bien plus large que le simple thème du renseignement, et qui renvoie à la constitution politique de l'Europe. Mais comment élaborer - si ce n'est une position

« européenne » commune sur le renseignement - au moins des grands principes généraux, dans ces conditions ?

- **Les services de police et de justice souvent sous utilisés :**

  Le bilan des entités de police et de justice non spécialisées dans le renseignement, mais qui participent à cette activité (soit en produisant elles mêmes du renseignement soit en l'exploitant) est également mitigé :

  - *Europol* n'a toujours pas des résultats très convaincants car il n'est pas doté d'une compétence opérationnelle. Il reste un organisme d'analyse et d'échange d'informations sans capacité d'intervention et dont l'efficience est dépendante de la volonté des Etats.
  - *Eurojus*t reste, en dépit des améliorations, un organisme assez méconnu, modeste et aux pouvoirs limités. Le taux de transmission de dossiers relatifs au terrorisme, par les Etats européens plafonne à un niveau très bas : 6% en 2003, 7% en 2004.
  - Les *équipes d'enquêtes communes* et la *Task Force des Chefs de Police* (TFCP) sont encore trop rarement utilisées.

Il n'existe au sein de l'UE, aucune organisation ou système de recueil communs du renseignement.

De plus, l'échange du renseignement se fait la plupart du temps entre services nationaux, par le biais de collaborations ponctuelles rassemblant la plupart du temps deux ou trois pays et en dehors du cadre des institutions européennes.

Des progrès parfois considérables ont été réalisés dans les dernières années, particulièrement avec la création de SITCEN et de la cellule de « renseignement » au sein de l'Etat-major de l'Union Européenne (EMUE). Mais ces initiatives sont tributaires encore et toujours de la volonté des Etats membres de les alimenter et/ou d'y participer, ce qui les rend parfois aléatoires et partielles.

Sur le renseignement technique, malgré l'augmentation des capacités de collecte, l'Europe se situe toujours très loin des américains. Le Centre satellitaire de Torrejon dispose par exemple d'un personnel peu adapté et souvent en nombre insuffisant. Mais surtout, et davantage encore que pour les entités d'échange de renseignement humain, les systèmes d'interceptions techniques au niveau de l'espace européen reposent quasi exclusivement sur des collaborations étatiques se faisant en dehors du cadre de l'Union. C'est le cas par exemple

pour le programme Hélios (France, Italie, Espagne). Le renseignement de source spatiale est probablement plus que n'importe quel autre, le fruit d'une mise en commun ponctuelle de programmes nationaux, et non d'une véritable politique globale et concertée.

L'idéal serait de réaliser l'« Europe du renseignement » qui passerait par la mise en place d'une vraie entité européenne œuvrant dans ce domaine, sorte de « CIA à l'européenne »[103]. Mais une telle agence de renseignement intégrée ne s'inscrit pas dans un horizon à court terme, du fait des réticences politiques de la majorité des Etats membres, qui verraient dans une telle initiative, une remise en cause de leurs pouvoirs nationaux. Un exemple parlant est à chercher dans le Traité simplifié de l'Union Européenne (ou Traité de Lisbonne). Ce dernier mentionne que « *la sécurité nationale reste de la seule responsabilité de chaque Etat membre* ».

En attendant, l'élaboration d'une politique générale du renseignement au sein de l'Union pourrait représenter un premier pas vers une intégration plus forte, car elle permettrait d'uniformiser les positions nationales et donc de d'établir les bases d'une vision et démarche communes, sans altérer le principe de souveraineté. De même les institutions européennes doivent continuer leur effort pour harmoniser les politiques nationales du renseignement et les juridictions.

Mais encore une fois, il ne s'agit même plus ici d'une question spécifique au renseignement. C'est plus généralement la question d'une Europe politiquement unitaire et tangible qui est posée. Tant qu'elle ne sera pas réalisée, tant que la souveraineté nationale prendra le pas sur les outils à l'échelon européen, le contre-terrorisme et le renseignement manqueront de moyens et d'efficience.

[103] On pourrait tout de même discuter du bien fondé de ce terme, puisque la CIA bien qu'étant l'agence de renseignement la plus célèbre du monde, n'est qu'une des 16 agences de renseignement aux Etats-Unis, et n'est ni la plus importante en terme de budget ni la plus importante en en terme de personnel. Mais quoi qu'il en soit cette expression est la plus utilisée pour évoquer la constitution d'une grande agence de renseignement européenne, car la plus « parlante », nous la reprendrons donc ici.

III) Bilan au niveau français.

1) Evolution « en douceur » sur la période 2001-2007.

Contrairement à d'autres pays ou organisations du monde, le dispositif contre-terroriste français était déjà en place, bien avant le 11 septembre. Ou du moins il était plus complet que ceux de la majorité des acteurs mondiaux dans ce domaine.

Touchée très tôt par le terrorisme islamiste (dès 1986) la France a eu l'« avantage » si l'on peut dire d'avoir construit et adapté son appareil de lutte et de prévention sur la durée. Ainsi il a « mûri » avec le temps et évolué avec le terrorisme.

Même si la menace terroriste est omniprésente sur la France (mais ni plus ni moins que pour ses voisins européens, la probabilité d'attentat terroriste islamiste étant relativement égalitaire entre les pays), les faits parlent en faveur de cette expérience et de cette particularité puisque aucun attentat d'origine islamiste n'a frappé le territoire français depuis 1995. C'est pourquoi, après le 11 septembre les autorités ne se sont pas précipitées pour apporter des changements au dispositif anti terroriste.

Des évolutions se sont produites mais elles ont été réalisées sereinement et non pas dans une situation d'urgence ou de nécessité.

Ainsi, contrairement à d'autres Etats ou organisations (les Etats-Unis en premier lieu), la France n'a pas remis en cause son système de renseignement après 2001. Elle s'est contentée à cette période d'augmenter raisonnablement les budgets, de renforcer son arsenal anti-terroriste et de renseignement, de favoriser la coordination en interne, de participer davantage à la coopération internationale, etc., mais aucune refonte majeure ne fut engagée.

Pourtant, force est de constater que le renseignement français présente des faiblesses, sans que l'on puisse toutefois parler de « point noir ».

En effet, même si la France est la seule nation de l'Union Européenne à disposer d'une autonomie complète en matière de renseignement, le système national demeure déficient, surtout quantitativement, et tant ses effectifs que ses moyens financiers restent moindres que ceux des américains, britanniques et même allemands.

Concrètement, l'après 2001 fut marqué par des avancées réelles, mais qui ne remettaient cependant pas en cause la communauté française du renseignement :

- La loi du 23 janvier 2006 relative à la lutte contre le terrorisme élaborait ou améliorait un certain nombre de procédures administratives concernant les données de communications et modernisait le « *Fichier National Transfrontière (FNT)* » relatif aux documents de voyage et visas.

- La loi du 9 octobre 2007 quant à elle, impulsait enfin le tant attendu contrôle parlementaire du renseignement.

- Les moyens techniques de renseignement furent renforcés notamment par les biais des satellites d'écoutes et observation des communications.

- Les hausses budgétaires allouées aux organes de renseignement du Ministère de la Défense avant 2001 se sont légitimement poursuivies après les attentats. A noter cependant qu'elles ne concernent pas exclusivement le renseignement.

Mais malgré ces signes positifs, le renseignement n'était toujours pas une priorité, ni au niveau politique ni en termes de budget. Celui accordé aux services de renseignement dans le cadre de la loi de programmation militaire 2003-2008 ne constituait pas un objectif de premier rang. En dépit de l'augmentation des moyens depuis plusieurs années, les capacités restaient et restent d'ailleurs toujours en deçà de nos principaux partenaires.

Par rapport aux Forces Armées, depuis 2001 et même plus généralement depuis la chute du Mur, la réflexion sur l'avenir du renseignement français n'a pas été aussi fructueuse que ne l'espéraient les autorités compétentes. Tout comme pour le renseignement « classique » les améliorations certes réelles ont surtout concerné les moyens de collecte, plus que la redéfinition de l'architecture globale des services et les dirigeants politiques considèrent toujours que le renseignement ne fait pas partie de leur processus de décisions.

