L'UNION EUROPÉENNE ET LE RENSEIGNEMENT

PERSPECTIVES DE COOPÉRATION ENTRE LES ÉTATS MEMBRES

Thierry Coosemans

rue Van Hoorde, 33
B-1030 Bruxelles

Tél.: +32.2.241.84.20
Fax: +32.2.245.19.33
Courriel : admi@grip.org
Internet : www.grip.org

Sommaire

Introduction

Le 11 septembre 2001 révéla une menace nouvelle, d'une ampleur inégalée que François Heisbourg qualifia « d'hyper-terrorisme ». Impressionnés tant par le déchaînement de violence que par l'incapacité des Etats-Unis – unique puissance mondiale que l'on croyait intouchable – à en prévenir la manifestation sur son propre territoire, les dirigeants de l'Union Européenne s'engagèrent, la main sur le cœur, à lutter de concert. L'opinion publique y trouva matière à se rassurer. Mais deux ans plus tard, si des progrès substantiels ont été réalisés en matière de « justice et d'affaires intérieures » (mandat d'arrêt européen, renforcement d'EUROPOL, création d'équipes d'enquête communes), force est de constater que « l'Europe du renseignement » reste à la traîne.

La présente étude entend s'inscrire pleinement dans cette perspective d'intégration européenne, sans naïveté ni faux-fuyants. Nulle intention de promouvoir, envers et contre tout, une « Europe du renseignement » – *en sautant comme un cabri* – pour reprendre l'expression de cet Homme d'Etat qui connut bien les Services.

Notre approche se veut prudente et réaliste. Si la nécessité d'un approfondissement de la coopération au sein de l'UE constitue effectivement notre postulat de base, nous n'avons d'autre ambition que d'établir un certain nombre de scénarios, qu'il appartiendra aux responsables politiques, mais aussi aux professionnels du renseignement, de débattre.

Le premier chapitre vise à rappeler au lecteur un certain nombre de définitions et de concepts nécessaires à une bonne compréhension de la problématique du renseignement, appréhendée dans toute sa diversité. Le second chapitre établit un état des lieux de la coopération européenne en matière de renseignement au lendemain du 11 septembre. Le troisième chapitre développe les conditions selon nous préalables à un approfondissement de la coopération entre SR.

Nos conclusions s'efforceront de replacer l'approfondissement de la coopération entre SR de l'UE dans la perspective plus vaste du défi d'un nouvel environnement et d'une nouvelle finalité du renseignement.

I. Éléments de compréhension du renseignement

1. Le renseignement au cœur du processus de décision

Un officier de renseignement nous confia un jour, par boutade, qu'il exerçait « le plus vieux métier du monde » car avant de rejoindre Eve, Adam eut préalablement à s'informer de l'endroit où elle se trouvait.

Plus sérieusement, nul ne contestera que le renseignement occupe une place centrale dans tout processus de prise de décision : *au cours des siècles, les décideurs prudents - gens d'affaires, militaires, politiques, économistes - ont cherché à se tenir pleinement au courant des moyens et des intentions des personnes ayant des intérêts semblables ou opposés aux leurs. Il est relativement plus facile de s'informer sur ses amis et alliés, et plus difficile de le faire au sujet de ses rivaux. Mais les deux ensembles de renseignements sont nécessaires à la prise de décisions propres à protéger et favoriser au mieux ses propres intérêts.*[1] Et plus que jamais, *dans un système de tensions à l'échelle planétaire, les décideurs doivent avoir une connaissance poussée de leur environnement, des perspectives d'évolution de celui-ci, des opportunités qui s'y présentent, mais également des menaces qui les guettent, et ce quasiment en temps réel. La maîtrise de cette information est devenue impérative pour la survie des nations comme l'était déjà pour celle des entreprises.*[2] En somme, pour reprendre l'aphorisme d'Auguste Comte, il faut *« savoir pour prévoir afin d'agir ».*[3]

Trois arguments au moins plaident en effet, selon nous, en faveur d'une approche européenne de la sécurité.

D'une part, la criminalité organisée a pris une dimension multiforme : les trafics de drogues, d'armes, d'êtres humains, le blanchiment des capitaux ne sont que quelques exemples auxquels les événements tragiques du 11 septembre nous obligent d'ajouter la menace « hyper-terroriste ». Et déjà les experts évoquent le spectre du bio-terrorisme ou du cyber-terrorisme.

D'autre part, le phénomène de mondialisation, l'avènement du « village global » où personnes, marchandises et capitaux circulent à une vitesse accélérée, donne à la criminalité organisée une dimension nouvelle qui nous contraint de réviser nos stratégies tant préventives que répressives.

Enfin, les attentats de New York et de Washington nous ont fait prendre conscience que la distinction jadis établie entre notre « sécurité intérieure » et notre « sécurité extérieure » n'était plus pertinente. Seule une approche globale, menée au niveau de l'Union Européenne, est capable d'appréhender le problème dans sa nouvelle dimension.

Une étude de l'Institut d'Etudes de Sécurité de l'UEO posait déjà en décembre 1998 ce constat fondamental : *le renseignement revêt aujourd'hui beaucoup plus d'importance que pendant la guerre froide. Alors qu'il fallait naguère maintenir l'équilibre de la terreur, empêcher une guerre en Europe et être attentif à tout ce qui pouvait provoquer une confrontation politico-militaire dans le tiers monde, le rôle du renseignement est à l'heure actuelle beaucoup plus vaste et plus varié dans la mesure où il aide les responsables à orienter leurs politiques vers un nouvel ordre mondial, de nouveaux équilibres de la puissance et des environnements économiques différents, tout en évitant les risques traditionnels ou plus récents.*[4]

Mais le renseignement ne pourra jamais tout prévoir, tout anticiper. La plupart du temps, il se limitera à élaborer des scénarios en évaluant leur degré de probabilité. Il ne rendra malheureusement pas notre monde plus juste, ni nos gouvernants plus sages, comme le note Michael Herman[5].

2. Le cycle du renseignement

Il est généralement admis que le respect du « cycle du renseignement » constitue un fondement essentiel à la définition et à la mise en œuvre d'une politique de renseignement efficiente[6]. Ce cycle se caractérise par un processus

1. SEABORN Blair, « *Renseignement et politiques : constantes et évolution* », in Commentaire n° 45, Publication du Service Canadien du Renseignement de Sécurité, juin 1994, www.fsa.ulaval.ca/personnel/vernag/
2. http://www.geocities.com/Pentagon/7209/rma.html
3. http://www.geocities.com/Pentagon/7209/recherche.html
4. BECHER Klaus, MOLARD Bernard, OBERSON Frédéric et POLITI Alessandro, « *Vers une politique européenne de renseignement* », Les Cahiers de Chaillot, Institut d'Etudes de Sécurité de l'UEO, Paris, Décembre 1998.
5. HERMAN Michael, « *Sharing Secrets* », The World Today, The Royal Institute of International Affairs, Volume 57, Number 12, December 2001
6. WALDEN Alexander, « *Le renseignement humain face au développement des nouvelles technologies* », Mémoire de DEA, Droit mention « Défense nationale et sécurité

en quatre étapes (la planification, la collection, l'exploitation, la diffusion), chacune d'elle révélant une fonction particulière, et devant se concevoir dans un continuum temporel aussi appelé «boucle du renseignement». L'OTAN le définit comme *une séquence d'opérations par lesquelles les renseignements bruts sont obtenus, regroupés, transformés en renseignement et mis à la disposition des utilisateurs. Ces opérations comprennent :*

- *L'orientation - Détermination des besoins en renseignement, établissement du plan de recherche, envoi de demandes de renseignement et d'ordres de recherche aux organismes de renseignement et contrôle permanent de la production de ces organismes.*
- *La recherche - Mise en oeuvre des sources par les organismes de renseignement et transmission des renseignements bruts obtenus aux organismes d'exploitation appropriés pour leur utilisation dans l'élaboration du renseignement.*
- *L'exploitation - Transformation des renseignements bruts en renseignement par regroupement, évaluation, analyse, synthèse et interprétation.*
- *La diffusion - Envoi du renseignement en temps utile par tous moyens adaptés et sous une forme appropriée, à ceux qui en ont besoin.*[7]

3. Différentes définitions utiles à la compréhension du renseignement

Une bonne compréhension de la problématique du renseignement nécessite de rappeler un certain nombre de définitions fondamentales.

3.1. Définitions générales

Les concepts « d'information » et de « renseignement » sont souvent – et à tort – confondus. Leur distinction est pourtant fondamentale. Le Comité R[8] suggère les définitions suivantes : *l'information est un élément de connaissance susceptible d'être codé pour être conservé, traité ou communiqué ; le renseignement est un ensemble des connaissances de tous ordres sur un adversaire potentiel, utiles aux pouvoirs publics et au commandement militaire. En d'autres termes le renseignement est une information traitée, analysée et diffusée à qui de droit.* [9]

L'Assemblée de l'UEO met pour sa part en exergue un « renseignement de type général », *qui couvre des domaines variés tels que le politique, le social, l'économique. Il a pour objet de fournir au gouvernement des informations très nombreuses qui ont trait soit à son domaine intérieur, soit à la sphère extérieure. Ces informations concernent principalement la surveillance de régions à risques, la criminalité organisée, les migrations illégales ou bien encore le terrorisme international (...).*[10]

Mais au-delà de ces définitions générales, chacun s'accordera sur le constat exprimé par l'Assemblée de l'UEO : *on peut dire que le renseignement est une « matière première » qui s'avère indispensable aux gouvernements. La connaissance de l'information et la maîtrise corrélative de celle-ci garantissent la liberté d'appréciation des gouvernants, élément fondamental pour l'indépendance de toute décision politique.* [11]

3.2. Définitions particulières

Un certain nombre de définitions particulières, plus précises, nous permettront d'affiner notre propos.

Ainsi, Alexander Walden, de l'Université de Lille 2, distingue le « renseignement extérieur » du « contre-espionnage ». Pour le « renseignement extérieur », il renvoie à la définition figurant dans l'Executive Order 12036 de janvier 1978 sur les activités de renseignement des Etats-Unis : *renseignement concernant les capacités, intentions et activités de puissances, d'organisations ou de personnalités étrangères. Il ne comprend pas le contre-renseignement, à l'exception des renseignements sur les activités terroristes.* Par ailleurs, il relève trois acceptions au « contre-espionnage » (CE) : le CE actif ou

européenne », Université des sciences juridiques, politiques et sociales de Lille III, Année universitaire 1999-2000

7. Doc OTAN AAP-6(2003)

8. Le Comité R est l'organe de contrôle des services de renseignement en Belgique. Ses rapports annuels ne se limitent toutefois pas à cette seule mission, mais ils procèdent aussi à l'analyse de divers aspects du travail des SR dans une perspective comparée. La qualité de ses travaux nous a incité à en faire une abondante utilisation.

9. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1997

10. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, rapport présenté au nom de la Commission de défense par M. Lemoine, Document A/1775, 4 juin 2002, quarante-huitième session.

11. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

répressif (la recherche et l'arrestation d'espions ou d'agents étrangers en opération sur le territoire concerné); le CE passif ou défensif (qui vise à gêner ou empêcher les activités d' espionnage d'un groupuscule étranger, que ce soit un gouvernement ou une entreprise pratiquant l'espionnage industriel ; il peut être entrepris sur le territoire national ou à l'étranger) ; le CE offensif (qui cherche des informations sur les services de renseignement étrangers afin de mieux connaître leurs méthodes et leurs intentions, et les intoxiquer en diffusant des informations erronées, soit en recrutant un membre « en place » de ces services, soit en y plaçant un agent double)[12]. Notons que l'OTAN définit pour sa part le contre-espionnage comme *l'action ayant pour but de détecter l'espionnage et de s'y opposer*, et la contre-ingérence comme *l'opération visant à déceler et à neutraliser toute menace contre la sécurité résultant des activités des services de renseignement, d'organisations ou d'agents se livrant à l'espionnage, à la subversion ou au terrorisme*[13]. On touche ici au « renseignement de sécurité », défini par l'OTAN comme *le renseignement sur la nature, les possibilités ou les intentions d'organisations ou d'individus hostiles, qui sont ou pourraient être engagés dans les activités d'espionnage, de sabotage, de subversion ou de terrorisme.* [14]

Le Comité R distingue le « renseignement ponctuel » (ou « Current Intelligence »), *celui qui se focalise sur ce qui arrive à l'instant présent à un endroit précis. Un suivi continu des sources d'informations, une bonne analyse ainsi qu'un reporting aussi rapide que possible sont les conditions nécessaires du renseignement court terme. Une mise à jour continue, notamment à l'occasion de l'apparition de nouveaux éléments, est primordiale ;* du « renseignement de base » (« Basic Intelligence ») qui *s'attache plutôt aux problèmes de fond, en répertoriant des capacités: localisation des capacités industrielles d'un pays, calcul préalable des cibles potentielles des missiles ennemi.*[15]

Enfin, la « communauté du renseignement » américaine propose une typologie plus complète, qui distingue « Current Intelligence » (*addresses day-to-day events, seeking to apprise consumers of new developments and related background, to assess their significance, to warn of their near-term consequences, and to signal potentially dangerous situations in the near future)*, et « Research Intelligence » (*more in-depth than current intelligence and can be used to support specific operations or decisions, or address a new development in greater detail.* Il peut déboucher sur un « Basic Intelligence », conçu de la sorte : *a structured compilation of geographic, demographic, social, military , and political data on foreign countries)*, « Estimative Intelligence » (*deals with what might be or what might happen …(It) starts with the available facts, but then it migrates into the unknown, even the unknowable. The main roles of estimative intelligence are to help policymakers navigate the gaps between available facts by suggesting alternative patterns into which those facts might fit and to provide informed assessments of the range and likelihood of possible outcomes)*, « Warning Intelligence » (*a subset of estimative intelligence focusing on developments that could have sudden and deleterious effects in US security or policy such as impending crises or long-term dangers)*, et « Scientific and Technical Intelligence » (*includes information on technical developments and characteristics, performance, and capabilities of foreign technologies. It covers the entire spectrum of sciences, technologies, weapon systems, and integrated operations).*[16]

3.3. Le renseignement de défense

Le renseignement de défense mérite d'être isolé, dès lors qu'il développe un certain nombre de spécificités propres, car comme le souligne Charles Baker : *Intelligence is unequivocally linked with defence. Simply, changes in defence imply changes in intelligence. Military superiority must be complemented by effective intelligence capabilities in order to prevent conflicts or win battles. The world's greatest military powers are all dependent on intelligence for making informed evaluations. Therefore intelligence has become an integral part of defence, whether it be in the form of protecting national security, equipping armies with information or identifying prospective hostilities.* [17]

12. WALDEN Alexander, op. cit.
13. Doc OTAN AAP-6(2003)
14. Document OTAN AAP-6(2003)
15. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1997
16. A ce sujet, voyez: Central Intelligence Agency, "*A Consumer's Guide to Intelligence*",Undated, p. 4,26,27. cité par MARTIN Stephen, « *Homeland Security and the Analysis of Foreign Intelligence* », Markle Foundation Task Force on National Security In the Information Age, 15 July 2002; Voyez aussi "*United States Intelligence Community-Who We Are and What We Do*", www.odci.govlic/functions.html
17. BAKER Charles, « *The search for a European intelligence policy* ». Document disponible sur www.fas.org

D'une manière générale, l'Assemblée de l'UEO confie au renseignement de défense *la mission de participer à la prévention des crises internationales, de procéder à des évaluations de situation devant permettre de décider d'éventuelles actions, notamment militaires, ainsi que de conduire, le cas échéant, des opérations militaires.*[18]

Mais une typologie plus précise est nécessaire. Le Comité R, citant une source interne aux SR belges, distingue à cet égard le « renseignement stratégique », le « renseignement opérationnel », et le « renseignement tactique ».

Le « renseignement stratégique » est constitué *d'une part, du renseignement nécessaire* à *la prise de décision au plan national (gouvernement) ou international (ONU, OTAN, UEO), et, d'autre part, du renseignement utile en matière de planification par l'autorité militaire (Etat-major général ou supérieur) d'une opération en appui de cette décision. Il y a donc lieu de collecter des informations relatives* à *une puissance ou un groupe de puissances dans les domaines suivants: biographie, économie, sociologie, transports et télécommunications, géographie militaire, forces armées, politique, science et technologie.*

Le « renseignement opérationnel » est *le renseignement nécessaire pour la planification et la conduite de campagnes et d'opérations importantes visant* à *atteindre des objectifs stratégiques dans des théâtres ou des zones opérationnels. Il englobe le renseignement sur les moyens militaires, la structure des forces, la doctrine, l'armement, les équipements, les infrastructures, l'instruction et les intentions des pays ennemis ou des parties en présence en cas d'opérations de paix.*

Pour ce qui est du « renseignement tactique », *il s'agit du renseignement qui permet au commandant tactique de préparer et de mener à bien des opérations tactiques à son niveau (bataillon, brigade, division, éventuellement corps d'armée). Il comprend la connaissance de l'ennemi ou des parties en présence (en cas d'opérations de paix), des circonstances géographiques et atmosphériques (météo) et de l'attitude de la population civile dans et autour de la zone d'action considérée. Outre la connaissance de la doctrine et des procédés tactiques, de l'effectif, de l'armement et du matériel de l'ennemi ou des parties en présence (forces armées et organismes paramilitaires), le commandant tactique a besoin de renseignements relatifs au terrain dans lequel vont se déployer ses troupes.* [19]

Pour sa part, l'OTAN définit le « renseignement stratégique » comme *le renseignement nécessaire à la formulation de la politique, à la planification militaire et à la fourniture d'indices et d'indicateurs d'alerte*, et le « renseignement tactique » comme *le renseignement nécessaire à la planification et à l'exécution des opérations au niveau tactique*. [20]

L'Assemblée de l'UEO propose une autre classification en trois catégories, à savoir le « renseignement de documentation » (*acquis dès le temps de paix, pour avoir une connaissance générale des zones de crises potentielles: mouvements politiques, géographie des lieux, forces armées et milices, installations militaires)*, le « renseignement de situation » (*acquis au moment de la crise, que l'on peut différencier en fonction du niveau de réflexion de l'état-major qui va l'utiliser : niveau stratégique (état-major de l'UE, état-major du commandant d'opération), niveau opératif (état-major du commandant de force sur le théâtre d'opération), niveau tactique (état-major qui met en oeuvre une composante de la force pour une opération localisée)* et le « renseignement de combat » (*qui permet au combattant sur le terrain de conduire l'action (évaluation des tirs, position des combattants).*[21]

L'OTAN distingue pour sa part le « renseignement brut de combat » (*Donnée d'une validité souvent éphémère recueillie au combat par des unités ou qui leur est directement communiquée. Elle peut être utilisée pour les opérations et l'appréciation de la situation. Cette donnée entrera dans les circuits du renseignement)* du « renseignement de combat » (*renseignement sur l'ennemi, les conditions atmosphériques et géographiques nécessaires au commandement pour la préparation et la conduite des opérations de combat*). [22] Quant au « renseignement opérationnel », il s'agit du *renseignement nécessaire à la planification et à la conduite de campagnes au niveau opératif*. [23]

En somme, et nous reprenons ici le raisonnement du Lieutenant-Colonel de Barmon, dans

18. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

19. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1997

20. Document OTAN AAP-6(2003)

21. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

22. Document OTAN AAP-6(2003)

23. Ibid.

la conduite des opérations, *la finalité du renseignement est donc de prévoir ce que fera l'adversaire de manière à produire à temps les plans avant l'action, à ajuster la manoeuvre en cours d'action et à évaluer les effets après l'action. Ainsi, le renseignement, qui s'inscrit dans une logique d'anticipation et de permanence, a toujours été un facteur primordial dans l'application des principes de la guerre, positif ou négatif, selon qu'on l'utilise ou qu'on l'ignore: la liberté d'action dans la recherche de la sûreté (renseignement d'alerte), la concentration des efforts par l'identification du point d'application de l'effort (centre vitaux, centres déterminants) et de l'évaluation des risques encourus (renseignement d'objectif) ; l'économie des forces, par la recherche des informations précises et actualisées permettant au chef d'ajuster son dispositif selon une synergie optimale.* [24]

4. Distinguer « Law Enforcement » et « Intelligence »

Enfin, il nous semble important de distinguer – et nous reprenons ici la terminologie anglo-saxonne - les concepts de « Law Enforcement » et de « Intelligence », dont la confusion est elle aussi de nature à susciter une certaine incompréhension, voire des craintes, au sein de l'opinion publique à l'égard des SR. Sous couvert d'une lutte accrue contre la criminalité organisée ou le terrorisme, les SR ne risquent-ils pas en effet de se transformer en « Moloch » dont les méthodes particulières, trop peu respectueuses des droits des citoyens, contribueraient à une justice trop « expéditive » ?

Déjà des voix s'élèvent, comme celle d'Ignacio Ramonet du « Monde Diplomatique », qui dénonce : *le 11 septembre 2001 a marqué en matière de respect des droits humains une rupture nette. Au nom de la « juste guerre » contre le terrorisme, beaucoup de transgressions ont soudain été permises. (...) Les défenseurs des droits publics ont de quoi être inquiets, le mouvement général de nos sociétés, qui tendait vers un respect toujours plus grand de l'individu et de ses libertés, vient d'être brutalement stoppé. Et tout indique que l'on dérive désormais vers un Etat de plus en plus policier et paranoïaque…* [25]

Le Canadien Jean-Paul Brodeur, de l'Ecole de criminologie de Montréal, souligne pour sa part que *la convergence du renseignement de sécurité et du renseignement criminel (...) est problématique et que le maillage des réseaux ne s'effectuera pas sans difficulté, s'il se réalise jamais. (...) Le renseignement criminel a pour but de conduire à l'arrestation de criminels et de les amener devant un tribunal pour qu'ils y subissent un procès. A cause du caractère public de ces procès et des contre-interrogatoires des témoins, le risque que des informations confidentielles y soient divulguées est toujours présent. C'est pourquoi les services de renseignement de sécurité ont de fortes réticences à partager avec les forces policières les renseignements dont ils disposent. Le but du renseignement de sécurité est la prévention de l'action violente avant qu'elle ne soit perpétrée, par divers moyens. Le recours aux tribunaux demeure une option parmi d'autre et, au vrai, un recours ultime*[26]. Gregory Treverton confirme que *parce que les services de renseignements cherchent avant tout à protéger leurs sources et leurs méthodes, les responsables du renseignement veulent désespérément éviter de se retrouver dans la chaîne de possession des indices pour ne jamais avoir à témoigner en cour. De leur côté, les organismes d'application de la loi ne s'intéressent pas aux politiques. Ils s'occupent plutôt des poursuites judiciaires. Et ils savent que pour constituer un dossier, ils doivent être prêts à révéler des choses qui expliqueront comment ils en sont venus à savoir ce qu'ils savent.* [27]

Si l'opinion publique européenne est relativement « compréhensive » en matière de lutte anti-terroriste (il existe des précédents, comme la lutte contre l'IRA en Irlande du Nord), voire dans la lutte contre certaines formes de criminalité organisée mettant en péril l'Etat lui-même (la lutte anti-mafia en Italie) ou de criminalité revêtant une dimension peu ou prou « politique » (trafic d'armes, de composantes d'armes de destruction massive, le trafic de drogues, le mercenariat), elle s'émeut par contre lorsqu'on évoque

24. de BARMON (Lieutenant-Colonel), *« La fonction renseignement »*, in « Objectif Doctrine », publié par le Commandement de la Doctrine et de l'Enseignement Militaire Supérieur de l'Armée de Terre, Octobre 2000.
25. RAMONET Ignacio, *Surveiller et réprimer*, Le Monde Diplomatique – Manière de voir 71, « Obsessions sécuritaires », bimestriel, octobre-novembre 2003
26. BRODEUR (Jean-Paul), « *Les services de renseignement et les attentats de septembre 2001* », Centre international de criminologie comparée, Université de Montréal. Disponible sur le site www.unites.uqam.ca
27. TREVERTON Gregory F., « *Remodeler le renseignement pour le partager avec « nous-mêmes* », Commentaire n° 82, Publication du Service Canadien du Renseignement de Sécurité, 16 juillet 2003 (disponible sur le site csis-scrs.gc.ca)

l'immigration illégale (et son sordide corollaire, la traite des êtres humains) en termes de « menace contre la sécurité nationale ».

Nous verrons ultérieurement que le Conseil européen, lui-même, risque d'alimenter cette polémique en introduisant les SR dans ses projets de coopération « policière », que sont Europol et les équipes d'enquête communes.

5. La diversité des compétences à travers la multiplication des services[28]

Le « paysage » du renseignement en Europe offre l'aspect d'une mosaïque, puisque tous les Etats membres, ou presque, disposent en fait d'une « communauté du renseignement » constituée de plusieurs services, dont les missions, les compétences et l'articulation sont variables.

En Allemagne, le Bundesnachrichtendienst (BND) est orienté vers l'extérieur du territoire ; il a pour tâche de surveiller les pays à risque, la criminalité organisée, ou encore le blanchiment d'argent ; le Bundesamt für Verfassungsschutz (BfV), qui relève du Ministre de l'intérieur, est chargé du contre-espionnage et de la lutte contre la subversion; l'Amt für Nachrichtenwesen der Bundeswehr (ANBw) et l'Amt für Fernmeldewesen der Bundeswehr (AFBw) se concentrent sur le renseignement militaire.

En France, la Direction générale de la sécurité extérieure (DGSE) a pour fonction de rechercher et d'exploiter les renseignements intéressant la sécurité de la France ainsi que de détecter les activités dirigées contre les intérêts français émanant de l'extérieur du territoire national ; la Direction de la surveillance du territoire (DST) a pour mission de rechercher et de prévenir, sur le territoire français, les activités de nature à menacer la sécurité du pays ; la Direction du renseignement militaire (DRM) est chargée de recueillir et de trouver les informations ayant un caractère militaire ou des informations générales de types politique, social ou économique qui sont nécessaires au ministère de la défense et qui pourraient avoir une influence sur l'organisation d'une opération militaire ; la Direction de la Protection et de la Sécurité de la Défense (DPSD), rattachée au Ministre de la défense, assure des missions classiques de sécurité militaire.[29]

En Grande-Bretagne, le Secret Intelligence Service (SIS) (plus connu sous son ancien nom de MI6), qui dépend du Ministre des affaires étrangères, est chargé du renseignement extérieur stratégique ; le Security Service (SS) (autrefois appelé MI5), dépend du Ministre de l'intérieur, et est chargé du terrorisme au Royaume-Uni, de la lutte contre le terrorisme international, du contre-espionnage, du crime organisé ; le Defence Intelligence Staff (DIS) s'intéresse aux domaines qui touchent à la défense, y compris des problèmes économiques, politiques ou technologiques ; le Government Communications Headquarters (GHCQ), procède aux écoutes électroniques. La «Special Branch» de Scotland Yard et le National Criminal Intelligence Service (NCIS) complètent le dispositif.

En Espagne, le Centre national d'information (CNI), compétent tant à l'extérieur que sur le territoire national, est chargé du terrorisme, des mouvements extrémistes, du contre-espionnage et renseignement économique ; le Centre général d'informations (CGI), qui dépend du Ministre de l'intérieur, conduit les enquêtes sur le territoire (subversion, ETA, stupéfiants, délinquance économique et financière) et dispose aussi d'une unité de renseignement extérieur (intégrisme islamiste, coopération internationale, veille économique, etc.) ; l'Etat-major général (EMACON) est responsable du renseignement de défense.

En Italie, le Servizio per le Informazioni e la Sicurezza Democratica (SISD) est spécifiquement attaché à la protection des intérêts de la sécurité intérieure, tandis que le Servizio per le Informazioni e la Sicurezza Militari (SISMI) est chargé des tâches de renseignement plus spécifiquement militaire et de sécurité extérieure.

En Belgique, la Sûreté de l'Etat (SE), qui est placée sous l'autorité du Ministre de la justice, mais que le Ministre de l'intérieur peut requérir pour des missions relevant de l'ordre public et de la protection des personnes, a pour mission le renseignement aux menaces contre la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le

28. Sauf indications contraires, les données ci-dessous sont issues de : Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

29. Assemblée Nationale, Rapport d'information n° 3460 déposé par la Commission de la défense nationale et des forces armées en conclusion des travaux d'une mission d'information sur les conséquences pour la France des attentats du 11 septembre 2001, et présenté par MM. Paul Quilès et René Galy-Dejean et Bernard Grasset

potentiel scientifique ou économique ou tout autre intérêt fondamental du pays; le Service Général du Renseignement et de la Sécurité (SGRS) placé sous l'autorité du ministre de la défense nationale, a pour mission le renseignement relatif aux menaces contre l'intégrité du territoire national, les plans de défense militaires, l'accomplissement des missions des Forces armées ou la sécurité des ressortissants belges à l'étranger ou tout autre intérêt fondamental du pays ; il est aussi chargé de la sécurité militaire du personnel relevant du Ministre de la défense nationale, et des installations militaires.[30]

Si l'Assemblée de l'UEO considère que les SR ont *des structures semblables et des intérêts identiques,*[31] il n'en reste pas moins que cette multiplication de services illustre la volonté des pouvoirs politiques d'éviter la constitution de structures trop puissantes, qui se révéleraient incontrôlables. Le problème de la coordination entre services se révèle en outre récurrent, mais il ne sera pas développé ici.

30. Loi organique du 30 novembre 1998, Moniteur Belge du 18 décembre 1998
31. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

II. Le 11 septembre 2001 et ses conséquences : état des lieux de la coopération européenne en matière de renseignement

1. Le 11 septembre 2001 : les leçons de l'échec américain et la prise de conscience européenne

Les attentats du 11 septembre 2001 ont placé les services de renseignement américains sur la selette. Entre autres conclusions, le rapport final du Congrès, publié le 10 décembre 2002 , conclut que *pour diverses raisons, l'Intelligence Community n'a pas exploité l'importance, tant sur le plan individuel que global, d'informations dont le lien avec les événements du 11 septembre est clair. Dès lors, elle a manqué des occasions d'interrompre le scénario du 11 septembre, en refusant l'entrée sur le territoire aux pirates de l'air potentiels, ou en les gardant en détention ; de tenter au moins de dévoiler ce qui se tramait grâce à une surveillance et une investigation accrues à l'intérieur des Etats-Unis ; enfin, de renforcer la vigilance et de rendre ainsi la patrie plus résistante à l'attaque*.[32]

Dès le lendemain des attentats, les plus hautes autorités de l'UE soulignèrent la nécessité d'approfondir la coopération en matière de renseignement au sein de l'Union. [33]

Le 14 septembre, la déclaration commune des chefs d'Etat et de gouvernement de l'UE promettait que *dans la lutte contre le terrorisme, nous développerons nos efforts en matière de renseignements.*

Le Conseil Justice et Affaires intérieures (JAI) a adopté, le 20 septembre, un long catalogue d'intentions - dont un chapitre est d'ailleurs spécifiquement intitulé « coopération policière/services de renseignement » - qui précise : *le Conseil rappelle l'importance, pour la qualité des analyses d'Europol, d'une transmission rapide par les autorités policières, mais aussi par les services de renseignement des Etats membres, de toute donnée pertinente en matière de terrorisme, conformément aux dispositions de la Convention Europol. (...) Le Conseil souligne le rôle important des services de sécurité et de renseignement dans la lutte contre le terrorisme. Les informations qu'ils fournissent représentent un atout inestimable pour révéler à un stade précoce d'éventuelles menaces terroristes ou intentions de terroristes ou groupes terroristes. Ces services ont par conséquent une mission essentielle dans la prévention du terrorisme. La coopération et l'échange d'informations entre eux doivent être intensifiés. Afin d'accélérer ce processus, les responsables de ces services dans les Etats membres de l'Union européenne se réuniront régulièrement dès avant le 1er novembre 2001. Ils prendront sans retard les mesures nécessaires pour améliorer ultérieurement leur coopération. La coopération entre les services de police, y compris Europol, et les services de renseignement devra être renforcée.*

Les conclusions du Conseil européen extraordinaire du 21 septembre insistent globalement sur la mise en oeuvre des conclusions du Sommet de Tampere visant à établir « un espace de liberté, de sécurité et de justice ». Pour ce qui concerne plus spécifiquement les services de renseignement, le Conseil européen répète qu'*une meilleure coopération et un meilleur échange d'informations entre tous les services de renseignement de l'Union s'imposent. Des équipes communes d'enquête seront constituées dans ce but*.

Le 12 octobre 2001, les Ministres de la Défense des Quinze réunis en Conseil informel ont décidé d'améliorer la coopération entre les services de renseignement militaires pour lutter contre le terrorisme. Le Haut Représentant pour la PESC, Javier Solana, a été chargé de la mise en œuvre cette décision. En marge de cette réunion qu'il présidait, le Ministre belge de la défense, André Flahaut, s'est prononcé en faveur de l'extension de cette décision aux services de renseignement civils.

Le 19 octobre 2001, le Conseil européen confirmait sa détermination à combattre le terrorisme *par exemple en renforçant la coopération entre les services opérationnels chargés de la lutte contre le terrorisme: Europol, Eurojust, les services de renseignement, les services de police et les autorités judiciaires*.

Enfin, l'annexe V des conclusions du Conseil européen de Séville des 21-22 juin 2002 dispose qu'*en matière de lutte contre le terrorisme, y compris dans le domaine de la PESC et de la PESD l'Union européenne devrait par priorité: (...) renforcer les mécanismes d'échange de renseignements et recourir davantage à l'évaluation des situations et aux rapports d'alerte*

32. Traduction publiée par Le Monde, 26 juillet 2003
33. Pour le texte complet des documents mentionnés ici, voyez : www.europa.eu.int

rapide, en se fondant sur un maximum de sources différentes, se doter d'une évaluation commune de la menace terroriste qui pèse sur les Etats membres ou les forces déployées en dehors de l'Union, dans le cadre de la PESD, pour des opérations de gestion de crises, y compris de la menace d'une utilisation à des fins terroristes d'armes de destruction massive.

D'autres voix plaident en ce sens.