Malgré l'existence d'un plan de renseignement gouvernemental et d'un « *Comité Interministériel du Renseignement (CIR)* », aucune stratégie claire au niveau national n'était définie pour instaurer une véritable « communauté française du renseignement » qui serait concertée et coordonnée. Ce manque de vision globale a souvent empêché les différents acteurs français du renseignement de s'adapter entre eux aux nouvelles menaces, de telle sorte qu'il existe souvent aujourd'hui des chevauchements entre les fonctions, prérogatives et missions de ces organismes.

Toutes ces considérations sont restées valables jusqu'à 2008, et la publication du *Livre Blanc sur la Sécurité et la Défense Nationale*. C'est d'ailleurs la raison pour laquelle nous avons choisi d'employer « l'imparfait » pour parler du renseignement français dans les paragraphes précédents. Car en effet, depuis le début de l'année, et plus généralement depuis l'arrivée au pouvoir de Nicolas Sarkozy au printemps 2007, les choses ont changé et elles sont supposées le faire davantage dans les mois et années à venir.

Nous sommes encore à l'heure des discours et donc dans l'impossibilité d'évaluer véritablement l'efficience de tous ces projets tout juste en marche.

Cependant, et en restant au stade des textes et des intentions politiques, que peut on attendre du Livre Blanc, quelles perspectives s'ouvrent pour le renseignement français ?

2) Le Livre Blanc 2008 : une « révolution » pour le renseignement français ?

Rappelons brièvement le contenu du Livre Blanc dont nous avons détaillé la teneur dans le Chapitre 2 :

- Une amélioration de l'organisation et de la coordination de la communauté, notamment par la création de la DCRI. Mais aussi par la création du *Conseil National du Renseignement* (CNR) qui sera dirigé par le *Coordonateur National du Renseignement* et directement rattaché à la Présidence de la République.

- Une augmentation des ressources humaines et des moyens qui passera notamment par la refonte de la formation et du recrutement des personnels, et par des efforts budgétaires pour acquérir de nouveaux moyens d'interceptions techniques.

Ces mesures affichent clairement la nouvelle priorité gouvernementale accordée « au renseignement et à l'anticipation», laquelle sur le fond n'est contestée par personne et ne peut qu'aller dans le sens de ceux qui de longue date plaidaient et attendaient cette reconnaissance (du renseignement). En revanche, c'est sur les modalités voire la faisabilité que les critiques s'élèvent.

La DCRI (regroupement de la DST et des RG) apporte un exemple éclairant à cet égard, car même si elle ne résulte pas directement du Livre Blanc, elle entre pleinement dans le cadre général de la réforme.

Si sa création suscite dans son principe et son objectif des enthousiasmes, elle risque de se heurter sur le terrain à un certain nombre d'écueils :

- Comme lors de la mise en œuvre du *Department of Homeland Security* aux Etats-Unis après le 11 septembre 2001 (qui a accompagné, nous l'avons vu, une refonte plus ou moins profonde des agences de renseignements et de sécurité du pays), les

obstacles les plus importants relèveront très probablement et essentiellement du facteur « humain ».

La naissance du sigle DCRI signifie l'effacement de deux services emblématiques, en action depuis plusieurs décennies et de cultures très différentes. Si la préparation de cette fusion a duré près d'un an, pour rapprocher les points de vue, obtenir un certain aval des fonctionnaires et travailler en étroite collaboration avec les syndicats de police, sur le terrain l'adhésion n'est pas garantie et prendra du temps.

- C'est d'ailleurs la crainte d'incompatibilités entre ces deux entités « rivales » qui faisait dire à la Ministre de l'Intérieur le 9 juin 2007 dans les colonnes du Monde:

  « Nos services de renseignement ont des cultures différentes, les mettre dans un même lieu permettra d'améliorer leurs échanges (…). Je ne pense pas qu'à court terme, il soit possible ou utile d'aller au-delà. L'idée d'une fusion me paraît pour le moins prématurée… ».

La fusion effective à ce jour prétend additionner les talents et les savoir-faire, mais de nombreuses interrogations voire suspicions surgissent d'emblée :

- Elle entraîne l'exclusion du pôle de « renseignement intérieur » de 20% des agents des RG qui rejoignent ou rejoindront d'autres directions de la Police Nationale.

- C'est Bernard Squarcini, un proche de Nicolas Sarkozy et ancien directeur de la DST qui a pris la tête de cette nouvelle agence du renseignement intérieur. C'est pourquoi il est souvent dit en coulisse que la création de la DCRI résulte en fait de l'absorption pure et simple des RG par la DST, et non de la fusion des deux.

- De plus, même si l'émergence d'un seul interlocuteur devrait simplifier l'échange d'information, notamment avec les services étrangers, on peut aussi craindre, du moins dans les premiers temps, que ces derniers (ainsi que des Sources qui collaborent avec eux) se montrent réservés vis-à-vis de ces nouvelles modalités.

- Enfin et surtout, beaucoup d'observateurs pointent le fait que la DCRI - et au-delà, la réforme impulsée par le Livre Blanc - émanent plus de logiques et de motivations économiques que d'une volonté d'améliorer l'efficience du renseignement. En effet, en mutualisant les moyens (informatique, locaux, parc automobile etc.), en évitant les doublons et les gaspillages d'effectifs, des économies non négligeables seront réalisées sur toutes les dépenses de fonctionnement. Cette baisse notable des coûts ne peut soulever la désapprobation, mais à condition qu'elle ne s'avère pas à terme être la motivation principale de ces changements.

Théoriquement la DCRI dispose d'une multitude d'atouts pour devenir et s'imposer sans contestation possible comme la grande agence de renseignement intérieur du pays et continuer à faire de la France une référence de la lutte anti-terroriste au niveau international. Il est bien évident qu'un premier bilan ne pourra intervenir avant quelques mois, voire quelques années de fonctionnement.

Mais à l'heure où se lance ce chantier d'envergure, nous pouvons constater que la France, à travers la création de la DCRI, reste fidèle à l'adaptation et à l'anticipation sur le long terme.

Elle ose faire évoluer un système qui fonctionnait jusque-là correctement (pour preuve l'absence d'attentat islamiste sur notre sol depuis douze ans malgré de nombreuses tentatives), et construire un modèle plus moderne et plus approprié à contrer les « nouvelles menaces » et à déjouer les « futures » sans attendre qu'elles aient frappé.

Il est en effet préférable de ne pas avoir à tirer les enseignements et à faire les changements, après « l'explosion des bombes », mais plutôt de se préparer en amont.

À ce titre, si les promesses qui accompagnent la création de la DCRI peuvent être tenues dans la réalité, cette refonte justifiera sa raison d'être et, en dotant la France d'un renseignement fiable et efficient, elle participera à l'amélioration la lutte contre le terrorisme au niveau national et international.

De même, d'autres critiques s'élèvent, surtout concernant la forme des décisions impulsées par le Livre Blanc :

- Si les deux innovations que constituent la création du *Conseil National du Renseignement* (CNR) et celle du poste de *Coordonateur* sont très largement approuvées, le fait que l'un et l'autre soient directement rattachés auprès du Président de la République - et non pas au Premier Ministre ou aux ministères de l'Intérieur et la Défense dont relevaient jusqu'à présent la DST et la DGSE - soulève des inquiétudes et des critiques.

  Des voix dans l'opposition dénoncent le danger de concentrer ainsi le renseignement au service du Président tandis que d'autres observateurs voient ici un transfert trop important du renseignement vers l'Elysée et donc un éventuel problème en matière de contrôle. Ainsi Jean Pierre Maulny[104] énonce à ce propos : « *Concrètement on peut s'interroger sur la manière dont le contrôle sur la politique du renseignement sera opéré s'il y a un transfert de celle-ci vers l'Elysée […] il y a un risque évident d'opacité à transférer les déterminations des politiques publiques vers l'Elysée, non pas qu'il y ait une intention maligne dans ce projet, mais simplement parce qu'il n'y a pas d'administration qui puisse effectuer ce contrôle à l'Elysée* »[105].