Un rapport de l'Assemblée de l'UEO estime que *les attentats (...) ont révélé les difficultés, mais également les faiblesses, de l'acquisition et de l'exploitation du renseignement face au terrorisme international. Afin d'éviter ces difficultés, l'Europe devra mettre en place des structures efficaces de coordination dans le domaine du renseignement entre les différents Etats participants*. [34] L'Assemblée de l'UEO estime encore qu'*améliorer la capacité de l'Union Européenne de décider de façon autonome [c'est-à-dire à l'abri de toute ingérence extérieure] implique, ipso facto, de la doter, dans les meilleurs délais, d'une capacité véritablement autonome de renseignement, qu'il s'agisse de la recherche et du recueil, de l'exploitation ou la diffusion. C'est là une condition sine qua non si l'on veut échapper à une situation de dépendance chronique à l'égard d'autres pays, alliés ou partenaires, qui disposent de la panoplie des moyens de renseignements modernes et qui sont les seuls à pouvoir décider en toute indépendance. Chacun connait le poids de « l'image preuve » aux yeux de nos décideurs politiques, à condition que la fiabilité de ce document ne puisse être mise en doute*. [35] Elle ajoute, plus précisément, qu'*il est clair que les satellites transportant des charges capables de capter et de transmettre de l'imagerie (optique, infrarouge ou radar) ou des informations d'origine électro-magnétique constituent l'ossature d'un système de renseignement stratégique.*[36] En conséquence, l'Assemblée propose à la Convention sur l'avenir de l'UE *d'inclure dans ses débats la discussion de propositions de modification des institutions afin de permettre (...) : le développement et la modernisation des capacités de défense nationales et communes de l'UE, et portant une attention particulière au domaine du renseignement humain, électronique et dans l'espace extra-atmosphérique, pour assurer le maintien d'une autonomie aussi complète que possible*.[37] Dans le cadre plus particulier de la lutte anti-terroriste, l'Assemblée recommande au Conseil d'inviter les pays de l'UEO *à coopérer et à coordonner étroitement leurs actions dans l'ensemble des domaines associés à la lutte antiterroriste, à savoir le renseignement, la police et la justice, la coopération financière et l'emploi de moyens militaires en poursuivant une politique « globale » contre cette menace ; à se doter d'une capacité militaire coordonnée au niveau européen, capable de participer efficacement à la lutte contre le terrorisme en donnant la priorité aux moyens de renseignement et de communication associés - notamment les satellites d'observation optiques et radar, l'aviation de reconnaissance et les drones, ainsi que les cellules d'analyse et d'interprétation du renseignement - et aux munitions guidées de précision.*[38]

De même, un rapport de l'Assemblée Nationale française conclut que *les attentats du 11 septembre mettent en évidence la nécessité d'une coopération et d'un échange d'informations plus étroits entre ces services de renseignement et leur homologues européens et américains.* Les contacts qui sont en train de mettre en place restent, pour elle, insuffisants : *la concertation doit donc être plus permanente, ce qui suppose que des rencontres aient lieu régulièrement au sein d'un comité européen du renseignement, dont la mission d'information suggère la création sur le modèle du comité interministériel du renseignement français.* [39]

Mais au-delà de ces viriles déclarations, essentiellement de nature à rassurer l'opinion publique, force est de constater qu'à l'heure où ces lignes sont écrites, les progrès ne sont que modestes, même si des structures – que nous allons maintenant passer en revue – existent.

34. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
35. Ibid.
36. Ibid.
37. Assemblée de l'UEO, « *Une politique de défense européenne : contribution à la Convention* », Document C/1798, 9 octobre 2002, quarante-huitième session, rapport présenté au nom de la commission de défense par M. Schloten, président et rapporteur
38. Assemblée de l'UEO, Document A/1783 – Recommandation n°706 sur les capacités militaires européennes dans le contexte de la lutte contre le terrorisme international
39. Assemblée Nationale, Rapport d'information n° 3460, op. cit.

2. Les structures de coopération existantes

2.1. Les échanges de renseignements entre SR : les principes de base

Un humoriste déclara un jour qu'un secret est une information que l'on confie à tout le monde, en demandant de ne la répéter à personne. Telle n'est évidemment pas l'approche des SR !

Larry Wentz, un analyste américain note très justement la propension naturelle des SR à ne pas partager leurs informations : *Intelligence is one of the hardest things to share in a coalition environment. Each partner, no matter how dedicated to the general cause, has a natural tendency to mask his intelligence capabilities and to retain control of what tasks he performs and how his products are disseminated. Furthermore, there are differences in national doctrine and disclosure rules.*[40]

Pour évoquer l'approche des SR en matière d'échanges, le Comité R belge estime qu'*il est un fait reconnu que les services de renseignement opèrent dans le monde entier sur la base d'un système de troc consistant pour chaque service à obtenir des informations exclusives qui pourront par la suite être échangées avec d'autres services qui détiennent eux des informations inaccessibles au premier service. (...) Le principe de l'échange implique celui de la réciprocité.*[41] En effet, les SR opèrent dans le monde entier sur la base d'un système de troc consistant pour chaque service à obtenir des informations exclusives qui pourront par la suite être échangées avec d'autres services qui détiennent eux des informations inaccessibles au premier service. La *«règle du tiers»* constitue le fondement de la collaboration entre services. Il s'agit là d'une des règles les plus anciennes et les plus strictes qui se justifie par l'impératif de la protection des sources. A titre d'exemple, l'article 5§1 qui régit la procédure d'échange de renseignements au sein du Club de Berne (Cf infra) dispose que *les renseignements qui sont échangés au sein du Club ne peuvent être adressés* à *une instance étrangère au Club, ni être utilisés* à *d'autres fins que celles contenues dans l'information sans l'accord formel du service qui en est à l'origine.* Il s'agit ici non seulement de la règle du tiers, mais également de la règle du service tiers.[42] L'article 18(4) de la Convention EUROPOL établit que toute information communiquée à EUROPOL par un Etat membre ne peut être transmise à un Etat tiers qu'avec l'accord de l'Etat d'origine. Des dispositions semblables sont prévues dans les accords de coopération conclus entre EUROPOL et des Etats tiers. De telles dispositions figurent aussi bien entendu dans les règlements de sécurité «C-M(55)15» de l'OTAN et «VR 100» de l'UEO qui prévoient explicitement qu'avant toute dissémination d'informations, l'accord préalable doit être donné par celui qui les a fournies. On retrouve la même logique dans la Convention du 28 janvier 1981 du Conseil de l'Europe, relative à la protection de la vie privée dans laquelle il est stipulé qu'il est dangereux de fournir, par l'intermédiaire d'une autre partie, des informations liées aux personnes à un Etat qui n'est pas partie à la convention.[43] Enfin, le service juridique d'INTERPOL nous signale qu'aucune information ne peut être transmise sans le consentement du Bureau Central National (BCN) qui en est à l'origine. La transmission d'une information émise par un BCN à un autre BCN (voire à une organisation internationale) est donc toujours soumise à autorisation du premier, que cette autorisation soit expresse ou admise par convention préalable (pour tel type de message par exemple). Cette règle s'impose au Secrétariat général comme aux pays membres.[44]

Dans une étude intitulée « Vers une politique européenne de renseignement » publiée par l'Institut d'Etudes de Sécurité de l'UEO en décembre 1998, Klaus Becher, Bernard Molard, Frédéric Oberson et Alessandro Politi estiment que le premier obstacle à une coopération accrue est la sécurité : *la confiance et la sécurité sont nécessaires pour protéger le renseignement sensible et les méthodes de recueil, notamment les sources, d'une diffusion inopportune et inappropriée*. (…) *Tout laisse croire qu'avec la multiplication des échanges de renseignements, les risques potentiels tendront à augmenter, ce qui créera des réticences vis-à-vis de ces échanges.* Mais a contrario, ils estiment que *plus les agences impliquées sont nombreuses, plus les contrôles de sécurité se multiplient*, d'autant que *la sécurité de l'information n'est pas une fin en soi : elle est une fonction de sa diffusion appropriée*. Le second obstacle réside potentiel à la

40. WENTZ Larry, « *Intelligence Operations* », http://216.156.87.17
41. Ibid.
42. Comité permanent de contrôle des services de renseignement, rapport d'activité 2000
43. Ibid.
44. Notes personnelles de l'auteur

coopération est *la crainte que l'intensification des échanges européens ne nuise aux relations privilégiées avec des partenaires importants*. L'allusion aux relations « privilégiées » entre la Grande-Bretagne et les Etats-Unis, est limpide. Mais les auteurs objectent que *tant que les décideurs considéreront que le principal problème est d'analyser ce que les agences européennes pourraient réaliser de la façon la plus satisfaisante avec leurs propres moyens, la question ne semble pas très problématique. Au contraire, une politique européenne de renseignement pourrait même pérenniser un partenariat bilatéral, qui bénéficierait d'une contribution globale plus significative dans le domaine du renseignement de la part de l'acteur mineur et du profil accru qu'offre une entreprise conjointe plus importante. Pour finir, chacun y trouverait son compte*. Les auteurs pointent encore *l'esprit de corps qui incite toute organisation de renseignement à n'avoir véritablement confiance qu'en son propre travail*. Enfin, un dernier obstacle réside dans *la crainte qu'une agence appartenant à un pays plus petit puisse être infiltrée, influencée, contrôlée et, pour finir, phagocytée par des partenaires plus grands*. Mais nous rejoignons l'opinion des auteurs pour qui *cette crainte ne tient pas compte du fait fondamental qu'en Europe, aucune agence nationale de renseignement (en fait, aucun Etat-nation) ne peut aspirer, et encore moins prétendre à une position dominante. A l'échelle mondiale, la scène européenne du renseignement semble être un groupe d'entités de taille variable dont la maigre consolation est peut-être qu'ils sont dans une position analogue à celle de nombreuses autres instances*. L'alternative est donc simple : *les agences européennes devraient se demander si elles souhaitent devenir plus utiles collectivement grâce à des synergies pragmatiques, ou si elles préfèrent conserver une taille dérisoire par rapport au reste du monde.* [45]

2.2. L'état de la coopération entre SR européens au sein d'enceintes multilatérales

Le Préfet Bernard Gérard, ancien directeur de la DST française, commentait en ces termes l'existence d'une réelle coopération européenne, certes limitée au seul problème du terrorisme : *le grand public connaît mal la connivence organisée, durant les années 1980, entre les services européens de renseignement et de sécurité dans la lutte contre les terrorismes internationaux. Elle s'appuyait sur un réseau de communication instantané protégé – Intranet avant l'heure – aujourd'hui institutionnalisé*.[46] Ole Villadsen, un analyste américain confirme: *What is not as well recognized is the scale of other less complete exchanges that have developed with other Western countries and between them. The result is a patchwork of bilateral and multilateral arrangements of all kinds and all degrees of intimacy. The patchwork is unusual in its secrecy, but otherwise is not unlike the intergovernmental arrangements that have developed in other specialized areas.*[47]

Nous n'évoquerons ici que les structures dont l'existence a été mentionnée dans des sources ouvertes, avec toutes les réserves et les limites que cela implique.

Le groupe TREVI, acronyme pour «Terrorisme, Radicalisme, Extrémisme et Violence Internationale», fut créé en 1975 pour réunir les Ministres de l'intérieur et de la justice de la Communauté européenne afin de renforcer la coopération policière contre la criminalité organisée, le terrorisme, ou le trafic de stupéfiants. Le Traité de Maastricht a engendré une modification du statut du groupe qui, devenu permanent, est chargé d'organiser les échanges de renseignements et d'harmoniser les législations et réglementations européennes.[48] TREVI a maintenant fait place à la coopération JAI (Justice/Affaires Intérieures), et le Comité K 4, composé de hauts fonctionnaires, est chargé de la préparation et de l'exécution des décisions prises par le Conseil JAI. [49]

Le Club de Berne, moins connu, fut créé en 1965, [50] et regroupe aujourd'hui 18 pays. En fait, ce «club» serait le cadre de nombreuses réunions organisées par thèmes en fonction des préoccupations du moment. Il permettrait des contacts

45. POLITI Alessandro, « *De la nécessité d'une politique européenne de renseignement* » in BECHER Klaus, MOLARD Bernard, OBERSON Frédéric et POLITI Alessandro, « *Vers une politique européenne de renseignement* », op. cit.

46. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

47. VILLADSEN Ole, « *Prospects for a European Common Intelligence Policy »*, Document disponible sur www.cia.gov/csi/studies

48. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

49. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1995

50. ou en 1971, selon les sources.

informels par petits groupes.[51] Mais un rapport de l'Assemblée de l'UEO constate que *les synthèses de situation élaborées au niveau des directeurs de service ne servent qu'à informer les pays membres puisqu'il n'y a pas d'autorité politique européenne destinataire de ce renseignement, comme pourrait l'être le Haut représentant pour la PESC, M. Solana. Il est vrai que le renseignement, accompagné d'une appréciation de situation, peut engager la politique d'un pays et que cela pose des problèmes de souveraineté aux Etats membres*. [52] Le Club de Berne se réunirait tous les six mois au niveau des chefs des services et ne déciderait qu'à l'unanimité. Une fois par an, *«Les Cours du Club»* seraient organisés au profit de « *middle-rank officers* » afin d'harmoniser les procédures de formation et de promouvoir les contacts.[53]

Le Kilowatt Group comprenait, lors de sa création en 1977, 15 membres (9 Etats membres de la CEE, Canada, Norvège, Suède, Suisse, USA et Israël). Dans ce groupe, il ne s'agirait pas d'échanges « donnant donnant ». Chaque service de renseignement national mettrait à la disposition des autres les informations qu'il possède sur le terrorisme. Ce ne serait en fait qu'un réseau de télex. [54] Selon Roland Jacquard, Kilowatt aurait été réactivé au lendemain du 11 septembre 2001.[55]

Le Comité spécial de l'OTAN réunit des services de sécurité des pays membres de l'Alliance. Il a pour compétence le contre-espionnage et la lutte contre le terrorisme, notamment pour la protection des troupes – essentiellement américaines – déployées à l'étranger. Néanmoins, le grand nombre de participants et des divergences de vues sur la définition du terrorisme limitent la confidentialité des renseignements échangés.[56]

Citons encore la conférence des ministres de l'intérieur de la Méditerranée occidentale, créée à Rome en 1982, à l'initiative de la France, et qui regroupe la France, l'Espagne, la Tunisie, l'Algérie et le Maroc, pour lutter contre le fondamentalisme islamique et le crime organisé. Ou la *Middle European Conference* (MEC), une association de fait entre les patrons des services civils de renseignement et de sécurité d'Europe de l'Ouest et d'Europe Centrale.[57]

Enfin, les séminaires ILETS (« International Law Enforcement Communication Seminars ») visent à constituer un lieu de discussion et de coopération au sein duquel la problématique des interceptions légales des télécommunications peut être abordée au un niveau international. ILETS se présente comme une rencontre informelle de services mais le Comité R considère que la « déclaration d'intention concernant la surveillance légale des télécommunications » signée par les autorités américaines et par le Secrétariat général du Conseil de l'UE et présentée à la signature des autres participants le 25 octobre 1995 (document ENFOPOL n° 112) constitue un acte légitimant l'existence d'ILETS.

Ce document prévoit de mettre au point des mesures techniques d'interception de télécommunications en concertation avec des Etats non soumis aux exigences de la convention européenne des droits de l'homme et des directives de l'UE en ce domaine. Lors de la réunion ILETS qui s'est tenue à Bonn en 1994, les participants ont approuvé un document de directives politiques auquel était annexée une liste de «International User Requirements» (IUR 1.0 ou IUR 95) énumérant les spécifications auxquelles les opérateurs de télécommunications doivent se conformer pour faciliter les interceptions. Cette IUR servit de base à la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, que nous examinerons plus loin.[58] La «révélation» des séminaires ILETS suscita une certaine émotion dans plusieurs pays européens, lorsqu'il apparut que les instances de contrôle parlementaire de plusieurs pays participants n'étaient pas informées de ces réunions. Un rapport du Parlement fédéral belge conclut d'ailleurs que *les ILETS sont un instrument permettant aux services de renseignements américains d'imposer leurs priorités en matière de technologie de surveillance à l'Union européenne et aux autres pays participants*.[59]

51. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
52. Ibid.
53. Comité permanent de contrôle des services de renseignements, Rapports d'activité 2000
54. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
55. Le Figaro, 13 octobre 2001
56. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
57. Comité permanent de contrôle des services de renseignements, Rapports d'activité 2000
58. Comité permanent de contrôle des services de renseignements – Rapport d'activité 2001
59. Sénat et Chambre des Représentants de Belgique, Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé « Echelon », rapport fait au

Face à ce panorama, forcément incomplet, le Comité R conclut que *le développement de la coopération entre les services de sécurité et/ou de renseignements au sein de l'Union Européenne oscille entre deux conceptions divergentes entre lesquelles le débat reste ouvert : certains pays conçoivent cette coopération dans un cadre intergouvernemental; d'autres pays comme la Belgique la conçoivent sur le plan des institutions communautaires.* [60] D'autres, par contre, dénoncent les dangers potentiels de ces structures. Ainsi, l'Assemblée Nationale française estime que *l'existence de clubs informels en matière de renseignement pose la question fondamentale de l'enjeu de ces clubs et de leurs objectifs. Dans de telles structures, bien des possibilités de manipulation et d'orientation des informations sont concevables.* [61]

2.3. Les structures de coopération dans le cadre du « second pilier » - Justice et Affaires Intérieures (JAI)

D'aucuns estiment que la coopération dans le domaine du renseignement pourrait s'inspirer de la Convention Europol, signée en 1995 et entrée en vigueur le 1er octobre 1998, et chargée notamment de *faciliter l'échange d'informations entre les Etats membres; rassembler et analyser les informations et renseignements; communiquer aux services compétents des Etats membres les informations les concernant et les informer immédiatement des liens constatés entre des faits délictueux; faciliter les enquêtes dans les Etats membres; gérer des recueils d'informations informatisés.* [62]

L'application de la Convention dans chaque Etat se fait grâce à une « unité nationale », seule autorisée à assurer la liaison entre Europol et les services nationaux concernés et compétents. Cette unité envoie auprès d'Europol au moins un officier de liaison, chargé de représenter les intérêts de son pays au sein de l'organisation. L'article 3 de l'Acte du Conseil d'administration d'Europol du 15 octobre 1998 relatif aux droits et obligations des officiers de liaison détermine les conditions requises pour exercer cette fonction : *les officiers de liaison des Etats membres doivent, afin de pouvoir s'acquitter de leurs tâches au sein d'Europol, réunir au moins les conditions ci-après, chaque Etat membre appréciant si elles sont effectivement réunies: les officiers de liaison sont des fonctionnaires des services compétents en matière de prévention et de répression des délits qui relèvent de la compétence d'Europol au sens de l'article 2 de la convention Europol, selon le droit national de l'Etat membre qui les a désignés; ils connaissent au moins deux langues officielles de l'Union européenne; ils réunissent les conditions d'aptitude et de capacité nécessaires à l'exercice de leurs fonctions.*[63] Rien n'interdit donc un Etat membre d'intégrer des membres de ses SR, soit au sein de « l'unité nationale », soit en qualité d'officier de liaison. Mais d'aucuns observent que Europol est « contrôlé » par les Ministères de la justice, et qu'il ne constitue dès lors pas un forum d'échanges entre services de renseignement.[64] De plus, des limitations aux échanges de renseignements restent possibles si leur transmission *porte atteinte à des intérêts nationaux essentiels en matière de sécurité; compromet le succès d'enquêtes en cours ou la sécurité d'une personne ou concerne des informations relevant de services ou d'activités spécifiques de renseignements en matière de sûreté de l'Etat* – une phraséologie qui recouvre largement les missions habituelles des SR qu'à l'évidence, le législateur a souhaité se réserver le droit de soustraire à la démarche de coopération/intégration d'Europol.