[104] Chercheur français à l'*Institut des Relations Internationales et Stratégiques* (IRIS).
[105] Jean-Pierre Maulny, *Nicolas Sarkozy et la politique de défense : bilan d'un an de présidence,* IRIS, 30/4/08, 6p

Pour notre part et à ce jour, nous pensons que ce rapprochement vers le plus haut sommet de l'Etat semble attester de la meilleure reconnaissance accordée au renseignement et qu'en contrepartie de ce qui peut être vu comme une « centralisation », une délégation parlementaire au renseignement a été créée pour éviter d'éventuelles « dérives ».

- Nous ajouterons également que le *Coordonateur du Renseignement* n'aura aucune autorité hiérarchique sur les services - qui continueront de se référer à leur Ministre de tutelle - mais qu'il « *sera le point d'entrée des services de renseignement auprès du Président de la République* »[106].

- L'annonce de la priorité nouvelle donnée au renseignement doit être relativisée. En effet, malgré les augmentations de budget, d'effectifs, de moyens techniques, etc. : « *la DGSE le principal service français représente seulement 0.9% du budget de la défense, lequel représente moins de 2% du budget de l'Etat ! C'est bien peu pour une priorité nationale* »[107] et globalement, les mesures du Livre Blanc sont encore bien modestes par rapport aux besoins.

- Enfin, on peut regretter que le renseignement militaire, par le biais de la DRM, ne fasse l'objet d'aucune réforme, comme celle qui consisterait en un rapprochement avec la *Direction de la Protection et de la Sécurité de la Défense* (DPSD).

Pour conclure, nous dirons que le Livre Blanc augure des changements très importants pour le renseignement appliqué à la lutte contre le terrorisme en France. Mais il doit être envisagé comme le point de départ d'évolutions à moyen et long terme, et non comme un aboutissement.

Notre renseignement national certes se redresse mais ses moyens sont encore loin d'égaler ceux d'autres pays dans lesquels les budgets sont plus importants et/ou en continuelle hausse depuis plusieurs années.

Néanmoins, le Livre Blanc sur la Défense et la Sécurité Nationale de 2008 marque un réel tournant dans le sens où, pour la première fois il instaure le renseignement au centre du dispositif de Défense et crée les bases d'une véritable « communauté française du renseignement ».

Après avoir étudié jusqu'à maintenant, en très grande partie, les évolutions « passées » du renseignement, concentrons nous sur le futur.

Quelles perspectives sont envisagées et envisageables à moyen terme ?
Quels dangers sont susceptibles de concerner cette activité dans les années à venir ?

[106] *Ibid.* Livre Blanc, Op.cit. p 90.
[107] Eric Denécé, *Le renseignement plus que jamais une priorité nationale*, Le Figaro, 11/07 /08.

IV) Perspectives futures : privatisation, problèmes éthiques et nouvelles voies.

1) Contrôler l'externalisation du renseignement.

Comme nous l'avons dit précédemment l'externalisation ou la privatisation du renseignement est plus qu'une tendance, c'est une véritable réalité même si pour l'instant le phénomène est surtout limité aux Etats-Unis (mais il commence à se développer aussi en Grande-Bretagne et même en France).

Aujourd'hui entre 50 et 70% du budget du renseignement américain engagé dans la lutte contre le terrorisme irait à des entreprises privées.

Et si l'externalisation peut s'avérer bénéfique :

- Notamment par l'apport dans la collecte et l'analyse des millions d'informations issues de sources ouvertes, qui permet la réduction pour les agences gouvernementales des coûts des systèmes techniques, etc.,

Les « dangers » qu'elle comporte sont néanmoins importants :

- Externaliser peut engendrer indirectement l'absence de réforme pour les agences, la fuite des employés des agences gouvernementales vers des acteurs extérieurs, etc.

Mais aujourd'hui, le phénomène est tellement répandu qu'il est de plus en plus difficile de faire la distinction au sein des agences, entre ce qui est produit par le « public » et ce qui provient du « privé ».

Il faut donc trouver les bonnes méthodes de maitrise et de contrôle :

- Définir un cadre légal.

Une première piste doit être entrevue du côté de la mise en place d'un cadre législatif clair et respecté qui régirait scrupuleusement l'externalisation des activités du renseignement. Comme le mentionne Raphael Ramos[108], si la privatisation est aujourd'hui si importante aux Etats-Unis, on le doit en grande partie à la « faiblesse » de la législation.

En 1981, une directive présidentielle entérina la possibilité pour les agences gouvernementales du renseignement de passer des contrats avec des sociétés privées. Mais parallèlement, elle prévoyait que les « fonctions inhérentes au gouvernement » devaient rester l'apanage des employés fédéraux, et que les activités relevant de « l'action de gouverner » et impliquant « l'intérêt publique » ne pouvaient être externalisées.

Cependant, elle laissait le soin aux agences de déterminer elles mêmes quels domaines de leur activité pourraient être sous traités, et lesquels ne le pourraient pas…ce qui minimisa sa portée.

En 2000, un mémorandum du Pentagone chercha à clarifier la situation en indiquant que le renseignement tactique était par essence du ressort exclusif du gouvernement et que, compte tenu de leur importance pour la sécurité nationale, les activités relevant du renseignement stratégique ou opérationnel devraient elles aussi être « fermées » aux acteurs privés. Mais dans le même temps, ce document autorisait le recours à des sous traitants dans les cas où les moyens fédéraux s'avéraient insuffisants. Là encore, la porte de l'externalisation restait entrouverte.

De toute évidence - et les nombreuses « bavures » ou « dérives » survenues en Irak du fait de certains de ces acteurs privés l'ont démontré - il est nécessaire d'élaborer une législation bien plus claire et approfondie. Des travaux du Département de la Défense sont d'ailleurs en cours pour permettre une évaluation complète de la problématique. Mais pour le moment, aucun cadre légal ne définit aux Etats-Unis quelles activités peuvent être concernées par l'externalisation et selon quelles modalités.

- Contrôler l'externalisation par le bais « parlementaire ».

Le contrôle parlementaire du renseignement est indispensable pour encadrer et surveiller les activités des agences gouvernementales, mais il l'est d'autant plus lorsqu'il s'agit d'activités de renseignement menées par des acteurs privés. Et la aussi, on constate un « vide » en matière de mécanismes de contrôle. Aujourd'hui, et contrairement aux fonctionnaires du « public », les employés privés ne sont donc pas tenus de rendre des comptes sur leurs pratiques. Les autorités américaines semblent avoir pris conscience du « danger » et ainsi, en 2007, le Congrès à décidé par le biais de la loi de financement du renseignement, que pour l'année 2008, les agences de

[108] *Ibid.* Raphael Ramos, Op.cit. p53.

renseignement seraient contraintes de faire état des activités qu'elles ont externalisées et des coûts engendrés.

Ce n'est qu'avec la définition et le respect d'un nouveau cadre légal ainsi que le renforcement du contrôle parlementaire que le secteur privé représentera un réel apport pour les agences de renseignements fédérales, et qu'il pourra être envisagé comme une contribution largement positive.

Nous ne le développerons pas ici mais il nous faut néanmoins signaler qu'au-delà de la privatisation du renseignement, c'est le sujet plus général de la « mercenarisation » de tout le volet « sécurité et défense » américain (mais la tendance commence à se généraliser à d'autres pays) qui pose problème. Les employés de Sociétés Militaires Privées (SMP) représentent actuellement le deuxième contingent militaire étranger en Irak et leur nombre de cesse de croître sur tous les théâtres d'opération dans le monde. Et tout comme les sociétés spécialisées dans le renseignement, ces SMP sont à l'origine de bavures, utilisent des méthodes répréhensibles, etc., et ne sont soumises à aucun contrôle digne de ce nom.

2) Savoir gérer le nouvel environnement entre le renseignement, la société et le politique.

Si la place du renseignement a considérablement évolué au sein de la lutte contre le terrorisme depuis quelques années, elle a également beaucoup bougé au sein de la société.

Il s'agit désormais d'un élément absolument central pour la sécurité et la défense des Etats, ce qui lui octroie de fait de nouvelles responsabilités.

Aujourd'hui lorsqu'un attentat survient, les services de renseignement sont les premiers remis en cause non seulement par les autorités compétentes et les pouvoirs politiques mais aussi par tout un chacun. C'est là une caractéristique de nos sociétés qui depuis ces dernières années, se montrent de plus en plus sensibles en matière de sécurité individuelle et collective; elles sont aussi plus promptes à dénoncer les abus : le citoyen accepte de moins en mois bien les risques (qu'ils soient avérés ou potentiels) desquels il estime devoir être préservé, il supporte de moins en moins bien les dérives concernant l'éthique, le respect des libertés individuelles et des droits de l'homme. Il veut davantage de performance mais aussi de transparence pour les activités militaires en général, et le renseignement en particulier.

Ce dernier doit donc désormais s'adapter à ce nouvel environnement et intégrer :

- **L'exigence de transparence démocratique** qui se matérialise par la généralisation et le renforcement du contrôle parlementaire des services de renseignement, au sein de tous les Etats.

Pendant plusieurs décennies, le renseignement, sous prétexte qu'il oeuvrait dans un domaine clé pour la défense et la sécurité du pays, et n'avait de comptes à rendre qu'à l'exécutif.

Mais pour les raisons précédemment évoquées plus haut, il est aujourd'hui impensable que cette activité ne soit pas soumise à un contrôle en toute rigueur et clarté, du moins dans les pays démocratiques.

C'est donc pour cela que l'on a généralisé le contrôle parlementaire, qui selon les Etats, peut aller du simple « suivi », à la « supervision », voire dans certain cas jusqu'à un contrôle très étroit[109].

Dans certains pays, aux Etats-Unis en particulier, culturellement on entrevoit ce contrôle comme un gage de développement et de reconnaissance. A l'inverse, dans d'autres Etats - ce fut le cas par exemple pendant longtemps en France - il est davantage envisagé comme un frein, comme une contrainte pour l'activité des services.

Pourtant, le contrôle parlementaire du renseignement ne doit pas être uniquement envisagé sous un aspect de « surveillance », pour éviter d'éventuelles dérives. Il permet également aux élus de se familiariser avec cette activité, de comprendre pour quelles raisons elle est absolument vitale pour assurer la sécurité et la défense du pays et ainsi le vote des budgets nécessaire aux missions des services peut se faire plus facilement et plus abondamment.

Cependant, malgré la généralisation de ce contrôle, les dérapages existent toujours. Les interrogatoires à Guantanamo et Abou Ghraïb, ou encore les transferts extra judiciaires par la CIA de suspects sur le sol de pays européens, ont démontré qu'il existe toujours des déficiences dans ce domaine. Principalement parce que malgré l'amélioration du contrôle du renseignement, les rapports avec l'autorité politique ne sont toujours pas clairement clarifiés.

- **Le « nouveau » rapport avec le politique** qui repose sur trois réalités :

  - La menace terroriste a pris ces dernières années – et surtout depuis le 11 septembre 2001 - une importance considérable au sein des sociétés « occidentales ».

[109] *Ibid.* Eric Denécé Op.cit. p17.

- Le renseignement s'est vu parallèlement attribué l'un des rôles principaux dans la lutte contre le terrorisme et cette menace qu'il représente.

- Plus globalement, et en se détachant ici de la problématique du terrorisme, nos sociétés ont un besoin croissant de sécurité.

Le rapport entre le renseignement et le pouvoir politique s'est renforcé, ce qui a favorisé l'augmentation des budgets des agences, mais aussi fait peser sur ces dernières une plus grande pression.

Il s'agit là d'une évolution positive, sous réserve toutefois que l'autorité politique ne verse pas dans la « manipulation », ou l'abus de position…ce qu'elle tend à faire fréquemment.

Ainsi, les services se voient souvent imputés des torts ou des déficiences qui concernent en fait tout un système car ils ne peuvent pas ou difficilement « protester ». Ce fut le cas aux Etats-Unis après les attentats du 11 septembre 2001. Certes, les agences de renseignement avaient indubitablement leur part de responsabilité mais elles n'étaient pas les seules en cause.

Et lorsque l'autorité politique se sert directement des organismes de renseignement à des fins détournées, le danger est encore plus grand : en 2003, l'Administration Bush demanda à certains de ses services de fabriquer des preuves démontrant l'existence d'un programme d'armes de destruction massive en Irak et de liens avec Al-Qaida.

Au-delà de la condamnation purement « morale » ou « éthique » qu'elles inspirent, de telles pratiques ont eu pour effet de complètement discréditer l'activité des agences en question, mais également de ternir encore davantage l'image du renseignement dans son ensemble et dans le monde entier.

Il apparaît donc indispensable qu'elles cessent et/ou ne puissent définitivement plus avoir lieu.

3) Pratiquer un renseignement « éthique ».

Il s'agit d'un thème d'ailleurs directement connecté aux précédents, puisque nous l'avons vu, l'emploi de sociétés privées dans les domaines du renseignement et de la sécurité était très souvent associé à des pratiques « douteuses ».

Mais le débat est bien plus vaste : il concerne la guerre faite au terrorisme, les méthodes illégales utilisées en son nom et leurs conséquences en matière de violations des droits de l'homme et de valeurs démocratiques.

Les attentats du 11 septembre 2001 ont propulsé la lutte anti-terroriste au rang de priorité non seulement pour les Etats-Unis mais pour l'ensemble des dirigeants des pays occidentaux. Les différents gouvernements ont adapté leurs discours, réorganisé leurs politiques et leurs forces de sécurité et de défense, afin de mieux coopérer et d'être plus efficaces contre le radicalisme islamique. L'urgence et l'ampleur de cette « nouvelle menace » ont renforcé le rôle des services de renseignement et leur ont donné une place particulière : perçus comme les seuls à même de « prévenir et d'empêcher », de nombreuses mesures législatives et de restrictions des libertés furent alors adoptées pour faciliter leur travail, développer les échanges et assouplir les dispositifs juridiques qui les encadraient.

Au regard des résultats pour le moment très contrastés de la « Guerre contre le Terrorisme » impulsée par les américains depuis 2001, le principal questionnement est bien de se demander si elle ne se révèlera pas complètement contre-productive en générant indirectement plus de terroristes qu'elle n'en élimine.

La « *Global War on Terrorism* » est une « guerre » très médiatique et médiatisée, ostentatoire, visible…qui a pris cette tournure dès les premières déclarations des hauts dirigeants américains, au lendemain du 11 septembre.

Pour ce qui est du renseignement, le risque est d'aller au-delà des principes et limites pourtant propres à un Etat démocratique.

Pratiquer un « renseignement éthique » n'est pas seulement une obligation qui relève de l'aspect moral, c'est également un impératif pour ne pas décrédibiliser la lutte contre le terrorisme.

Le scandale de la prison irakienne d'Abou Ghraib et des interrogatoires menés de façons humiliantes et dégradantes eut par exemple un impact néfaste considérable. Il a contribué à la montée de l'animosité du peuple irakien envers les américains, puis dans un deuxième temps à la réalisation d'actions de plus en plus violentes.

Si cet épisode résulte d'un dérapage semble-t-il « isolé » de la part des américains, ses conséquences n'en demeurent pas moins dévastatrices et durables. Et il semblerait que les « bavures » et « infractions » se soient multipliées au cours de ces années.