Les équipes communes d'enquête pourraient constituer un autre outil utile de coopération. Le Conseil européen de Tampere des 15 et 16 octobre 1999 avait demandé que les équipes communes d'enquêtes prévues par le traité soient mises sur pied pour lutter contre le trafic de drogue et la traite des êtres humains, ainsi que contre le terrorisme.[65] Le 11 septembre a brus-

nom de la commission chargée du suivi du comité permanent de contrôle des services de renseignement et de sécurité (Sénat) et de la commission spéciale chargée de l'accompagnement parlementaire du comité permanent de contrôle des services de police (Chambre) par Madame Lizin et M. Van Parys, 25 février 2002, Doc 754/1 (Sénat) et 1660/001 (Chambre)

60. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1995

61. Assemblée Nationale, Rapport d'information n°2623 du 11 octobre 2000, déposé par la commission de la Défense nationale et des forces armées sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, présenté par M. Arthur Paecht, Député.

62. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

63. Journal officiel n° C 026 du 30/01/1999 p. 86 - 88

64. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

65. JO C 197 du 12.7.2000, p. 1 ; Cette décision-cadre deviendra caduque le jour où la convention relative à l'entraide judiciaire en matière pénale entre les Etats membres

quement accéléré ce processus qui tendait à s'enliser. Aux termes de la décision-cadre 2002/465/JAI du Conseil du 13 juin 2002, une équipe commune d'enquête sera créée *avec un objectif précis et pour une durée limitée pouvant être prolongée avec l'accord de toutes les parties, pour effectuer des enquêtes pénales dans un ou plusieurs des Etats membres qui créent l'équipe. La composition de l'équipe est arrêtée dans l'accord*.[66]

Pour ce qui relève des perspectives d'avenir, on notera qu'en matière de coopération policière, l'article 111-176 du projet de Constitution rédigé par la Convention dispose que *l'Union développe une coopération policière qui associe toutes les autorités compétentes des États membres, y compris les services de police, des douanes et d'autres services répressifs spécialisés dans les domaines de la prévention ou de la détection des infractions pénales et des enquêtes en la matière*. On le constate : les SR ne sont même pas évoqués !

2.4. Les structures de coopération dans le cadre du « troisième pilier » - PESC/PESD[67]

La dépendance de l'Europe à l'égard du renseignement US, révélée lors de la première guerre du Golfe, et confirmée lors des conflits dans les Balkans, en Afghanistan ou en Irak, convainquit les Etats membres d'améliorer leurs capacités de collecte autonome de renseignement, notamment spatial. Un analyste américain en conclut d'ailleurs que : *Some European governments were frustrated by their inability to provide independent assessments of developments in the Balkans based on their own intelligence, further highlighting Europe's lack of an independent intelligence collection capability to support a CFSP.* [68]

La déclaration franco-britannique de Saint-Malo de 1998, qui constitue un tournant dans le développement de la défense européenne, établit clairement qu'en cas de crise internationale, l'UE devra pouvoir prendre en toute «autonomie » la décision d'une éventuelle intervention: *l'Union doit disposer d'une capacité d'évaluation des situations, de sources de renseignement, et d'une capacité de planification stratégique, sans duplication inutile*. Dans la foulée, les conclusions de la Présidence du Conseil européen de Cologne des 3-4 juin 1999 affirment que *l'objectif est de renforcer la PESC en se dotant d'une politique européenne commune en matière de sécurité et de défense. Cela suppose une capacité d'action autonome s'appuyant sur des capacités militaires crédibles ainsi que des instances et des procédures de décision appropriées.* (…) *En outre, l'Union européenne aura besoin d'un dispositif d'analyse des situations, de sources de renseignements et de moyens lui permettant d'assurer une planification stratégique adéquate.* Enfin, troisième étape, le Conseil européen d'Helsinki des 10-11 décembre 1999 entérine un accord sur le « Headline Goal », *un grand objectif commun européen sera adopté de sorte que des moyens militaires prêts à être déployés et des objectifs collectifs de capacités en matière de commandement et de contrôle, de renseignement et de capacité de projection seront mis au point rapidement, et ce grâce à la coordination volontaire des efforts nationaux et multinationaux, afin de mener à bien l'ensemble des missions dites de Petersberg. (...) Ces forces devraient être militairement autosuffisantes et dotées des capacités nécessaires de commandement, de contrôle et de renseignement, de la logistique et d'autres unités d'appui aux combats ainsi que, en cas de besoin, d'éléments aériens et navals. (...) Les Etats membres ont également décidé de déterminer rapidement des objectifs collectifs de capacité en matière de commandement et de contrôle, de renseignement et de transport stratégique, domaines également identifiés par l'audit de l'UEO.*

Mais la « Déclaration d'engagement de capacités militaires », adoptée lors du Sommet de Laeken de décembre 2001, admet les carences européennes : *en matière de renseignement, outre les capacités d'interprétation d'images du Centre satellitaire de Torrejon, les Etats membres ont offert un certain nombre de moyens qui peuvent contribuer à la capacité d'analyse et de suivi de situation de l'Union européenne. Néanmoins, ils ont noté que des efforts sérieux seront nécessaires dans ce domaine pour disposer à l'avenir de davantage de renseignement de niveau stratégique*. Parmi les seize groupes de travail constitués, on notera que l'un est chargé d'examiner la collecte de renseignements stratégiques ISR IMINT, l'autre les drones (HALE, MALE et drones tactiques). Un premier rapport de synthèse a été finalisé le 1er mars 2003, mais sans être rendu public.

---

de l'Union européenne sera en vigueur dans tous les Etats membres.

66. Journal Officiel L 162, 20 juin 2002

67. Pour le texte complet des documents mentionnés ici, voyez : www.europa.eu.int

68. VILLADSEN Ole, « *Prospects for a European Common Intelligence Policy* », op. cit. Document disponible sur www.cia.gov/csi/studies

En termes de structures, à l'issue du Sommet de Nice de décembre 2000, trois nouveaux organes ont été institués au sein du Secrétariat du Conseil afin de permettre la mise en œuvre de la PESC/PESD : le Comité politique et de sécurité (COPS), le Comité militaire (CMUE) et l'Etat-Major (EMUE). Ces structures ont été déclarées « opérationnelles » lors du Sommet de Laeken de décembre 2001.[69] En outre, le SG/HR dispose d'une division « Renseignement », créée au sein de l'EMUE. Elle contribue à l'évaluation de situation, à l'alerte rapide (veille stratégique) et assure un soutien aux opérations en cas d'engagement européen, mais ne s'occupe pas de renseignement de documentation. Pour fonctionner, elle s'appuie sur une trentaine de personnes (23 officiers et sept sous-officiers). Au moins un expert de chaque Etat membre y participe. Ces experts travaillent tous pour le Directeur de l'EMUE, mais chacun dispose d'une liaison sécurisée vers le service national de renseignement auquel il appartient. Ainsi, il peut recevoir les contributions de son pays et les solliciter en cas de besoin. Cet arrangement a demandé la mise en place d'infrastructures spécifiques et chaque Etat membre a défini quel organisme national est responsable de la fourniture des renseignements. A partir des renseignements reçus cette division doit fournir une évaluation de situation qui ne doit pas forcément « refléter une position européenne commune », qui n'existe pas forcément au moment ou le sujet est présenté au COPS. Les documents produits sont transmis au Directeur général de l'Etat-major, au Comité militaire, au Centre de situation (Cf infra) et aux organismes nationaux de renseignement.[70]

Le Centre de situation (SITCEN) est la clé de l'effort de synergie entre les renseignements d'origine civile et militaire. Placé sous l'autorité du SG/HR, et dirigé par son « Conseiller spécial» il est chargé de lui fournir tous les renseignements nécessaires à l'évaluation et au suivi de la situation. Il comprend une cellule de recueil et d'analyse du renseignement en provenance des services civils de renseignement, cellule constituée par du personnel mis à disposition par les Etats membres. Outre la cellule précitée, son personnel provient de l'UPPAR – que nous évoquerons plus loin –- et de la division Renseignement de l'EMUE. Le SITCEN a un rôle de synthèse de l'information et en assure la diffusion. En cas de crise déclarée, il se transforme en cellule de suivi de crise et assure donc une permanence.[71] Quel que soit le niveau d'information dont le SITCEN dispose, il apparaît que seule une partie réduite est transmise au COPS. Les décisions prises au COPS ne sont pas influencées par les informations soumises par le SitCen, mais bien uniquement par les informations dont les Etats membres disposent à titre national. Il est vrai que le degré de prise de décision au COPS ne réclame sans doute pas de renseignements confidentiels. La recommandation n°706 de l'Assemblée de l'UEO sur les capacités militaires européennes dans le contexte de la lutte contre le terrorisme international estime à cet égard que si le SITCEN est *un acquis important*, il relève toutefois que *dans le domaine du renseignement et de l'évaluation de la menace terroriste en amont, les échanges entre Européens restent organisés dans le cadre de rencontres bilatérales ou de forums à participation restreinte, en fonction des pays réellement impliqués*.[72]

Enfin, l'Unité politique de planification et d'alerte rapide (UPPAR) travaille sous l'autorité du SG/HR ; elle a pour mission de « fournir des évaluations des intérêts de l'Union » en matière de PESC, de donner rapidement l'alerte en cas de situation de crise et d'établir des documents présentant, d'une manière argumentée, des options concernant la politique à suivre. Elle comporte plusieurs sections : Balkans/Europe centrale; PESD; questions horizontales et Amérique latine; Russie/Ukraine/relations transatlantiques/Asie; Méditerranée/Processus de Barcelone; Moyen-Orient /Afrique. Elle est composée d'une vingtaine de personnes et de hauts fonctionnaires du Secrétariat du Conseil et de la Commission. Elle s'appuie sur des informations diplomatiques, économiques, politiques, sociales, ouvertes ou obtenues auprès des missions diplomatiques des pays membres.[73] L'UPPAR est assistée par le SITCEN. Selon nos informations, elle s'appuie aussi sur les éléments donnés

69. Voyez aussi à ce sujet la Decision 2001/80/PESC du Conseil du 22 janvier 2001 instituant l'Etat-Major de l'UE et la Décision 2001/79/PESC du Conseil du 22 janvier 2001 portant création du Comité Militaire de l'UE (JOCE L 27 du 30 janvier 2001).

70. Assemblée de l'UEO, « *Les capacités militaires européennes dans le contexte de la lutte contre le terrorisme international »,* Rapport présenté au nom de la Commission de défense par M. Wilkinson, rapporteur, Document A/1783 3 juin 2002, Quarante-huitième session

71. Ibid.

72. Ibid.

73. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

par une structure de liaison au sein de l'EMUE (des officiers de renseignement de plusieurs pays y sont affectés). Les documents produits sont de nature générale, et constituent des supports utiles au débat en séance. Ils ne constituent cependant pas une source d'information pour les délégations et les Etats membres, qui continuent de s'appuyer exclusivement sur leurs informations d'origine nationale. Ces documents du Secrétariat du Conseil sont utiles pour ébaucher une position européenne commune. Par ailleurs, les informations collationnées par le SITCEN ont sans doute un rôle important à jouer pour alimenter l'action du Haut Représentant et de son cabinet. Selon nos informations, la structure fonctionne plutôt bien, étant donné ses capacités réduites, pour ce qui est de la formulation d'alternatives politiques. En ce qui concerne le renseignement, il semble toutefois qu'elle n'exploite pas pleinement les potentialités qu'offrent, en matière d'information, les services de la Commission (qu'on pense à ECHO, ou aux bureaux de représentation de la Commission à l'étranger). Cela est dû, d'une part, à un certain manque de communication entre la Commission et l'UPPAR, à un manque de « notoriété » de l'UPPAR au sein de la Commission, mais aussi au manque de moyens pour collationner et analyser les informations.

Ces différentes structures ont donc pour mission d'assurer la fonction « renseignement » en phase pré-décisionnelle, puis, dans l'hypothèse d'une intervention, de fournir des évaluations stratégiques qui serviront de base aux travaux de planification opérationnelle de l'état-major de l'opération. Mais l'Assemblée de l'UEO note les carences de passage du niveau « stratégique » au niveau « tactique » : *cet état-major aura besoin de renseignements plus pratiques et plus détaillés pour la conduite de l'opération. La réflexion sur l'organisation du cycle de renseignement au niveau de l'état-major d'opération et de l'état-major de forces déployé sur le théâtre d'opérations est l'objet des travaux actuels conduits par l'EMUE dans le cadre du concept ISTAR (Intelligence, Surveillance and Targeting).*[74] Ajoutons que l'évaluation de la mission ARTEMIS au Congo fournira très certainement de précieux enseignements.

En ce qui concerne les relations entre l'UE et l'OTAN en ce domaine, il faut noter le rôle particulier que devrait jouer le réseau informatisé d'informations confidentielles de l'OTAN, le BICES (*Battlefield Information Collection and Exploitation System*). En fait, l'OTAN n'est pas le fournisseur d'information car ce sont les alliés qui mettent certains documents sur ce réseau. Tous les experts estiment très important de voir le SITCEN ou la division Renseignement disposer d'un terminal sur ce réseau, mais ce n'est pas encore le cas car les arrangements sont encore loin d'être finalisés, notamment du fait de la présence à l'UE de membres n'appartenant pas à l'OTAN. Pour l'instant, le seul accord de sécurité intérimaire entre l'UE et l'OTAN ne permet pas l'échange de renseignement entre l'EMUE/SITCEN et l'OTAN (SHAPE/EMI), mais il faut noter que ces accords et la participation au réseau BICES existaient dans le cadre OTAN/UEO. [75]

L'UE a repris, sous le nom d'« ESDP net », le réseau WEUCOM qui était en place entre le Secrétariat général de l'UEO et les capitales des pays membres (11 pays raccordés). Mais le débit de ce système est considéré comme trop faible pour permettre le contrôle politique et militaire d'une opération en temps réel. Des études sont en cours pour la mise en place d'un système informatisé à grand débit entre le SITCEN/EMUE et les pays membres. [76] L'ESDP-Net servira à échanger des informations de nature miliaire à haut degré de classification entre le SGUE et les Etats membres. Il est à l'heure actuelle en phase d'accréditation et de test dans plusieurs capitales, et ne serait opérationnel qu'en novembre 2003, voire fin avril 2004 dans les futurs Etats membres où se posent des problèmes de financement, de matériel et de sécurité.

Enfin, on notera que le Conseil a adopté des mesures strictes de protection des données. On se référera principalement à la Décision 2001/264/CE du Conseil du 19 mars 2001 adoptant le règlement de sécurité du Conseil.[77] Les bâtiments du Secrétariat sont sécurisés. Le Conseil s'est également fait construire des salles de réunion sécurisées. Les habilitations des personnes amenées à manipuler des documents confidentiels sont vérifiées. La Commission (Direction Générale RELEX, département COPS) suit les mêmes règles. En pratique, comme le montre le fonctionnement de la « clearing house » chargée d'établir la liste des organisations terroristes au titre de la position commune 931/01, les procédures de garantie du secret sont inefficaces : les positions des Etats

74. Ibid.

75. Ibid.
76. Ibid.
77. Journal Officiel L 101 du 11 avril 2001, p. 1

membres sont parfois dès le lendemain dans la presse. Si les procédures utilisées au sein du Conseil sont sans doute compatibles avec celles de l'OTAN, le degré de protection des Représentations permanentes des Etats membres est, pour utiliser une litote, « variable ». Plus généralement, le manque de confidentialité est sans doute moins dû aux procédures qu'à la « culture d'entreprise » au sein de l'Union, qui est extrêmement ouverte.