Dans un autre registre, la mise en place de certains outils tels que le Patriot Act dans lesquels les prérogatives et les modalités sont mal définies, potentiellement sensibles et où l'absence

de mécanisme de contrôle peut donner lieu à certaines dérives ne fait qu'accroître le climat de suspicion, de méfiance tant à l'intérieur même du territoire concerné, qu'à l'extérieur. Certes, après sept ans d'existence, il a directement permis l'arrestation puis la condamnation de plus de 200 personnes impliquées dans le terrorisme. Mais de telles législations contribuent à maintenir un état de psychose et de tension quasi permanent et d'une certaine manière entrent dans le jeu des terroristes. Aucune limitation n'est vraiment explicite mais la peur des représailles ou d'être inquiétés a des effets inhibants sur les comportements. Les individus, d'origines étrangères, notamment d'Afrique du Nord et du Moyen-Orient, ou de confession musulmane tendent à être pointés du doigt, se sentent marginalisés, amalgamés.

On peut se poser des questions sur les incidences futures de la généralisation de ces pratiques, de tous les sentiments ou ressentiments qu'elles font naître au sein de la population et craindre que leurs effets soient à l'inverse de ceux escomptés.

Dans sa lutte contre le terrorisme (au niveau national) la première puissance mondiale se doit de rechercher et d'instaurer la sécurité bien légitime que ses habitants attendent mais sans stigmatiser voire humilier l'une ou plusieurs de ses communautés.

De même, les autres systèmes de renseignement/sécurité mis en place après 2001 dans le monde entier, notamment ceux utilisant les bases de données informatiques pour avoir accès à un certain nombre d'informations ayant trait à la vie privée des individus, posent nécessairement la question du respect des libertés publiques et individuelles.

Les révélations sur les transferts clandestins de simples « suspects », opérés par des agents de la CIA avec l'accord de certains pays, ou bien encore sur les écoutes de la NSA non seulement desservent la lutte contre le terrorisme, elles donnent aussi des justifications aux terroristes.

Par ailleurs, utiliser des soit disant « renseignements » comme le firent les américains lorsqu'ils justifièrent leur intervention en Irak par la présence d'armes de destruction massive, se révèle à long terme, extrêmement négatif.

Non seulement ce procédé a engendré des divisions à l'intérieur même des pays alliés, mais il a consolidé également un peu plus le sentiment d'impérialisme américain éprouvé par une partie de l'opinion mondiale et par la population des pays arabes en particulier. A terme le discours des terroristes n'en est que fortifié.

La « surcompensation » d'un acte terroriste par des directives éthiquement contestables est sans doute ce qu'espèrent et recherchent les leaders terroristes.

La responsabilité des Etats-Unis est grande, car ils sont le porte voix de l'Occident.

Mais les méthodes illégales ou les violations des libertés et droits individuels ne sont pas l'apanage des américains. C'est pourquoi on doit renforcer partout dans le monde les procédures de contrôles des activités de renseignement, dans leur acception la plus large. Car aujourd'hui la frontière est souvent très étroite entre le renseignement pur et les systèmes ou initiatives à vocations davantage sécuritaires.

La protection des droits de l'homme n'est en aucun cas un obstacle à la lutte effective contre le terrorisme. Au contraire, le respect des droits de l'homme, des libertés fondamentales et de la prééminence du droit sont des outils essentiels pour le combattre. En cas d'allégation crédible sur des dérives en la matière, les démocraties ne devraient jamais accepter d'invoquer le secret pour ne pas mener les enquêtes et les poursuites qui s'imposent.

Il faut réaliser l'équilibre entre les droits fondamentaux des personnes et le nécessaire besoin de sécurité. Mais dans beaucoup de cas, on ne l'a pas encore trouvé.

4) Quelques exemples d'évolutions futures.

Pour conclure ce travail, nous aborderons les évolutions futures, à court et à moyen terme, de l'activité du renseignement dans le cadre de la lutte contre le terrorisme, et plus généralement nous essaierons d'entrevoir son rôle en tant qu'acteur majeur pour la sécurité et la défense du territoire.

- **L'importance croissante du renseignement via les « sources ouvertes ».**

Ce type de renseignement est déjà très important, mais il devrait encore croître dans les années à venir, surtout dans le domaine militaire et de la lutte contre le terrorisme.

Jusqu'à maintenant, son utilité était surtout éprouvée dans les activités économiques. Par la consultation des sources ouvertes, on peut avoir accès à une multitude d'informations concernant des concurrents (identification des actionnaires et des gérants, obtention des CV de certains de ces gérants, indentification des employés, etc.)[110]. L'intérêt d'une telle démarche semblait cependant moins pertinente pour le renseignement ayant trait à la sécurité ou à l'activité militaire. Mais depuis que l'environnement global est caractérisé par l'imbrication des enjeux, notamment sur les théâtres d'opérations, le renseignement par source ouverte est devenu ici aussi un élément majeur.

Il faut aujourd'hui identifier, et du mieux possible, l'ensemble des acteurs d'une situation. Sur un théâtre d'opération, les forces sont confrontées désormais à la multiplication des intervenants, qu'il s'agisse des groupes armés, des ONG, des sociétés militaires privées (SMP), etc. Les sources ouvertes permettent donc non seulement de glaner des informations

[110] Jean-François Loewenthal, *Le renseignement via les sources ouvertes (OSINT) : une nouvelle discipline ?*, 6/01/08 : http://www.cf2r.org/fr/cyber-rens/le-renseignement-via-les-sources-ouvertes-osint-une-nouvelle-discip.php

sur ces acteurs précis mais également de se forger une connaissance « globale » de l'environnement.

Les sources ouvertes sont un excellent moyen pour constituer un canevas d'informations générales, avant de passer à la collecte par des moyens « non ouverts » qui apporteront des données plus précises. En ce sens, ces sources ouvertes ne sont pas à sous estimer et sont à envisager comme une étape préalable à toute recherche et acquisition plus ciblée. En 2006, Amnesty International rendait public un rapport sur les vols clandestins de la CIA transportant des présumés terroristes. Entièrement basé sur des sources ouvertes, il s'appuyait et exploitait des informations toutes consultables sur des sites Internet (permis accordés aux avions civils, données des vols internationaux par exemple). Ainsi, par des corrélations et recoupements, cette organisation a pu effectuer un travail et élaborer un document de synthèse que l'on aurait pu croire uniquement réalisable à partir de sources non ouvertes. C'est là une preuve qu'elles sont riches, utilisables et qu'elles ne doivent pas être écartées par le renseignement, mais au contraire intégrées en tant que possibilité de produire de l'information de qualité.

Cependant leur utilité dans la lutte contre les groupes « purement » terroristes semble plus limitée de par l'extraordinaire discrétion de ces groupes et de leurs activistes. En revanche, contre les groupes terroristes qui flirtent avec l'action armée, la guérilla, etc., et qui peuvent êtres combattus sur un théâtre d'opération, les sources ouvertes peuvent se révéler forts utiles.

Si la collecte des sources ouvertes ne pose plus de problème technique, la phase d'analyse, de recoupement de ces sources dispose, elle, d'une marge de progression importante. En effet, dans le flot de ces informations, repérer celles utiles est une nécessité mais c'est actuellement la difficulté principale.

C'est pourquoi des logiciels informatiques, laissant plus ou moins de place à l'intervention humaine ont été créés ces dernières années mais on attend d'autres développements informatiques qui permettront d'assurer une meilleure structuration des informations ainsi que leur harmonisation. Un des objectifs est la « *transcription automatique des conversations orales, la traduction automatique en de nombreuses langues, l'identification automatique des noms propres et des liens existants entre les personnes, etc.* »[111].

Ces nouveaux outils ne resteraient pas spécifiques et cantonnés aux sources ouvertes mais ils profiteraient à tous les types de sources d'informations et en optimiseraient l'exploitation.

Des réticences sont encore présentes au sein de la communauté de renseignement à l'égard de ces sources ouvertes parce que « *ce qui s'obtient trop facilement au goût de l'ancienne école est entaché de suspicion, de peur de faire l'objet d'une manœuvre d'intoxication. Ensuite, le succès à longtemps été mesuré à l'aune de ce que découvrait un service et qui ne l'était pas par les autres. L'accès libre à l'information remet en cause ce paradigme de façon assez déstabilisante* »[112].