Globalement, l'Assemblée de l'UEO tire de ces développements récents un bilan somme toute positif : *l'organisation se met en place de façon satisfaisante, et que le personnel détaché par les pays est de qualité et couvre par sa compétence les divers secteurs de crise. L'EMUE a déjà adressé des demandes de renseignements aux services nationaux qui ont été en grande partie satisfaites. Enfin, des réunions des directeurs des services de renseignement militaires des pays membres commencent à se tenir régulièrement sous chaque présidence.*[78]

78. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

III. Les conditions d'un approfondissement de la coopération européenne

Si « l'Europe du renseignement » est restée au stade des déclarations d'intention, c'est sans doute parce que le problème est plus complexe que les responsables politiques ne l'imaginaient, mais aussi que les SR eux-mêmes témoignent d'une certaine frilosité à reconsidérer leurs méthodes de travail.

Nous développerons maintenant les conditions requises pour un approfondissement de la coopération entre SR, sous forme d'une quintuple nécessité : la nécessité d'une volonté politique forte ; d'établir des structures de coopération réalistes et efficaces ; de définir les besoins de l'UE en matière de renseignement ; d'assurer un contrôle démocratique au niveau européen ; d'adopter une approche différenciée en fonction des différents moyens de collecte du renseignement.

1. La nécessité d'une volonté politique forte

La première condition à l'approfondissement de la coopération entre SR réside bien entendu dans l'existence d'une volonté politique forte.

Il y a un demi-siècle, cette volonté fut exprimée par des responsables visionnaires – Monnet, Spaak, de Gasperi, Schuman - porteurs d'un projet original et ambitieux. Mais force est de constater que les progrès les plus récents de l'intégration furent réalisés sous la pression d'un « intérêt », essentiellement de nature économique, comme le Grand Marché en 1993, puis le passage à l'Euro en 2002. En octobre 1999, déjà, les conclusions d'un colloque de l'Institut des Hautes Etudes de Défense Nationale étaient pessimistes sur les perspectives d'une telle coopération en matière de renseignement : *en l'absence de risque mortel commun à tous les pays alliés, on peut se demander dans quelle mesure la coopération peut fonctionner de façon harmonieuse tant que subsistent de grandes divergences d'approche des intérêts géopolitiques et une forte concurrence commerciale. Le renseignement n'est-il pas un des derniers refuges de la souveraineté des Etats ?* [79] Les Etats membres de l'UE n'auraient-ils donc pas un « intérêt vital » à coopérer davantage en matière de renseignement ? L'époque où les SR symbolisaient l'autorité d'un Etat dans ses prérogatives « régaliennes » n'est-elle pas révolue ? Même le plus borné des souverainistes serait enclin à l'admettre et à rejoindre Alessandro Politi pour qui, *si les services de renseignement sont la représentation et la concrétisation ultimes de la raison d'Etat, deux questions majeures se posent aujourd'hui en Europe occidentale : de quel Etat s'agit-il ? Qui cette raison d'Etat représente-t-elle ? A la veille de l'introduction de l'euro, l'Etat-nation d'Europe occidentale n'est sûrement pas l'entité toute puissante qui caractérisait le paysage du continent au début du siècle.* [80] Et pourtant …

Un approfondissement de la coopération européenne entre SR devra évidemment s'intégrer dans le nouveau contexte géo-politique. D'éminents spécialistes l'ont répété à l'envi : le 11 septembre 2001 représente une césure. Le titre de l'ouvrage d'Alexandre Adler est révélateur à cet égard : « *j'ai vu mourir le monde ancien* ». Mais force est de constater que tous les Etats membres (actuels ou à venir) n'ont pas la même lecture de ce bouleversement : les interventions successives en Afghanistan et en Irak ont montré une approche différente du « nouvel ordre mondial », certains n'hésitant pas opposer – de manière, selon nous, réductrice voire caricaturale – la « nouvelle » et la « vieille » Europe.

Les conséquences du 11 septembre sur le processus d'intégration européenne doivent être analysées avec finesse et différenciées selon les thèmes abordés. D'une part, le double processus d'approfondissement de l'intégration, et d'élargissement, n'a pas été entravé : une Convention sur « l'avenir de l'Europe » a été instituée, tandis que les négociations d'adhésion se sont poursuivies. La coopération entre SR de l'UE – dont les missions relèvent tant du domaine civil que du domaine militaire – ne peut manquer de subir les effets des forces centrifuges de l'approfondissement de la coopération en matière JAI, et des forces centripètes des divergences graves révélées en matière de PESC/PESD. A l'initiative de la Présidence belge, des progrès considérables ont été réalisés en matière de coopération JAI, avec l'extension du mandat d'Europol, la constitution d'équipes d'enquêtes communes, la mise en œuvre d'Eurojust, le renforcement des mesures anti-blanchiment, le mandat d'arrêt européen. Ces avancées suscitèrent de vifs espoirs dans les

79. « *L'adaptation de l'outil de renseignement français au nouveau contexte* », Rapport de l'Institut des Hautes Etudes de Défense Nationale, octobre 1999

80. Ibid.

rangs des partisans d'une Union fédérale, qui virent dans le 11 septembre 2001 un facteur d'accélération de l'intégration. Mais par contre, dans le domaine de la PESC/PESD, l'Europe s'est déchirée sur la place publique. D'une part, le modus operandi de l'opération militaire en Afghanistan fut déjà révélateur de « l'absence de l'Europe », puisque l'UE s'avéra incapable d'envoyer, sous son drapeau et son égide, une contribution à l'ISAF (Force de stabilisation) et que les différents contingents ont été déployés sur décision nationale ; tandis que, fidèles à leur nouvelle doctrine selon laquelle « la mission détermine la coalition » (et non l'inverse), les Etats-Unis ont monté l'opération « Libertés Immuables » avec des troupes essentiellement anglo-saxonnes (Grande-Bretagne, Australie, Nouvelle-Zélande, Canada), même si des troupes françaises ou allemandes sont aussi intervenues. Mais d'autre part, l'émergence, au cours de l'année 2002, du dossier irakien s'est révélée autrement plus « dramatique » pour la cohésion de l'UE : si la Grande-Bretagne et l'Espagne (et plus discrètement l'Italie, le Danemark, les Pays-Bas ainsi que certains Etats candidats) ont rejoint le camp des Etats-Unis, partisans d'une intervention armée, même sans aval des Nations Unies, la France, l'Allemagne et la Belgique) se sont opposés à Washington et, concluant une entente avec la Russie, pour privilégier le désarmement pacifique de l'Irak via les missions d'inspection de l'ONU.

De plus, d'aucuns ne se privent pas d'évoquer, à l'instar de l'Assemblée de l'UEO, la « relation spéciale » entre les Etats-Unis et la Grande-Bretagne *(qui) ne facilite pas cette perception de la nécessaire autonomie de l'UE dans ce domaine du renseignement, ni la mise sur pied d'un système de coopération européenne, dans la mesure où la Grande-Bretagne ne désire pas investir dans des satellites d'observation et ne peut pas partager avec les Européens tous les renseignements qu'elle possède. Cette situation peut conduire à des perceptions différentes de la crise, même si cela n'explique pas toutes les différences d'appréciation entre pays membres de l'Union.*[81] L'Assemblée Nationale française relevait, elle aussi, que *la construction de l'Europe de la défense comportera de manière inévitable un volet relatif au renseignement et conduira à de nouvelles relations entre membres de l'Union européenne notamment avec le Royaume-Uni. Une réflexion est d'ailleurs engagée dans ce pays sur la mise en commun du renseignement tout en maintenant un lien spécifique avec les Etats-Unis. Le développement de la coopération est cependant indissociable de la confiance entre partenaires car il n'y a pas de vérification possible entre eux. Les suspicions et les doutes doivent s'effacer.* [82]

Par ailleurs, la coopération en matière de « renseignement de défense » doit s'intégrer dans la « constellation institutionnelle » de la défense de l'Europe. Rappelons en effet que onze Etats membres de l'UE (Allemagne, Belgique, Danemark, Espagne, France, Grèce, Italie, Luxembourg, Pays-Bas, Portugal et Royaume-Uni) sont aussi membres de l'OTAN. A l'exception du Danemark, ils appartiennent également à l'UEO. Quatre Etats membres de l'UE (Autriche, Finlande, Irlande et Suède) ont le statut de pays neutres ou non-alignés, mais coopèrent avec l'OTAN au titre du Programme du Partenariat pour la Paix (PPP) et participent au Conseil de partenariat euro-atlantique (CPEA). Ils ont également un statut d'observateur à l'UEO. Le Danemark est un cas particulier puisqu'il bénéficie, dans le cadre de l'UE, d'un régime spécial (tel que défini dans un protocole annexé au traité). Quatre des futurs Etats membres de l'UE (Hongrie, Pologne, République tchèque, Turquie) sont déjà membres de l'OTAN, d'autres ont été invités à rejoindre l'OTAN lors du sommet de Prague des 21 et 22 novembre 2002. Les pays candidats à l'Union européenne déjà membres de l'OTAN sont également « membres associés » de l'UEO, les autres (Bulgarie, Estonie, Lettonie, Lituanie, Roumanie, Slovaquie, Slovénie) ont le statut de « partenaires associés » et gagneront certainement le statut de « membres associés » après leur adhésion à l'OTAN. Deux des pays candidats restent non-alignés (Chypre et Malte).[83]

2. Des structures de coopération réalistes et efficaces

Mais en ce domaine comme dans d'autres, la coopération – ou l'intégration – européenne ne se fera pas sans un respect de la diversité qui caractérise l'UE, comme le confirme l'Amiral Lacoste : *pour comprendre le rôle des Services*

81. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

82. Assemblée Nationale, Rapport d'information n°2623 du 11 octobre 2000, op. cit.

83. Rapport du Président du Groupe de travail VIII « Défense » à la Convention, 16 décembre 21002, CONV 461/02

Spéciaux dans les sociétés modernes et pour définir leur place dans les institutions, il est indispensable de tenir compte de l'expérience et des traditions propres à chaque culture nationale.[84] Un rapport de l'Assemblée Nationale française relève d'ailleurs que *deux pays, comme la France et le Royaume-Uni, qui ont une longue tradition de services de renseignement, s'opposent sur l'image différente du renseignement dans l'opinion publique. En France, le renseignement a une connotation souvent péjorative, ses réussites sont tues et il est souvent assimilé aux services d'action dont les échecs sont médiatisés. Le Royaume-Uni a en revanche su cultiver auprès de ses élites une image valorisante de la communauté du renseignement. Plus la proximité culturelle est grande entre pays, plus il est facile de s'allier sur des sujets sensibles comme le renseignement. Les relations de connivence qu'entretiennent souvent les pays anglo-saxons favorisent ce type d'alliance.*[85] Pour Michael Herman, *qu'importe leur degré d'imbrication, les services de renseignements nationaux et étrangers des pays démocratiques sont assujettis à des restrictions légales et politiques très différentes et il s'y développe, en conséquence, des tournures d'esprit distinctes. Réussir à les fusionner semble difficilement réalisable, voire souhaitable*.[86] Le Général François Mermet résume très justement : *nous parlons des hommes, avec leurs cultures, leurs identités, qui sont bien sûr beaucoup plus difficiles à infléchir que des concepts organisationnels*. [87]

Définir des structures permettant un approfondissement de la coopération entre SR est un exercice auquel peu d'auteurs se sont livrés.

Pour l'Assemblée de l'UEO, *l'idéal serait de constituer une véritable « Europe du renseignement », efficace et cohérente, et dotée de l'architecture appropriée. Mais ceci ne peut être envisagé à court terme car tout est à construire dans un domaine très sensible pour les souverainetés nationales.* L'Assemblée formule donc des propositions considérées comme davantage réalisables à court terme, comme officialiser les réunions de directeurs nationaux du renseignement et organiser des réunions thématiques (terrorisme, renseignement de défense, crises en cours) ; instituer auprès du SG/HR un « Service de renseignements sur les zones de crises », composé de représentants des services nationaux de renseignements des Etats membres sur le modèle de la division Renseignement de l'EMUE (qui sera par ailleurs développée pour être capable d'assurer le suivi de tous les théâtres de crises potentielles) ; développer et militariser le CSUE qui devra être capable d'assurer l'interprétation de tous types d'images ; inciter les Etats membres à investir une part croissante de leur budget de défense dans les systèmes de recueil de renseignement dans une démarche de coopération européenne ; développer les forces spéciales et les unités chargées du recueil du renseignement, et favoriser leur coopération par l'organisation d'exercices appropriés. L'Assemblée suggère encore la création d'une « unité de renseignement et de lutte contre le terrorisme », qui entretiendrait des rapports étroits avec la branche renseignement de l'EMUE et avec la cellule antiterroriste d'Europol. [88] L'Assemblée de l'UEO propose aussi de définir une politique européenne du renseignement, préparée et décidée par le Conseil. Une Haute autorité européenne du renseignement serait chargée de proposer au Conseil la politique à adopter, puis de l'appliquer sous la direction du COPS. [89]

Dans l'étude « Vers une politique européenne de renseignement » publiée par l'Institut d'Etudes de Sécurité, Klaus Becher, Bernard Molard, Frédéric Oberson et Alessandro Politi tablent, dans un premier temps, sur une « coopération informelle » accrue entre SR, tout en précisant que *les thèmes examinés devraient être suffisamment techniques pour être traités sans exiger au préalable des mandats politiques contraignants*. Il permettrait d'accroître la confiance *entre les grandes et les petites instances, ainsi qu'entre les nouveaux et les anciens alliés*. Ensuite, lorsqu'il s'agira de réaliser des évaluations communes, les réseaux d'experts externes connus de chaque service seraient progressivement inclus, contribuant à la création *de facto* d'un réseau *ad hoc* d'experts. Ce réseau, qui fonctionnerait ensuite *de façon plus souple*

84. LACOSTE Pierre, « *Missions et déontologie des Services Spéciaux »*, SISDE (Servizio per le Informazioni e la Sicurezza Democratica, – Rivista di intelligence e di cultura professionale, n°11 May-August 1998.
85. Assemblée Nationale, Rapport d'information n°2623 du 11 octobre 2000, op. cit.
86. HERMAN Michael, « Le renseignement après le 11 septembre : un point de vue britannique », Commentaire n° 83, Publication du Service Canadien du Renseignement de Sécurité, 17 juillet 2003 (disponible sur le site csis-scrs.gc.ca)
87. Le Figaro, 8 octobre 2001
88. Ibid.
89. EHRHART Hans-Georg, « *Quel modèle pour la PESC* ? », Cahiers de Chaillot, n°55, Institut d'Etudes de Sécurité de l'Union Européenne, Paris, Octobre 2002.

et plus systématique, devrait disposer de bases de données de haut niveau qui contribueraient à *une confiance mutuelle*. Mais les auteurs sont plus ambitieux : *alors que cette approche du bas vers le haut s'impose progressivement, une approche du haut vers le bas pourrait simultanément être envisagée. Les acteurs seraient des instances parlementaires, à la fois nationales et internationales, et des gouvernements*, même s'ils admettent que *les gouvernements évolueront probablement à un rythme plus lent*.[90] Ils estiment toutefois que *l'intégration du renseignement ne prendra probablement pas la forme d'une « agence de renseignement européenne » supranationale. Les structures, les moyens et le financement resteront généralement nationaux, tout comme les efforts entrepris pour promouvoir la coopération et l'intégration. Les cultures nationales existantes dans le domaine du renseignement et leur capacité de s'adapter aux nouveaux besoins limiteront les perspectives des nations de l'UE concernant l'édification d'une assise intégrée pour leurs politiques étrangères, de sécurité et de défense*.[91] En conséquence, *le renseignement européen devra être synthétisé par l'intermédiaire d'un réseau intergouvernemental et interadministratif qui n'existe pas encore même sous une forme rudimentaire. (...) le processus pourrait aboutir, en plus d'un réseau concret entre agences, à la création d'une instance intergouvernementale de hauts responsables du renseignement - un conseil européen d'évaluation du renseignement - aidé par un comité de rédaction. Cela constituerait un cadre commun régulier permettant d'évaluer les renseignements, qu'ils soient fondamentaux ou d'actualité, sur des questions spécifiques revêtant une importance immédiate ou future, telles que, par exemple, la situation au Kosovo. Sa principale fonction serait d'éviter que les politiques communes de l'Europe soient entravées par un renseignement « non consolidé ». Surtout, il lui faudrait définir de façon aussi opportune que possible, dans chaque cas, dans quelle mesure l'existence de divergences entre les capitales de l'UE se fonde sur des interprétations différentes de données disponibles, reflète une information qui n'a pas encore été prise en compte par les autres, et persiste en dépit d'une évaluation commune de la situation. C'est seulement à partir du moment où un tel mécanisme existera que la politique européenne étrangère, de sécurité et de défense pourra véritablement prétendre exprimer une position commune.* [92]

Alessandro Politi propose plusieurs modèles susceptibles de contribuer au développement d'une coopération entre SR européens. Le premier modèle table sur une « évolution naturelle », qui commencerait par un accroissement de la coopération informelle entre Etats membres, et débouchant sur une structure plus formalisée. Le second modèle offre une approche plus organisée fondée sur trois cercles de coopération: un « cercle extérieur » avec des réunions annuelles d'organisations gouvernementales et non-gouvernementales intéressées par le renseignement qui se réuniraient en « terrain neutre » ; un « cercle intérieur », par une réunion formelle des agences de renseignement chargées de la supervision des besoins en la matière ; et enfin, un « troisième cercle » qui assurerait la gestion des demandes de renseignement. [93]

Enfin, le Général François Mermet, qui dirigea la DGSE française de 1987 à 1989 propose la création d'un conseil de sécurité sur le modèle du Joint Intelligence Committee britannique, à savoir *un conseil indépendant de l'état-major des armées dirigé par Javier Solana qui réunisse, sans lien hiérarchique, tous les protagonistes du renseignement, des grandes entreprises aux militaires en passant par les diplomates, les banquiers, les avocats*. [94]

Les propositions émises ci-dessus ont le grand mérite de poser en termes concrets un certain nombre d'hypothèses de travail. Néanmoins, elles pêchent selon nous par leur caractère « global » relevant d'une approche insuffisamment différenciée que pour prendre en compte les particularités de la « communauté du renseignement ». Il en va ainsi de la distinction entre les différentes missions des SR : contre-espionnage et renseignement « intérieur », d'une part, et « renseignement extérieur » d'autre part ; des particularités du « renseignement de défense » ; des conséquences de la logique des « piliers » de l'UE, et notamment de la distinc-

90. POLITI Alessandro, « *De la nécessité d'une politique européenne de renseignement* », op. cit.
91. Ibid.

92. BECHER Klaus, « *Une politique européenne de renseignement: les besoins politiques et militaires »* in BECHER Klaus, MOLARD Bernard, OBERSON Frédéric et POLITI Alessandro, « *Vers une politique européenne de renseignement* », Les Cahiers de Chaillot, Institut d'Etudes de Sécurité de l'UEO, Décembre 1998.
93. POLITI Alessandro, "*Towards a European intelligence policy*", cité in BAKER Charles, « *The search for a European intelligence policy* », cjb7@aber.ac.uk
94. Le Figaro, 8 octobre 2001

tion entre le « second pilier » (JAI) et le « troisième pilier » (PESC/PESD).

Fondamentalement, que décide-t-on d'échanger ? Des informations « brutes », non traitées ? Des informations « recoupées » (des renseignements) ? Des analyses ?

Dans le domaine JAI, il s'agit en outre de déterminer le « niveau » des échanges de renseignement : faut-il opérer au niveau des chefs de service sur le modèle du Club de Berne, ou évoluer vers un niveau plus « opérationnel », et promouvoir les échanges entre analystes et agents de terrain. Dans un second temps, il faudra déterminer la structure : faut-il opter pour une structure permanente, de type Europol, avec un staff propre et des officiers de liaison ? ou faut-il se contente d'une structure non-permanente, de type OTAN, fondée sur des réunions régulières ? En fonction du choix de la structure, on pourra envisager de « valoriser » le modèle Europol, notamment sous le double aspect de « structure de travail collectif » entre professionnels et de gérant de bases de données informatiques permettant des échanges d'informations en temps réel. On pourra également examiner l'opportunité de « valoriser » le modèle des équipes d'enquête communes, bien qu'il soit sans doute prématuré d'évaluer leur apport réel. Enfin se pose la question du droit d'initiative de la Commission, du contrôle démocratique du Parlement européen et du contrôle juridictionnel de la Cour de Justice. Mais ce débat relève d'une problématique plus générale quant à l'avenir de la structure en piliers de l'UE.

Pour ce qui est du renseignement dans le cadre de la PESC/PESD, nous distinguerons, pour la clarté de notre propos, le renseignement stratégique du renseignement tactique, chacun étant en effet intégré dans une logique et une dynamique propre.

En matière de renseignement stratégique, deux options semblent envisageables : soit on continuera de s'appuyer sur les structures développées actuellement par le HR ; soit on misera sur la création éventuelle d'un Conseil des ministres de la défense, et une réunion des chefs des services de renseignement des Etats membres pourrait alors en constituer un sous-groupe de travail, à l'image du groupe K4 pour le Conseil JAI. En fait, les deux options pourraient autant être complémentaires que paralysantes. Elles seront complémentaires si leur articulation respecte une hiérarchie des tâches : les chefs de service détermineront des stratégies et des options communes, tandis que les structures du HR réaliseront un travail de synthèse quotidien. Mais elles seront paralysantes si les responsables politiques restent dans une logique intergouvernementale.

En matière de renseignement tactique, les capacités européennes dépendront de deux facteurs. D'une part, les Etats membres seront, tôt ou tard, contraints de prendre davantage en compte les conséquences budgétaires d'investissements et d'achats de matériels coûteux et de haute technologie, particulièrement dans les domaines du SIGINT, du COMINT et de l'IMINT. Si l'Europe peut d'ores et déjà faire état de réalisations concrètes notables dans des domaines aussi variés que l'Airbus A-400M ou Hélios II, d'aucuns entendent oeuvrer à la constitution d'une « agence européenne de l'armement » (qui irait beaucoup plus loin que les structures actuelles, comme l'OCCAR ou le GAEO), et donc la suppression de l'article 296 du TUE qui soustrait les entreprises de l'armement aux règles de la libre concurrence communautaire. D'autre part, la multiplication de Corps d'Armées – actuellement un peu cacophonique – impliquera inéluctablement une standardisation des équipements et une prise en compte croissante de l'aspect « renseignement » dans la planification des opérations et des exercices des troupes. En terme de personnel, les forces armées des Etats membres disposent déjà d'un potentiel non négligeable, de grande qualité, d'unités capables d'effectuer des missions de renseignement tactique.

Enfin, l'UE serait selon nous heureusement inspirée de développer une approche commune en matière d'installation « d'officiers de liaison » : nous faisons ici allusion aux réseaux des attachés de défense (considérés comme officiels) et des « résidents » des services de renseignement civils (considérés comme « quasi » officiels). Les attachés militaires dépendent souvent de leur service de renseignement national même s'ils ne font pas nécessairement du « renseignement » à proprement parler, puisqu'ils sont facilement identifiables (bien que cela doive être relativisé selon les pays d'accréditation). Une coopération européenne pourrait certainement s'instaurer à ce niveau. On pourrait imaginer des réunions régulières et formelles des attachés militaires de l'UE dans les pays où ils sont accrédités. Ils pourraient confronter leurs informations et leurs analyses, dont ils feraient ensuite rapport à leurs services nationaux. Les plus petits Etats membres, qui

n'ont pas les moyens de développer des réseaux très étoffés, bénéficieraient ainsi d'informations sur des zones où ils ne sont pas implantés. Cette réunion des attachés militaires pourrait être présidée soit par le représentant de l'Etat assurant la Présidence de l'UE, soit par le représentant de la délégation de la Commission sur place. On y verra un progrès symbolique : la Commission pourrait disposer, petit à petit, d'une expertise militaire. Enfin, une coopération européenne pourrait aussi s'instaurer entre les « résidents » des services civils, avec toutefois la réserve que ces agents mènent une existence qui se veut plus discrète, sous couverture diplomatique.

3. La nécessité de définir les besoins de l'UE en matière de renseignement

Chacun s'accorde à pointer le terrorisme international – et singulièrement celui constitué par le fondamentalisme islamiste - comme la menace la plus immédiate pour la sécurité de l'UE. Sans prétendre le moins du monde minimiser l'évidence de cette affirmation, il nous semble toutefois nécessaire d'élargir le débat en prenant en considération d'autres paramètres. A défaut, l'Occident commettrait la même erreur qui lui fit se focaliser sur le Pacte de Varsovie, à l'Est – sans voir l'émergence d'autres problèmes – au Sud. Or, force est de constater qu'une telle réflexion fait défaut à l'UE.

Le travail de la JAI reste fondé sur les conclusions du Sommet de Tampere de 1999 qui vise à réaliser un « espace de liberté, de sécurité et de justice », complétées de manière disparate par des textes ultérieurs, comme les conclusions du Conseil européen de Séville de juillet 2002.

Pour ce qui est de la PESC/PESD, l'UE s'est longtemps révélée incapable de réaliser un « Livre Blanc sur la Défense », qui déterminerait ses intérêts, sa doctrine d'intervention et les moyens dont elle dispose (ou devrait disposer). Le récent rapport du HR Javier Solana, « Une Europe sûre dans un monde meilleur – stratégie européenne de sécurité », vise à combler cette lacune. Sans entrer dans une analyse complète de ce document, qui sortirait du cadre de la présente étude, bornons nous de constater que s'il établit que *nous devons être prêts à agir avant qu'une crise se produise*, il n'en tire pas pleinement les conséquences en matière de renseignement, qui reste absent du chapitre « développement des capacités ». Tout au plus est-il mentionné *que pour faire face au terrorisme, il faut parfois combiner le recours au renseignement et à des moyens policiers, judiciaires, militaires et autres*.[95] On continue de s'interroger sur l'opportunité autant que sur la portée du terme « parfois »…

4. La nécessité d'assurer le contrôle démocratique des SR au niveau européen

Remparts et défenseurs de la démocratie dans les Etats de droit, les SR s'en sont aussi, dans l'histoire, parfois révélés les fossoyeurs : il n'est pas de dictature qui ne se soit appuyée sur ses « services secrets » comme instrument de répression. Et pourtant, Bismarck n'évoquait-il pas « un métier de Seigneurs » ?

S'il est illusoire – voire franchement naïf – d'attendre d'un SR qu'il respecte scrupuleusement les prescrits légaux – « raison d'Etat » ou « cynisme d'Etat » oblige –, l'Amiral Lacoste, ancien directeur de la DGSE française, prend très justement la mesure du problème : *à une époque où les principes démocratiques et les droits de l'homme sont de plus en plus reconnus comme des valeurs universelles, les citoyens de tous les pays tendent à exiger de leurs gouvernements la transparence dans la conduite des affaires publiques. Beaucoup sont réticents à admettre que les hommes politiques et les administrations puissent arguer du « Secret d'Etat » pour dissimuler certaines informations à leurs concitoyens. Au-delà des aspects sensationnels ou des polémiques portant sur des cas particuliers, il s'agit bien là d'un sujet capital, car il est éminemment politique, au sens noble du mot. C'est un débat de société qui ne devrait laisser personne indifférent*.[96]

Selon nous, l'Assemblée de l'UEO a raison de souligner que *la recherche du renseignement se heurte toujours à un problème de déontologie : il existe une limite éthique aux moyens que l'on peut employer pour la recherche du renseignement. C'est un problème de démocratie, qui exige un suivi parlementaire et une connaissance sans faille des lois et règlements par les services concernés*.[97] Dans un autre rapport, l'Assemblée conclut à juste titre que le contrôle démocratique est donc impératif : (…) *une série*

95. Pour le texte complet, voyez : http://www.grip.org/bdg/pdf/g4054.pdf
96. Compte-rendu du colloque « Secret d'Etat ou transparence ? », 20 janvier 1999 - Comité permanent de contrôle des services de renseignement, Rapport d'activités 1999
97. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

de contrepoids doit être mise en place au sein de la société démocratique contemporaine pour garantir le respect des lois qui gouvernent l'existence et l'activité des centres d'investigation et de renseignement: ainsi, tandis que le pouvoir exécutif en supervise la gestion et que le pouvoir judiciaire remédie aux manquements à la loi, le pouvoir législatif est appelé à régler par la loi le cadre d'action et à contrôler le respect de celui-ci.[98] Mais il n'en reste pas moins que l'exercice reste difficile : *les renseignements nécessaires à la sécurité de l'Etat sont toutefois bien particuliers, et par nature leur contenu ne peut pas être dévoilé à l'avance ni, dans bien des cas, être discuté et porté à la connaissance de l'opinion publique. Les services ne peuvent pas non plus être dirigés trop méticuleusement, ni contrôlés dans les détails, car leur efficacité opérationnelle risquerait d'en souffrir. En même temps, il s'agit d'une activité exercée dans des pays démocratiques, où les droits à la liberté et à la dignité individuelle sont respectés par le système, et où l'opinion publique n'admet pas les abus de pouvoir. Dans ce contexte, il est difficile de concilier les exigences de confidentialité et l'exercice du contrôle parlementaire ainsi que le respect des droits des citoyens.*[99]

Les Parlements, émanation de la représentation populaire, constituent évidemment les enceintes les plus indiquées pour l'exercice de ce contrôle. L'examen de la situation en Allemagne, en Autriche, en Belgique, en Espagne, en Italie, aux Pays-Bas et au Royaume-Uni montre que ces pays se sont tous dotés, entre 1952 et 1994 de dispositifs *ad hoc* constitués selon des modalités très diverses. Les missions et les compétences des instances parlementaires de contrôle sont également très différentes.[100]

Dans la perspective d'une plus grande coopération entre SR au niveau européen se posera tôt ou tard la question du rôle dévolu au Parlement européen, seule institution élue au suffrage universel direct, émanation de la volonté des peuples d'Europe, dans le contrôle démocratique. Si le PE apparaît évidemment comme le dépositaire « naturel » de ce contrôle, il y a fort à parier que les Etats, à travers leurs gouvernements, renâcleront, comme ils le firent pour l'exercice du contrôle démocratique sur EUROPOL.

5. La nécessité d'une approche différenciée

Il nous semble fondamental de procéder à une analyse différenciée des différents aspects du travail des SR, d'une part en distinguant la récolte (ou l'acquisition) du renseignement, de son analyse (ou de son exploitation), et, d'autre part, en affinant le propos en fonction des différents moyens d'acquisition du renseignement : les « sources ouvertes (OSINT ou Open Sources Intelligence) ; le renseignement humain (HUMINT ou Human Intelligence) ; et les différentes formes de renseignement technique : SIGINT (ou Signal Intelligence) ; IMINT (ou Imagery Intelligence). Nous n'évoquerons pas ici le MASINT (ou Measurement and Signature Intelligence).

5.1. OSINT (Open Sources Intelligence)

Haut fonctionnaire civil et spécialiste du renseignement et de l'informatique, Robert David Steele fut chargé en 1988 de créer le US Marine Corps Intelligence Center, avec un budget initial de 20 millions USD. Mais quelques mois plus tard, il se rendit compte que son système informatique sophistiqué, connecté sur les banques de données des autres agences de renseignement américaines, supposées performantes comme la CIA, la NSA ou la DIA ne lui était d'aucune utilité : il n'y trouvait aucune information sur les pays où les Marines étaient susceptibles d'intervenir, comme la Somalie. Par contre, un simple ordinateur personnel doté d'un modem lui ouvrait l'accès aux banques d'informations privées comme Lexis-Nexis, Easynet ou Jane's Information Group, qui, pour un coût annuel de 20.000 USD seulement, rencontraient bien plus la majeure partie des besoins des Marines.[101] Ainsi naquit le concept de « Open Sources Intelligence » ou OSINT.

La notion de « sources ouvertes » doit être définie clairement.[102] En effet, le concept

98. Ibid.
99. Assemblée de l'UEO, « *Le contrôle parlementaire des services de renseignement dans les pays de l'UEO – Situation actuelle et perspectives de réforme* », rapport présenté au nom de la commission pour les relations extérieures et publiques par Mme Kestelijn-Sierens, Document A/1801 du 4 décembre 2002
100. Sénat français, « *Le contrôle parlementaire des services de renseignement* », Les documents de travail du Sénat – Série législation comparée – n° LC 103, Mars 2002
101. CLOUTIER Pierre, « *Renseignement et sécurité dans l'âge de l'information: les défis du Québec* », Centre de recherche sur la sécurité et le renseignement, cloutip@cam.org
102. Nous n'aborderons pas ici la question des entreprises de renseignement privé, et notamment « d'intelligence économique » - à ne pas confondre avec l'espionnage économique ou industriel.

OSINT est mal connu et l'objet de malentendus. On se référera ainsi à la définition de l'OTAN, qui définit l'OSINT comme *le renseignement provenant d'informations accessibles au public et autres informations non classifiées dont la diffusion publique ou l'accès sont limités.* [103]

Pour la doctrine US, l'avantage serait considérable : *OSINT, if done correctly and systematically by knowledgeable professionals, is as rigorous, timely and focused as any other intelligence source available to decision makers*.[104] Le Comité R ajoute que *l'importance croissante des sources ouvertes s'explique par les nouvelles possibilités offertes par l'informatique et la télécommunication. Actuellement, il est possible de trouver très vite de l'information dans différents réseaux et bases de données et d'établir des recoupements. L'accès à l'information est simultané à l'échelle mondiale, grâce à la communication des données électroniques.* [105] Mais si le Comité R relève l'importance d'Internet, *version électronique de la bibliothèque légendaire d'Alexandrie*, il n'en constate pas moins que *le réseau Internet est trop anarchique et pas assez organisé pour constituer un outil vraiment utile pour les services de renseignements. L'information exacte ne peut être trouvée dans un délai acceptable, et est en outre parfois fausse.*[106] L'OSINT englobe en effet bien davantage qu'Internet, face visible d'un immense iceberg qui ne cesse de grossir.