---

[111] *Ibid.*

[112] Gaël Marchant, *L'évolution du renseignement vers les sources ouvertes*, 03/05/08 http://librairie.territorial.fr/PAR_TPL_IDENTIFIANT/31126/TPL_CODE/TPL_ACTURES_FICHE/PAG_TITLE/L'%E9volution+du+renseignement+vers+les+sources+ouvertes/302-actu.htm

Mais globalement toutes les agences s'y mettent. Aux Etats-Unis, le DNI a créé un *Open Source Center* au sein de la communauté de renseignement et l'idée d'une *Open Source Agency* est également défendue par certains, au motif que seule une agence indépendante serait à même d'organiser des échanges avec des organismes civils détenteurs d'informations mais qui hésitent à collaborer avec des services de renseignements. Ce serait là aussi un moyen de capter l'ensemble de l'information disponible dans le monde et de la diffuser.

- **La nouvelle tendance de l'*Intelligence-Led Policing* (ILP).**

C'est l'un des faits les plus marquants qui démontre l'importance croissante du renseignement pour la sécurité des Etats. Car en effet, ce terme d'*intelligence-led policing* (ou ILP) que l'on pourrait traduire par « *renseignement criminel de sécurité* »[113] est une doctrine anglo-saxonne qui définit une police de proximité dont le fonctionnement repose directement sur le renseignement.

Elaborée dans les années 90 en Grande-Bretagne, elle part de l'idée que la police perd trop de temps et consacre une trop grande partie de ses moyens à des situations d'urgences. Pour inverser la tendance, cette dernière doit donc privilégier la prévention de la délinquance par une place prépondérante accordée au renseignement.

Le bon fonctionnement de cette doctrine impose la diversification des sources de renseignements, la recherche de l'information n'est plus seulement l'apanage des services spécialisés mais surtout le renseignement ne doit plus être envisagé seulement comme un appui à la machine policière, il prend désormais un rôle d'orientation : « *les informations précèdent et orientent les actions de police administrative et judiciaire et non l'inverse* »[114].

Mais au-delà de la répression de la délinquance au quotidien, l'ILP peut représenter un véritable apport pour la lutte anti-terroriste. Les Etats-Unis l'ont précisément développée dans cette optique depuis les attentats du 11 septembre. Elle pourrait devenir dans le futur un des moyens privilégiés pour identifier les réseaux et, en raison de son caractère « préventif », s'avérer contre ces derniers plus efficace que les stratégies actuelles basées sur une approche répressive.

En outre, en concevant et en intégrant l'activité de renseignement au sein de la police, l'ILP tend à effacer la limite entre l'extérieur et l'intérieur, et s'inscrit donc parfaitement dans la nouvelle notion de « sécurité globale ».

Cependant, dans le cadre de la lutte anti-terroriste l'ILP demande la mise en place de moyens couteux, les résultats sont souvent invisibles et attendus sur le long terme, mais surtout cela peut se faire au détriment des autres missions « classiques », ce qui n'encourage pas les autorités politiques à s'orienter significativement vers ce type de police.

---

[113] Gaël Marchant, *Intelligence-led policing : stratégie policière ou mission de renseignement ?*, 15/07/07 : http://www.cf2r.org/fr/notes-de-reflexion/intelligence-led-policing-strategie-policiere-ou-mission-de-renseigne.php

[114] *Ibid.*

Enfin, ce système assez lourd doit nécessairement s'accompagner d'un plan national pour le renseignement et suppose de faire évoluer les structures et les prérogatives inhérentes à cette activité.

Et pour le moment, seul les Etats-Unis et la Grande-Bretagne se sont intéressés de façon effective à ce concept.

Conclusion Générale :

Le 11 septembre 2001 a représenté un énorme choc pour le monde entier. L'ampleur des destructions, le nombre de morts, mais également l'impact psychologique faramineux, ont donné à cet événement un caractère encore inédit qui propulsa le terrorisme, et surtout la lutte contre le terrorisme au premier rang des priorités internationales.

Comme nous le savons, les ripostes aux attentats s'organisèrent autour des interventions militaires américaines dans le cadre de la « Guerre contre le terrorisme » : en Afghanistan puis en Irak mais également dans beaucoup d'autres régions du monde.

Mais au-delà de ces actions d'envergure, une réflexion d'ensemble s'amorça pour tenter d'entrevoir les raisons de l'incapacité des autorités américaines à anticiper et empêcher ces attaques.

Le renseignement et les déficiences quant à sa transmission émergèrent très clairement comme les éléments majeurs de cette faillite. Mais surtout le 11 septembre apparut comme le symbole d'un monde qui avait considérablement changé depuis la Chute du Mur au début des années 90.

Ces attentats marquèrent donc l'échec des services de renseignement et de sécurité qui n'ont pas pu appréhender un évènement particulier (le 11 septembre), et qui au-delà, n'ont pas su s'adapter correctement à la nouvelle donne de ce monde post-Guerre Froide.

Dans ce nouvel environnement, caractérisé par des menaces désormais transnationales et émanant d'acteurs le plus souvent non étatiques, le renseignement prend une importance considérable pour les entités chargées d'assurer la défense et la sécurité des Etats, et notamment dans le cadre de la lutte contre le terrorisme. Des changements s'imposaient et ils ont été entrepris un peu partout dans le monde depuis 2001.

Les Etats-Unis, tout en ne remettant pas en cause l'existence des principales agences de renseignement (CIA, NSA, FBI, DIA, etc.) leur ont octroyé des moyens bien supérieurs à ce qu'ils étaient dans le passé dans le domaine du contre terrorisme et du renseignement. Mais surtout ils ont créé le poste de *Director of National Intelligence* (DNI) dans le but d'instaurer un véritable échange et partage des informations en interne, mais également en externe avec les services étrangers. Après la mise en place du *Department of Homeland Security* (qui concerne la sécurité et défense du territoire dans son aspect global) le DNI vint confirmer la volonté américaine de fédérer véritablement les agences de renseignements. Et il en fut encore de même au travers du 500 Day Plan.

En France, le Livre Blanc sur la Sécurité et la Défense Nationale de 2008 traduit de toute évidence une évolution certes plus tardive mais qui va dans le sens de celle opérée aux Etats-Unis. Avec la création du poste de *Coordonateur National du Renseignement* mais aussi de la DCRI (rassemblement des RG et de la DST) on ne bouleverse pas fondamentalement le système national du renseignement au niveau de la collecte, mais on cherche à assurer une meilleure communication entre les entités concernées pour qu'elles fonctionnent et travaillent

réellement en « communauté » et ne laissent pas échapper des informations qui pourrait se révéler capitales.

A des degrés différents, les changements impulsés dans ce domaine par l'ONU, l'OTAN et l'Union Européenne après les attentats de New-York et Washington, ont été de même nature que ceux pratiqués par les Etats-Unis et la France. Si les crédits ont été augmentés, si les moyens et les sources du renseignement ont été la plupart du temps diversifiés et améliorés, aucune évolution ne s'est produite en matière de collecte. En revanche on a, dans tous les cas, accordé une attention particulière et fait des efforts importants pour permettre et optimiser le partage et l'échange des renseignements collectés.

Car le 11 septembre n'a pas révélé l'insuffisance des services à « acquérir » des informations mais leur impossibilité à se les transmettre correctement et donc à les recouper de façon à anticiper et prévenir les attentats.

Mais d'un point de vue général, quelle conclusion, quel bilan peut-on tirer des évolutions ayant touché le renseignement dans le cadre de la lutte contre le terrorisme depuis ces évènements ?

Dans bien des cas, des progrès certains ont été réalisés et globalement la place du renseignement est meilleure aujourd'hui qu'elle ne l'était il y a quelques années. Non seulement ce dernier est probablement aujourd'hui le pilier numéro 1 de la lutte contre le terrorisme, mais au-delà, il est devenu l'un des éléments majeurs pour la défense et la sécurité des Etats. On a compris que le renseignement constituait probablement le meilleur rempart contre les nouvelles menaces qui se sont développées à partir de la fin de la Guerre Froide.

Mais bien souvent les voies entrevues et tracées sur le plan théorique n'ont pas pu être menées à bien dans la réalité, ou du moins n'ont pas été complètement à la hauteur des attentes suscitées, essentiellement en raison des réticences ou des lenteurs au sein des administrations ou des bureaucraties.

Plusieurs exemples peuvent être cités à l'appui de ce constat. Le plus parlant est sans doute celui des Etats-Unis qui voient leur détermination à vouloir constituer une communauté de renseignement se heurter au gigantisme et à l'immobilisme des agences y participant. Et en tout état de cause, la vitesse d'adaptation des plus réactives reste inférieure à celle du terrorisme.

Une autre illustration nous est donnée par l'Union Européenne : de nombreuses entités destinées au partage du renseignement existent. Depuis le 11 septembre 2001 mais davantage encore après les attentats de Madrid (2004) et Londres (2005), des actions ont été entreprises ou poursuivies pour améliorer les outils existants, et les Etats membres s'accordent sur l'utilité et surtout sur la nécessité d'un partage optimal de l'information pour empêcher que les terroristes ne fomentent des opérations.

Néanmoins, cette étape demeure à un stade « basique », en raison d'incompatibilités techniques mais plus encore par peur de remettre en cause la souveraineté étatique chère au pays européens.

Et l’on touche ici au thème central qui conditionne une très grande partie de l’activité du renseignement et qui limite son efficacité au sein de la lutte contre le terrorisme, à savoir sa relation avec la sphère politique.

Dans l'ensemble, les services mondiaux disposent d'outils suffisants et adéquats pour lutter contre les réseaux et les activistes sachant que les moyens et ressources de ces derniers sont souvent inférieurs à l'idée que l'on s'en fait et en tout cas moindres que ceux que peuvent mobiliser les agences de renseignement.

Il est vrai que cette dissymétrie des moyens fait la « force » des terroristes, mais malgré les difficultés qu’il faut surmonter, les services de renseignements ont tout ce qu’il faut pour les repérer et les combattre.

Mais c’est ensuite la relation entre la sphère politique et le renseignement qui fait la différence, et parfois altère les résultats. Le 11 septembre nous a en effet appris que le renseignement n’est d’aucune utilité s’il n’est pas correctement analysé puis diffusé et qu'accroître les capacités de collecte restera vain si l’exploitation qui en est faite est inadaptée ou si les orientations politiques ne suivent pas.

Ainsi les milliers d’analystes et d’agents de la CIA ou bien les gigantesques capacités techniques de la NSA verront toujours leur efficacité amoindrie si l’autorité politique n’est pas en mesure d'imposer et d'organiser le partage des informations collectées au sein de la « communauté », ou bien si cette même autorité politique décide de s’orienter vers des outils, moyens ou politiques qui ne seraient pas conformes aux objectifs recherchés.

La trop grande spécialisation vers un renseignement d’origine technique, ou la tendance actuelle à l’externalisation ont représenté et représentent encore des dangers liés avant tout à des décisions prises au niveau politique et qui ne proviennent donc pas des agences et structures du renseignement en tant que telles.

Bibliographie :

Ouvrages :

- Baud.J, *Encyclopédie des terrorismes et violences politiques*, Lavauzelle collection Renseignement&Guerre secrète, 2003, 752p.
- Baud.J, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 2002, 741p.
- Baud.J, *Le renseignement et la lutte contre le terrorisme*, Lavauzelle, 2005, 404p.
- Carroué.L, *Géographie de la mondialisation* (3ème édition), Armand Colin, 2007, 295p.
- *Défense et Sécurité nationale – Le livre blanc*, Odile Jacob, 2008, 350p.
- Delamotte.B, *Le renseignement face au terrorisme*, Editions Michalon, 2004, 133p.
- Géré.F, *Pourquoi le Terrorisme ?*, Larousse, 2006, 160p.
- Guelton.F, *Pourquoi le renseignement ? De l'espionnage à l'information globale*, Larousse, 2004, 152p.
- *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La documentation française, 2006, 135p.

Rapports/Mémoires :

- CHEM – CEREMS, *Terrorisme : Histoire et enjeux européens*, 2005, 40p.
- Coomans.M, *Non state actors : nouveaux acteurs dans le cadre de la globalisation*, Sécurité et Stratégie, Mai 2006, 46p.
- Commission de Défense (M. Lemoine), *Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil*, Juin 2002, 25p.

- Dasquié.G, *Quels outils et méthodes utilisés aux Etats-Unis et au Canada pour procéder à l'analyse stratégique du renseignement de sécurité intérieure ? Comparaison des agences de renseignement de ces deux pays (organisation, missions, moyens, efficience)*, 2004, 67p.

- *DNI annual threat assessment – statement for the record, Senate Select Committee on Intelligence,* fevrier 2008, 45p.

- Frémion.Y, *Avis présenté au nom de la commission de la défense nationale et des forces armées sur le projet de loi de finances pour 2005, TOME III : Défense, Espace, Communications et Renseignement*, octobre 2004, 31p.

  http://www.assemblee-nationale.fr/12/budget/plf2005/a1867-A03.asp

- IHEDN, *Etats défaillants et terrorisme*, 57ème session nationale, avril 2005, 31p.

- INHES, *Reconstruire la sécurité après le 11 septembre*, Les cahiers de la sécurité intérieure, 2004, 303p.

- Laumonier.I, *Internet sous l'œil des services de renseignement – Mythes et réalités*, Mémoire de DEA Technologie, Communication et Pouvoir, Université Paris I, 2003, 125p.
-
- Ministère de la Défense, *La Défense contre le terrorisme : une priorité du ministère de la Défense*, avril 2006, 48p.
-
- Nesterenko.M, *Une guerre nouvelle a commencé. Internet : un nouveau champ de bataille. Le terrorisme à l'épreuve de l'informatique*, 2002, 151p.

- OTAN, *Concept militaire de l'OTAN relatif à la défense contre le terrorisme*

  http://www.nato.int/docu/terrorisme-f.htm

- *Renseignement*, Politique Internationale n°102, 2004, 511p.

- Tenet.G, *Written Statement for the Record of the Director of Central Intelligence Before the National Commission on Terrorist Attacks Upon the United State*, 24 mars 2004.

  http://www.9-11commission.gov/hearings/hearing8/tenet_statement.pdf

- *Testimony of the Honorable Tim Roemer, Center for National Policy, Before the House Permanent Select Committee on Intelligence Subcommittee on Intelligence Community Management*, 6/12/2007.

  http://www.cnponline.org/ht/display/ContentDetails/i/2418

- *500 DAY PLAN – Integration and Collaboration*, United States Intelligence Community, 2007, 17p.

  http://www.dni.gov/500-day-plan.htm

Articles/Notes:

- Bauer.A et Rocard.M, *Pour un Conseil de sécurité nationale*, Défense Nationale et Sécurité Collective, 2007, 10p.
- Bonelli.L, *France, Grande-Bretagne, Espagne, les suspects font désormais office de coupables. Quand les services de renseignement construisent un nouvel ennemi*, Avril 2005, 8p.
- Cadène.N, *Livre Blanc sur la défense et la sécurité nationale*, 2008, 2p.

  http://debatsocialiste.blogspirit.com/archive/2008/06/17/livre-blanc-sur-la-defense-et-la-securite-nationale.html
- Cécile.J-J, *Internet. Outil de renseignement pour terroristes ?*, Histoire mondiale des conflits n°16, octobre 2004, 66p.
- Chevallier-Goven.C, *La lutte contre le terrorisme au sein de l'Union européenne*, Arès, Volume XXII, Décembre 2005.
- Chouet.A, *Questions du journal « Midi libre »*, Midi Libre, 8/4/2007, 5p.
-
- Choux.M, *Le renseignement stratégique de l'OTAN*, Défense Nationale n°7, Aout 2001, 2p.
- Clair J-F, *11 septembre 2001 : un choc pour la communauté internationale du renseignement*, Défense n°107, septembre-octobre 2003, 68p.
- Cogan.C et Pochon.J-P, *La réorganisation des services de renseignement face aux défis des nouvelles menaces*, Ecole de Guerre Economique, 12/4/2007, 3p.
-
- Colard.D, *Le rôle de l'ONU, du G8 et de l'OTAN dans la coopération internationale contre le terrorisme*, Arès N°56, Volume XXII, Décembre 2005, 12p.
- *Comment la CIA épie le financement du terrorisme*, Le Figaro, 23/6/08, 2p.
-
- Debril.C et Soubeyran.B, *Le renseignement français face aux menaces terroristes*, Défense n°119, janvier-février 2006, 66p.