D'aucuns insistent sur la fonction de complément, non de remplacement, de l'OSINT. Lors d'un congrès organisé en 1995 par « Open Source Solutions », une organisation privée spécialisée dans ce type de recherche, et dont la teneur fut rapportée par un membre du Comité R, il fut relevé que *les sources ouvertes restent complémentaires par rapport au travail classique du renseignement. Les sources ouvertes servent par exemple à vérifier la véracité des renseignements fournis par des informateurs. Elles permettent de situer l'information dans un contexte plus large. Cependant, celui qui travaille avec des sources ouvertes, se trouve inévitablement confronté à une situation paradoxale. En effet, beaucoup d'informations et de renseignements utiles aux besoins des services peuvent être trouvées dans les sources ouvertes. Le problème reste de savoir si ces informations sont complètes.*[107] Ce concept de « complément » est battu en brèche par Jacques Dewatre, qui va beaucoup plus loin et prédit une véritable « révolution » dans le monde du renseignement dont les objectifs deviendraient, dès lors, beaucoup plus ciblés : *dans un monde de plus en plus ouvert, de plus en plus affranchi des contraintes de l'espace et du temps, l'information tend à réduire le domaine d'activités des services de renseignement à l'essentiel, c'est-à-dire la recherche de l'information la plus secrète et la plus inaccessible. (...) Le champ du secret s'est donc déplacé. L'investigation clandestine apparaît alors comme la « pointe de diamant » du travail de renseignement, celle chargée de s'attaquer à ce qui résiste à l'investigation en sources ouvertes. Mais cela ne signifie pas que cette dernière en soit moins du renseignement : car ce qui fait sa valeur, c'est tout le travail de vérification, de recoupement et de synthèse, qui fait du produit final un renseignement de haute valeur qui doit être protégé, c'est-à-dire classifié, au même titre que les renseignements recueillis par moyens « discrets ».*[108]

Faut-il dès lors privatiser pour mieux gérer ?

Afin d'atteindre une utilisation optimale de cette vaste expertise et connaissance, Robert Steele introduit le concept de « Virtual Intelligence Community », fondée sur l'idée que les SR peuvent limiter leurs coûts et réunir des informations utiles en collaborant avec le secteur privé. Ainsi, le « service de renseignement de l'avenir » *s'offrira les services d'experts dans des domaines spécifiques (ex: politologues et enquêteurs) et leur confiera des missions provisoires d'une durée de quelques mois ou quelques années. Les analystes qui travaillent aux services de renseignement de façon permanente se voient alors attribuer le rôle de manager. Ils doivent superviser les travaux des experts temporaires, veiller au respect des normes de qualité requises, etc. Il faudrait, au sein des services de renseignement, engager des cadres moyens qui se sont forgés une expérience de dix à vingt ans dans un autre secteur.*[109]

Quel sera le profil de ce « filtre privé » agissant en amont des SR ? Une analyse américaine

103. Document OTAN AAP-6(2003)
104. « *Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations* », Defense Daily Network Special Report, posted 5 May 1998
105. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1996
106. Ibid.
107. Ibid.
108. MALIS Christian, « *Le renseignement stratégique à l'âge de l'information* », disponible sur www.Stratisc.org
109. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1996

y répond de la sorte : *The true OSINT provider is in the business of discovering, distilling, discriminating, and delivering open source intelligence. This is a completely different process with significantly more value than the process of open source information discovery and delivery. The greatest value that the true OSINT provider can offer is that of first echelon technical processing (de-duplication, weighting, clustering, and summarization) and first echelon human analysis by experts who can be relied upon to evaluate and discriminate and also to distill intelligently. In practical terms, this means that the over-burdened all-source analyst or decision-maker can avoid being overwhelmed by open sources because the true OSINT provider offers a complex filtering mechanism that relies primarily on subject-matter experts, and incidentally on technology.*[110]

Christian Malis évoque lui aussi ouvertement cette possibilité de sous-traitance : *on peut penser que le balayage systématique de certaines sources, ou plutôt de certains vecteurs d'information, comme Internet ou les grands serveurs américains de banques de données (Nexis, Dialog notamment), devrait être sous-traité à de petites structures privées ou semi-privées, en lien de confiance avec les services. (...) Avec Internet, on peut parier qu'il y a un grand avenir à la sous-traitance documentaire, et que l'immensité de l'univers Internet va susciter la naissance de raiders mercenaires spécialisés dans la traque de l'information. Cela aussi c'est la guerre de l'information.* [111]
L'architecture du traitement de l'information ouverte ressemblerait à ce que l'auteur appelle « une sorte de dispositif en étoile » : *au centre, le pôle de renseignement, dont les fonctions s'orienteraient essentiellement vers l'analyse et la synthèse. Pour l'information sur les événements bruts, ce pôle s'alimenterait, comme c'est déjà le cas actuellement, par abonnement aux grandes agences de presse. Un deuxième cercle serait constitué par des agences privées de filtrage systématique des informations pertinentes sur Internet, les grands serveurs de banques de données, etc., sur des thèmes d'intérêt spécifiques définis par le pôle de renseignement : la plus grande difficulté serait sans doute de s'assurer que ces agences respectent bien des règles strictes de confidentialité. Un troisième cercle correspondrait à des spécialistes du monde civil, consultés ponctuellement sur des points précis : industriels (d'ores et déjà ils sont souvent consultés pour expertise, par exemple sur les capacités prêtées à certains matériels militaires étrangers), universitaires, jugés compétents par exemple sur telle zone potentielle de crise d'intérêt militaire, journalistes. Enfin on pourrait envisager l'existence d'un quatrième cercle d'instituts ou de fondations de recherche largement financés par la Défense, petites structures démultipliant les capacités de traitement et d'analyse des experts du renseignement, avec des antennes éventuelles à l'étranger ; ces structures seraient comme des têtes chercheuses, susceptibles d'offrir leurs services aussi bien d'ailleurs aux services de renseignement qu'à divers ministères (Affaires étrangères ...). Naturellement, les structures en question devraient être assez « transparentes », et leurs personnels connus des services, pour que soient sauves les indispensables exigences de sécurité.*[112]

S'il fallait conclure provisoirement sur les perspectives d'une coopération européenne, nous rejoindrions l'avis d'Alessandro Politi qui estime que *l'OSINT devrait, par ailleurs, être considéré comme un domaine de coopération assez intéressant, permettant d'intensifier la confiance mutuelle. Il pourrait jouer un rôle crucial, qui ne découlerait pas nécessairement de ses possibilités intrinsèques, mais de la valeur qu'il revêt pour la formation au contrôle qualité et, à l'occasion, de son usage en tant que moyen d'information efficace dans les dispositifs politiques gouvernementaux et autres. Une approche coordonnée de l'OSINT au niveau européen n'empêcherait nullement de disposer d'une information « à la carte », mais contribuerait à économiser du temps et de l'argent.* [113]

5.2. HUMINT (Human Intelligence)

Au lendemain du 11 septembre, de nombreuses voix s'élevèrent pour dénoncer le sur-investissement des services américains dans le renseignement « technologique » (TECHINT), au détriment du renseignement humain, le HUMINT. La commission parlementaire d'enquête US ne relève-t-elle pas elle-même qu'*avant le 11 septembre, l'Intelligence Community n'a pas vraiment développé et utilisé de ressources humaines pour infiltrer le noyau dur d'Al-Qaida. Cette absence de ressources humaines fiables et*

110. « *Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations* », op. cit.
111. MALIS Christian, op. cit.
112. Ibid.
113. POLITI Alessandro, « *De la nécessité d'une politique européenne de renseignement* », op. cit.

bien informées a limité la capacité de l'Intelligence Community à se procurer des renseignements sur lesquels agir éventuellement avant les attaques du 11 septembre. En partie au moins, l'absence de sources antiterroristes unilatérales (c'est-à-dire recrutées par les Etats-Unis) est la conséquence d'une dépendance excessive par rapport aux services de liaison étrangers.[114]

Mais en fait, une analyse plus pointue fait apparaître que de telles déficiences avaient déjà été constatées lors de la première guerre du Golfe. Lorsque l'hebdomadaire français « Le Point » l'interrogea sur l'importance excessive qu'aurait accordée la CIA à la technologie, un ancien directeur de la Centrale, Robert Gates répondit: *ce débat entre l'espionnage technologique et les sources humaines dure depuis trente ans. On a besoin des deux. Mais la technologie en matière d'espionnage est très coûteuse. Si vous dépensez dix fois plus en technologie, cela ne signifie pas que vous avez des renseignements dix fois meilleurs. Pendant l'administration Carter, on a moins mis l'accent sur les agents parce que Carter était mal à l'aise avec l'espionnage humain. Ce n'est plus vrai. Le rôle des agents est encore plus important aujourd'hui, en particulier à cause des groupes terroristes « freelance » qui ne sont pas sponsorisés par un Etat. La pénétration de ces groupes-là est la seule manière de savoir ce qu'ils préparent. Car ils pourraient construire une bombe atomique dans leur chambre sans que les satellites n'en sachent rien*.[115] Le Directeur de la DST française, Pierre de Bousquet de Florian, confirme à ce sujet que *le fonctionnement traditionnel des services américains les amène à brasser des quantités absolument considérables d'informations. Et ce n'est pas un secret de dire qu'ils peuvent avoir des problèmes de tri. Nous fonctionnons d'une façon différente, en travaillant davantage sur des sources humaines. Les sources humaines sont à la fois plus précises et plus faciles à exploiter. Leur traitement est cependant délicat, ces sources pouvant elles-mêmes être manipulées*.[116]

L'Assemblée de l'UEO a selon nous raison de souligner que *le renseignement d'origine humaine et la capacité humaine d'interprétation des informations restent la base du renseignement et doivent être privilégiés. Il ne suffit pas de disposer de moyens techniques de recueil de renseignements, il faut savoir interpréter les données recueillies*.[117]

Les informateurs (ou « sources ») sont évidemment au cœur du HUMINT : *les informateurs sont essentiels pour les services de renseignement. Ils constituent la base de travail du renseignement. On attend d'un service de renseignement qu'il soit en mesure d'informer de manière objective les autorités sur les dangers potentiels ou réels pour lintégrité et la pérennité des institutions démocratiques d'un pays. (...) Il s'agit d'une problématique très délicate et complexe, en raison de l'importance des relations humaines dans les contacts entretenus entre agents et informateurs*.[118] Le Comité R propose la définition suivante d'un informateur : *une personne qui, rémunérée ou non, sollicitée ou spontanée, fournit des informations difficilement accessibles par d'autres voies et peut de ce fait encourir un risque matériel, moral ou physique*.[119]

La littérature a établi des typologies (par ailleurs d'intérêt variable) des informateurs. Ainsi, un ouvrage de P. Gill distingue un « informateur spontané » (*un citoyen ordinaire fournit une information unique sans aucune contrepartie. Dans ce classement interviennent aussi des personnes qui fournissent une information dans le but d'en retirer un avantage*), un « informateur occasionnel non suivi » (*un citoyen qui est encouragé à fournir une information dont il a eu connaissance fortuitement dans l'exercice de sa profession, par ex. un chauffeur de taxi, le personnel d'entretien, etc... Cette source n'est pas rémunérée)*, un « informateur suivi » (*il est régulièrement contacté et sollicité pour recueillir des informations. Cette source est rémunérée*) ; et un « informateur qui infiltre à long terme » (*cette source peut soit faire partie d'une organisation sur laquelle elle est disposée à fournir des informations, soit être membre d'un service de renseignement et s'infiltrer dans l'organisation sous une fausse identité*)[120].

114. Traduction disponible dans Le Monde, 26 juillet 2003
115. AUDIBERT (D.), « *CIA - Enquête sur un mythe »,* Le Point, n°1420, 3 décembre 1999, p.85, cité par WALDEN Alexander, op. cit.
116. Le Monde, 26 juillet 2003
117. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
118. Comité permanent de contrôle des services de renseignement, Rapport d'activités 2001
119. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1997
120. GILL P, « *Policing Politics- Security Intelligence and the Liberal Democratic State »* Frank CASS and Co. Ltd-Gainsborough House, Gainsborough Road, LONDON E11 1RS, England – cité par Comité permanent de contrôle des services de renseignement, Rapport d'activités 1997

Il est d'usage de décliner les modalités de recrutement d'une source par l'acronyme M.I.C.E, pour Argent (*Money*)-Idéologie-Chantage-Emotionnel. Mais le recrutement d'un informateur est, à chaque fois, un cas particulier, qui nécessite une utilisation « personnalisée » des différents « leviers » dont les SR disposent.

Examinons cependant quelques problèmes posés dans la perspective d'un approfondissement de la coopération au niveau européen.

La rétribution de l'informateur : l'argent reste une motivation certaine, mais elle n'est pas sans inconvénients dans la perspective d'une coopération européenne, car « européaniser » impliquera un minimum d'harmonisation des tarifs de rétribution des informateurs. A défaut, seuls les services les plus importants seront encore capables de recruter, engendrant inflation et compétition. D'autant que certains services procèdent à une évaluation de l'information avant de payer leur informateur, d'autres préfèrent les rétribuer sur base fixe. Acheter quelqu'un, c'est toujours courir le risque que quelqu'un d'autre double la mise. C'est la loi de l'offre et de la demande.

Le curriculum vitae de l'informateur place le débat aux confins de la loi et de l'éthique. Faut-il accepter de traiter avec un informateur qui se livre à des activités illégales, dont un SR a éventuellement connaissance mais sans les dénoncer à la justice. Faut-il une législation européenne sur les « repentis » ? Quid des infractions pénales commises par l'informateur qui infiltre ?

Les convictions de l'informateur restent sans doute le moyen le plus « sûr » de recrutement. L'expérience prouve qu'il s'agit du fondement le plus solide, même s'il ne peut être écarté (ou contrecarré par) d'autres paramètres, comme le chantage ou l'argent. Ces convictions sont extrêmement variables, et on citera à titre d'exemple le nationalisme ou le patriotisme, qui reste une corde « sensible », notamment dans le chef des communautés expatriées à l'étranger qui, en collaborant avec un SR, pensent « garder un contact » avec leur patrie d'origine ; l'idéologie : il fut une époque où l'anti-communisme était un levier de recrutement important pour les SR occidentaux ; aujourd'hui, il peut aussi s'agir de la défense d'une « certaine idée » de la Monarchie, de la République, de la Démocratie, voire même de « l'humanitaire » où rapporter à un SR des violations des droits de l'homme ou des trafics d'armes est perçu comme un moyen de promouvoir la paix et le développement ; une image positive de l'armée, par exemple acquise lors du service militaire.

Le « recrutement émotionnel » est très difficile à définir. Il peut s'agir d'une relation d'amitié et de confiance entre l'informateur et son officier traitant (OT) : dans ce cas, la source a l'impression de travailler pour une « personne » et non pour un service ou un Etat. L'informateur « personnalise » sa démarche, se sent même parfois protégé et valorisé. Mais le traitement de telles sources est délicat : elles ne parleront qu'à leur OT, et à personne d'autre, a fortiori à un étranger.

La notion « intérêts » recoupe celles de l'argent ou du chantage. Un informateur peut avoir besoin de « documents administratifs » (passeports, visas, droits de séjour en Europe sont souvent demandés) pour lui ou sa famille, à des fins légitimes ou criminelles. Un SR doit-il accepter de collaborer sur ces bases ?

Enfin, l'expérience démontre que la technique du chantage n'offre que des résultats aléatoires et souvent à court terme.

On le constate : le HUMINT est sans conteste le domaine où la coopération sera la plus problématique, non pas tant par manque de volonté des Etats qu'en raison du fondement même de ce type particulier de renseignement : la nature humaine, appréhendée dans toute sa complexité. En tout état de cause, une collaboration européenne dans le domaine du HUMINT nécessite une harmonisation de certaines règles de recrutement, comme la rétribution, la nature et l'ampleur des « services rendus », ou des règles éthiques et/ou légales vis-à-vis de la criminalité de droit commun. Deux points au moins posent un problème quasi insurmontable : le recrutement émotionnel, où la relation informateur-OT est le seul canal possible ; et le recrutement idéologique : certains ressortissants d'Etats membres refuseront de collaborer s'ils savent que les informations seront transmises au SR d'un autre Etat membre. On peut évidemment considérer que le sentiment d'appartenance à une « citoyenneté européenne » se développera à l'avenir et aplanira le problème, mais cette perspective ne peut s'envisager de façon réaliste qu'à très long terme.

La problématique du renseignement militaire tactique – autre forme de renseignement « humain » – nous invite à évoquer le rôle des

forces spéciales[121] et des unités de reconnaissance. Les grands conflits récents, comme l'opération « Liberté immuable » en Afghanistan ou l'opération américano-britannique en Irak, ont confirmé la nécessité d'obtenir un renseignement « humain » sur le terrain et, dans cette perspective, les « forces spéciales », les branches « action » des services de renseignements, et des unités militaires spécialisées dans la recherche du renseignement ont été largement utilisées.[122]

Parmi les unités des forces armées des Etats membres les plus connues du grand public, on distingue ainsi les Special Services britanniques, répartis entre le British Army's Special Air Service (SAS) fort de quatre escadrons de 50 hommes, et le Royal Navy's Special Boat Service (SBS), qui dispose de deux escadrons de 50 hommes. L'Allemagne peut compter sur les Kommando Spezialkräfte (KSK), créés récemment (en 1997) mais qui comptent déjà plus de 700 membres. Enfin, en France, le Commandement des Opérations Spéciales regroupe des éléments du 10ème Commando parachutiste de l'air (CPA 10), du 1er Régiment parachutiste d'Infanterie de Marine (RPIMa), et du Commandement des fusiliers marins et commandos (Cofusco), soit environ 2.000 hommes.[123] Nous n'avons pas connaissance d'une réflexion spécifique menée au niveau de l'UE sur une « doctrine europénne » d'utilisation des forces spéciales à des fins de renseignement. Gageons toutefois qu'ici aussi, l'opération ARTEMIS au Congo contribuera à ouvrir le débat. Nous n'évoquerons pas ici les opérations spéciales,[124] les opérations clandestines,[125] ou encore les opérations psychologiques,[126] popularisées par le cinéma ou la littérature, où l'aventure et l'exotisme se mêlent au romanesque et, faut-il le préciser, souvent à la fiction. Elles ne relèvent pas du renseignement, même si, dans quelques pays, elles sont « gérées » par un SR.