- Denécé.E, *Le renseignement français au milieu du gué*, CF2R, décembre 2005.
- Denécé.E, *Le renseignement plus que jamais une priorité nationale*, Le Figaro, 11/07 /08.
- Denécé.E, *La révolution du renseignement*, CF2R, 2008, 13p.
- De Barmon (Lieutenant-colonel), *La fonction renseignement*.
-
- De Jonge Oudraat.C, *Le conseil de sécurité de l'ONU et la lutte contre le terrorisme*, 2005, 14p.
-
- De Weck.H (Colonel), *Renseignement, terrorisme, contre-terrorisme et anti-terrorisme*, 5p.
-
- Diefenbacher.M et Frémion.Y, *Le budget 2008 du renseignement fra*nçais, 2007, 12p.

  http://www.voltairenet.org/article153693.html
- D'Orcival.F, *Renseignement contre hyperterrorisme*, Le Spectacle du monde n°505, octobre 2004, 96p.
- Klen.M, *Renseignement humain et terrorisme*, Défense Nationale, n°4, Juin 2002, 182p.
- Gagnon. B, *Les opérations contre-terroristes et anti-terroristes reseaucentriques (OCAR)*, Défense et Sécurité Internationale, n°17 juillet 2006.
- Gautier.L, Lamy.F et Quiles.P, *Le livre blanc de la défense fait-il fausse route ?*, Le Figaro 5/3/08, 2p.
- Général de Division Fleury, *Terrorisme et renseignement terrestre*, Doctrines n°9, Juin 2006, 4p.
- Grondin.D, *Vers une nouvelle centralisation du renseignement*, Observatoire sur les Etats-Unis, Chaire Raoul-Dandurand, 4p.
- Groupe Surcouf, *Le livre blanc de la défense : une espérance déçue*, 18/06/08, 4p.
- Guerrier.P, *Cyber-terrorisme : comment la DST surveille l'islamisme radical sur Internet*, 7/4/2007, 2p.
- Hayez.P, *Renseignement européen : l'impensable dimension*, IRIS, 18 /06/08, 3p.
- Henrotin.J, *Cessez de respirer, nous pourrions être attaqués*, 9/01/08, 3p.
- Junghans.P, *La nouvelle délégation parlementaire au renseignement va-t-elle améliorer l'efficacité des services ?*, Sécurité globale, Eté 2008, 12p.

- Lassere.I, *La France redéfinit sa stratégie de défense*, Le Figaro, 16/5/08, 2p.
- *La lutte contre le terrorisme islamiste*, Le Monde Dossier et Documents, Juillet 2007.
- *La sécurité internationale sans les Etats*, La Revue Internationale et Stratégique n°49, Mars 2003.
- Lepri.C, *Quelle réforme pour quels services de renseignement ?*, IRIS, 2007, 13p.
- *Le renseignement au cœur des nouvelles priorités stratégiques*, 16/06/08, France 24, 2p.

  http://www.france24.com/fr/20080616-renseignement-nouvelles-prioritesstrategiques-defense-elysee-livre-blanc
- Marchand.G, *L'évolution du renseignement vers les sources ouvertes*, 03/05/08.

  http://librairie.territorial.fr/PAR_TPL_IDENTIFIANT/31126/TPL_CODE/TPL_ACTURES_FICHE/PAG_TITLE/L'%E9volution+du+renseignement+vers+les+sources+ouvertes/302-actu.htm
- *Livre blanc sur la défense : deux des auteurs s'expliquent*, Le Monde, 18/6/08, 3p.
- Loewenthal.J-F, *Le renseignement via les sources ouvertes (OSINT) : une nouvelle discipline ?*, 6/01/08 :

  http://www.cf2r.org/fr/cyber-rens/le-renseignement-via-les-sources-ouvertes-osint-une-nouvelle-discip.php
- Marchand.G, *Intelligence – Led policing : Stratégie policière ou mission de renseignement ?*, CF2R, 2007, 2p.
- Marchand.G, *Ouverture de la première académie de l'antiterrorisme à Los Angeles*, Note d'actualité n°123, CF2R, Mars 2008, 3p.

  http://www.cf2r.org/fr/notes-de-reflexion/intelligence-led-policing-strategie-policiere-ou-mission-de-renseigne.php
- Martin.D, *La réforme des services de renseignement civils français*, Sécurité globale, Eté 2008, 11p.
- Maulny.J-P, *Nicolas Sarkozy et la politique de défense : bilan d'un an de présidence*, IRIS, 30/4/08, 6p.
- Moniquet.C (propos recueillis par Beck.D), *La frontière est extrêmement poreuse entre le renseignement et le mercenariat*, Septembre 2002, 12p.

  http://www.cyberscopie.info/pages/art_entre/art10_entre.html

- Negroponte.J, *Les services de renseignement sont mieux préparés*, The Washington Post, 10/11/06, 3p.
- Palluault.O, *Le 11 septembre 2001, une rupture dans la pratique de l'anti-terrorisme*, Technologie et Armement, 2005.
- Poucet.E (Colonel), *Le renseignement de source humaine, espoirs et problèmes*, Doctrines N°09, Juin 2006, 4p.
- *Pour une politique de renseignement*, Le Figaro, 6 /03/08, 2p.
- *Privatisation toujours…le renseignement US*, 1/8/07, 2p.

  http://www.dedefensa.org/article.php?art_id=4281
- Ramos.R, *Externalisation du renseignement : l'exemple des Etats-Unis*, ESISC, Décembre 2007, 10p.
- *Renseignement : L'Espagne met le paquet sur le Maroc*, 12 décembre 2006.

  http://www.spyworld-actu.com/spip.php?article3220
- *Renseigner pour les forces*, Doctrine n°9, 2006, 119p.
- Santo.S, *L'ONU face au terrorisme*, Groupe de Recherche et d'Information sur la Paix et la Sécurité (GRIP).
- Schmitt.R, *FBI is called slow to join the terrorism fight*, Los Angeles Times, 9/05/2008.

  http://latimes.com/news/nationworld/nation/la-na-intel9-2008may09,07865641.story
- Staub.J-P, *Renseignement de sécurité, un défi pour le renseignement d'intérêt militaire*, Défense Nationale, Janvier 2008, 8p.

Autres :

- Assemblée Nationale (Marc Francina), *Rapport au nom de la commission de la Défense Nationale et des forces armées sur le projet de loi (n°2277 rectifié) modifiant les articles 414-8 et 414-9 du code pénal*, Janvier 2007, 14p

  http://www.assemblee-nationale.fr/12/rapports/r3648.asp

- Déclaration du Sommet de Riga, 28 et 29 novembre 2006 :

  http://www.nato.int/docu/pr/2006/p06-150f.htm

- LOI n°2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* :

  http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124&dateTexte=

- LOI n° 2007-1443 du 9 octobre 2007 *portant création d'une délégation parlementaire au renseignement* :

  http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000252177&dateTexte=

Sites Internet :

- *Central Intelligence Agency* (CIA) :

  https://www.cia.gov/

- *Director of National Intelligence* (DNI) :

  http://www.dni.gov/

- *Federal Bureau of Investigationon* (FBI) :

  http://www.fbi.gov/

- *National Security Agency* (NSA) :

  http://www.nsa.gov/

- *Organisation des Nations Unies* (ONU) :

  http://www.un.org/french/

- *Organisation du Traité de l'Atlantique Nord* (OTAN) :

  http://www.nato.int/home-fr.htm