5.3. SIGINT (Signal Intelligence)

Le recueil de renseignement par l'interception des transmissions, ou SIGINT (Signal Intelligence), comprend trois sous-familles : le COMINT (ou Communications Intelligence), à savoir les techniques d'écoute et de captage, d'identification, de décryptage et d'analyse des messages. Le COMINT regroupe les informations techniques et les renseignements obtenus à partir des communications avec l'étranger par des personnes qui ne sont pas les destinataires de ces communications. Il concerne donc l'interception des communications avec l'étranger transmises par voie électromagnétique, sous forme cryptée ou non ; l'ELINT (ou Electronic Intelligence), couvre la radiogoniométrie, l'identification et l'analyse des sources d'émissions électromagnétiques. Certains auteurs isolent une sous-catégorie, le FISINT (Foreign Instrumentation Signals Intelligence) qui procède à l'interception des émissions électromagnétiques associées à des tests ou à des déploiements d'appareils spatiaux, aériens ou sous-marins ; et enfin le TELINT (Telemetry Intelligence) qui concerne les informations tirées de la télémétrie étrangère. [127]

Chacun se souvient de « 1984 », l'ouvrage majeur et effrayant de Georges Orwell qui décrit une société totalitaire et liberticide, où « Big Brother Is Watching You » : *dans le passé, aucun gouvernement n'avait eu le pouvoir de maintenir ses citoyens sous une surveillance constante. Maintenant, la Police de la Pensée*

121. Pour que la définition du terme soit précise, nous nous référerons au rapport de l'Assemblée Nationale française pour qui, en Europe, la notion de «forces spéciales» recouvre plus particulièrement *les éléments des commandos interarmées, équipes légères chargées de missions aussi diverses que les raids, les opérations psychologiques, l'encadrement de forces armées, le renseignement sur le terrain et, parfois, l'assistance à des populations civiles – Source :* Assemblée Nationale, Rapport d'information n° 3460, op. cit.

122. Assemblée de l'UEO, « *Les capacités militaires européennes dans le contexte de la lutte contre le terrorisme international* », rapport présenté au nom de la Commission de défense par M. Wilkinson, Document A/1783 du 3 juin 2002

123. Assemblée Nationale, Rapport d'information n° 3460, op. cit.

124. Selon la définition OTAN : *Activités militaires menées par des forces spécialement désignées, organisées, entraînées et équipées, utilisant des techniques opérationnelles et des modes d'action inhabituels aux forces conventionnelles. Ces activités sont menes dans toute la gamme des opérations militaires, indépendamment des opérations des forces conventionnelles, ou en coordination avec celles-ci, pour atteindre des objectifs politiques, militaires, psychologiques ou économiques. Des considérations politico-militaires peuvent nécessiter le recours à des techniques clandestines ou discrètes et l'acceptation d'un niveau de risque physique et politique non compatible avec les opérations conventionnelles*- Document OTAN AAP-6(2003)

125. Selon la définition OTAN : *Opération liée au renseignement, à la contre-ingérence et à d'autres activités similaires, organisée ou conduite de façon à en assurer le secret ou la dissimulation* - Document OTAN AAP-6(2003)

126. Selon la définition OTAN : *Activités psychologiques planifiées visant à influencer les attitudes et les comportements ayant une incidence sur la réalisation d'objectifs politiques et militaires* - Document OTAN AAP-6(2003)

127. WALDEN Alexander, op. cit.

surveillait tout le monde, constamment.[128] Les futurologues américains Alvin et Heidi Toffler, dans leur ouvrage « Guerre et contre-guerre » confirment un demi-siècle plus tard que *la révolution informatique, la multiplication des satellites, la vogue des machines à photocopier, des magnétoscopes, des réseaux électroniques, des bases de données, des fax, de la télévision par câble et des satellites de retransmission en direct, sans compter des dizaines et des dizaines d'autres technologies de traitement et de distribution de l'information, ont créés de multiples rivières de données, d'informations et de savoir qui se jettent désormais dans un immense océan sans cesse croissant d'images, de symboles, de statistiques, de paroles et de sons.*[129]

La « communauté du renseignement », pour qui *les oreilles sont aussi importantes que les yeux* – pour reprendre l'expression de l'Assemblée de l'UEO[130] – a pleinement tiré parti des nouveaux moyens d'interception électronique. Mais ces systèmes sont lourds, très onéreux et en constante évolution technologique. Assurer leur avenir sera un défi, comme l'a bien compris la commission du renseignement de la Chambre des Représentants US : *The most important challenges of the future may lie in the quantity and quality of what is being transmitted rather than the means of transmission. The ability to filter through the huge volumes of data and to extract the information from the layers of formatting, multiplexing, compression, and transmission protocols applied to each message is the biggest challenge of the future. Increasing amounts and sophistication of encryption add another layer of complexity. Signals Intelligence today is at a crossroads.*[131] Ces systèmes ont aussi montré leurs limites. Ainsi, selon Alexis Debat, la NSA produirait quotidiennement plusieurs dizaines de millions de gigaoctets de données, mais n'assurerait le traitement que de moins de 10 %, faute de disposer de systèmes de transcription vocale performants.[132]

Mais c'est le système Echelon, que nous allons examiner maintenant, qui est le plus controversé.

En 1999, la publication d'une étude intitulée « *une évaluation des techniques de contrôle politique »,* réalisée par la Fondation Omega de Manchester à la demande du Parlement Européen révéla au grand public l'ampleur du réseau Echelon - sorte de « secret de polichinelle » dont on trouvait déjà trace dans la littérature spécialisée depuis une dizaine d'années, en particulier avec les travaux du journaliste Duncan Campbell. [133] Cette étude établit que toutes les communications électroniques, téléphoniques et par fax en Europe sont quotidiennement interceptées par la NSA américaine, qui transfère ces informations vers Fort Meade, Maryland. Les sites de ce système sont basés à Sugar Grove et Yakima aux Etats-Unis, à Waihopai en Nouvelle Zélande, à Géraldton en Australie, à Hong Kong et à Morwenstow au Royaume-Uni. Echelon fonctionne sur base de l'accord dit « UKUSA » conclu en 1948 entre les Etats-Unis et la Grande Bretagne, auxquels se sont joints ultérieurement le Canada, la Nouvelle-Zélande et l'Australie. Le fonctionnement du système peut être ainsi synthétisé : *la technique utilisée repose sur l'utilisation de mots-clés préalablement sélectionnés et répertoriés dans des dictionnaires. Chaque agence de renseignement élabore ainsi des listes de mots selon les activités qu'elle souhaite suivre et contrôler. Les mots-clés correspondent par exemple à des noms de dirigeants politiques ou économiques, d'entreprises, d'institutions, de produits ou de références de répertoires. Pour éviter d'être submergé par la masse des données, le système est capable d'élaborer des combinaisons de mots-clés qui sont elles-mêmes indexées dans les dictionnaires. Les dictionnaires des ordinateurs sont interconnectés. Chaque système a en mémoire des listes de mots-clés ou des combinaisons de chaque agence nationale - mais pas forcément l'ensemble des listes ou des combinaisons du système-, ce qui lui permet de repérer les messages contenant ces mots-clés et de les transmettre à l'agence concernée. La mise à jour des dictionnaires est quotidiennement assurée par chacune des agences intéressées.*[134]

Quelle peut-être l'efficacité réelle d'un tel « aspirateur électronique « ? Les difficultés rencontrées sont en effet nombreuses, comme le

128. Cité par RAMONET Ignacio, « *Surveillance totale* », Le Monde Diplomatique, Août 2003, n°593, p.1
129. MALIS Christian, « *Le renseignement stratégique à l'âge de l'information* », op. cit.
130. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
131. Ibid.
132. DEBAT Alexis, « *Voyage au cœur du renseignement américain* », in Politique internationale, n°95, Printemps 2002.
133. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1999
134. Assemblée Nationale, Rapport d'information n°2623 du 11 octobre 2000, déposé par la commission de la Défense nationale et des forces armées sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, présenté par M. Arthur Paecht, Député.

note l'Assemblée nationale française : *une difficulté récente pour le système provient du développement des méthodes de cryptage utilisées par les plus grands groupes industriels ou certains services étatiques pour assurer la confidentialité de leurs communications. Une des explications apportées à la diffusion récente d'informations sur le réseau Echelon est liée à la difficulté croissante des services d'écoute face au développement de la cryptologie et à la nécessité pour ces services de suivre les progrès des technologies dans ce domaine et d'éviter que celles-ci n'empêchent une action qu'ils considèrent légitime.*[135] Un expert belge ajoute que *la technologie actuelle permet la surveillance exploratoire et généralisée sur base d'un dictionnaire de mots-clés du courrier électronique non chiffré et, dans une certaine mesure du trafic téléfax, à la condition expresse que ces télécommunications utilisent des satellites. La technologie actuelle ne permet pas cette surveillance exploratoire et généralisée des communications téléphoniques satellitaires (environ un pour-cent des communications téléphoniques internationales) mais autorise la reconnaissance d'un locuteur particulier sur base de son empreinte vocale.*[136]

Ces réserves n'empêchent pas l'Assemblée Nationale française de conclure que : *oui, les capacités d'un tel système sont réelles et elles le rendent performant, compte tenu des multiples vulnérabilités des systèmes d'information et de communication. Le développement du réseau s'est appuyé sur le développement de compétences techniques et la mise en place de multiples installations. Il a bénéficié d'importants investissements en hommes et en équipements depuis près de quarante ans. Il faut cependant ajouter que les performances ont atteint leurs limites, non seulement parce que les moyens engagés ne sont plus en rapport avec l'explosion des communications dans le monde mais aussi parce que certaines cibles ont appris à se protéger des interceptions.*[137] D'autres par contre en minimisent l'ampleur, comme le journaliste américain Jams Bamford pour qui *il est hautement improbable qu'Echelon surveille tout le monde partout comme les critiques le proclament. Il serait impossible à la NSA d'intercepter toutes les communications. L'agence a connu d'importantes réductions de personnel au cours des cinq dernières années alors que ses cibles pour la sécurité nationale ont augmenté en nombre: le déploiement des missiles nord-coréens, les essais nucléaires en Inde et au Pakistan, la circulation de présumés terroristes, etc ... Etre à l'écoute du business européen en vue d'aider des sociétés américaines ne serait qu'une mission de faible priorité. Et transmettre le produit d'interceptions secrètes à des compagnies serait rapidement découvert.*[138]

Mais en tout état de cause, les « révélations » sur Echelon se révéleront politiquement délicates. Un rapport du Parlement fédéral belge pose la question en ces termes : *si Echelon doit servir d'arme aux services de police et de renseignements comme aux responsables politiques dans la lutte contre le crime organisé, le terrorisme et les Etats parias (rogue States), il ne saurait en aucun cas justifier l'interception aveugle de toutes les communications de citoyens innocents, de pays amis, d'organisations non gouvernementales ou d'entreprises. Or, l'interception de communications par satellite permet de recueillir des informations sur la politique des pays tiers, des entreprises concurrentes et des opposants politiques, qui ne partagent pas nécessairement les opinions américaines sur l' « ordre mondial ».*[139]

Les Etats-Unis seraient-ils pour autant seuls « coupables » de ce genre de pratiques ? Certes non. Pour ce qui concerne la France, un article publié dans le « Nouvel Observateur » du 5 avril 2001 révèle les possibilités d'interception COMSAT de la DGSE, dont la principale station d'interception est située au centre radioélectrique de Domme, dans le Périgord. Une autre station, dite «Frégate» est dissimulée dans la forêt tropicale en Guyane française, et une troisième fut construite en 1998 sur l'île de Mayotte, dans l'océan Indien. Ces deux dernières stations sont exploitées en collaboration avec le BND allemand. Enfin, une quatrième station se trouve sur le plateau d'Orgeval, à l'ouest de Paris.[140] Les Pays-Bas disposent de la station d'écoutes de Zoutkamp, gérée par le Militaire Inlichtingendienst. En Allemagne, la section 2 du BND recueille des renseignements en interceptant des communications étrangères, parmi lesquelles

135. Assemblée Nationale, Rapport d'information n°2623, op. cit.
136. Comité permanent de contrôle des services de renseignements, Rapport complémentaire d'activités 1999
137. Assemblée Nationale, Rapport d'information n°2623, op. cit.
138. Comité permanent de contrôle des services de renseignements, Rapport complémentaire d'activités 1999
139. Parlement fédéral Belge, « *Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé « Echelon* », Doc 2-754/1 (Sénat) et 1660/001 (Chambre), 25 février 2002
140. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1999

COMSAT et, depuis mai 2001, les communications étrangères transmises par câble peuvent également être interceptées. Selon l'expert Duncan Campbell, le BND dispose d'une base en République Populaire de Chine, à Taiwan et, nous l'avons vu, en Guyane française.[141]

Mais au-delà des moyens techniques dont disposent les uns et les autres, les interceptions et autres écoutes posent évidemment la question du respect de la vie privée, dans sa double dimension juridique et éthique.

Sans entrer dans le détail des différentes législations nationales en vigueur dans les Etats membres de l'UE, nous nous limiterons à souligner les conclusions d'une étude comparative réalisée par le Comité R : *de manière générale, les législations de tous [les] pays [étudiés] protègent le droit à la vie privée des citoyens en prohibant les écoutes téléphoniques ainsi que l'interception d'autres ypes de communications privées, sous peine d'amendes et/ou d'emprisonnement. Toutes ces législations prévoient cependant des dérogations possibles en matières judiciaire et/ou de sûreté de l'Etat. Tous les pays étudiés permettent, sous certaines conditions, des écoutes judiciaires. Tous ne permettent pas de la même manière les écoutes de sécurité. Certaines législations se contentent de dire que des dérogations sont possibles (Danemark, Allemagne en ce qui concerne le contrôle stratégique); d'autres permettent aux services de renseignements d'acquérir certaines informations par des moyens techniques (Portugal); d'autres encore permettent d'intercepter toutes formes de communications (Canada, Grand-Duché de Luxembourg); cependant, certaines législations définissent de manière précise les opérations techniques permises ou traitent séparément les écoutes téléphoniques et les autres transmissions sans fil (Grande-Bretagne, Etats-Unis). La loi française du 10 juillet 1991 permet de procéder à des écoutes judiciaires et à des écoutes administratives.*[142]

Cette question a fait l'objet de nombreux textes au niveau international.

Le premier instrument international fut adopté au sein de l'OCDE le 23 septembre 1980, sous la forme d'une recommandation intitulée «Lignes directrices réglementant la protection de la vie privée et les flux transfrontaliers des données à caractère personnel».[143]

La Convention Européenne des Droits de l'Homme (CEDH) et sa jurisprudence constituent une autre source juridique importante. L'article 8§2 de la CEDH n'autorise les ingérences d'une autorité publique dans l'exercice du droit au respect de la vie privée *que pour autant que cette ingérence soit prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire* à *la sécurité nationale,* à *la sûreté publique, au bien-être économique du pays,* à *la défense de l'ordre et* à *la prévention des infractions pénales,* à *la protection de la santé ou de la morale, ou* à *la protection des droits et libertés d'autrui.* Ces ingérences doivent être proportionnées à la gravité de la menace et avoir un caractère subsidiaire, ce qui signifie que l'on ne pourra y avoir recours que pour autant que les autres moyens disponibles ne puissent aboutir aux mêmes résultats. Dans son arrêt « Klass contre RFA » rendu le 6 septembre 1978, la Cour Européenne des Droits de l'Homme détaille son interprétation de cet article, s'agissant des écoutes téléphoniques administratives. La Cour a ainsi admis que face aux menaces accrues, des dispositions législatives accordant aux autorités publiques des pouvoirs de surveillance secrète de la correspondance et des télécommunications sont nécessaires dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales. La Cour estime toutefois que *les Etats* (...) *ne disposent pas pour autant d'une latitude illimitée pour assujettir* à *des mesures de surveillance secrète les personnes soumises* à *leur juridiction. Consciente du danger, inhérent* à *pareille loi, de saper voire de détruire la démocratie au motif de la défendre,* (la Cour) *affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage, n'importe quelle mesure jugée par eux appropriée.* La CEDH a en fait déterminé par ses arrêts quatre conditions qui doivent encadrer une possible intervention de l'Etat : que l'interception n'ait lieu que dans le cadre des objectifs d'intérêt vital de l'Etat énumérés par la Convention elle-même; que ces finalités soient prévues par la loi, c'est-à-dire par un texte réglementaire accessible au public et rédigé de façon suffisamment précise pour que le citoyen puisse y répondre par un comportement adéquat (arrêt Kruslin du 24 avril 1990); que la mesure

141. Parlement fédéral Belge, « *Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé « Echelon* », op. cit.

142. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1995

143. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1996.

prise soit strictement proportionnée à l'objectif poursuivi. Les arrêts Klass (6 septembre 1978) et Leander (25 février 1987) rappelent qu'une surveillance exploratoire ou générale effectuée sur une grande échelle est prohibée; qu'un équilibre soit recherché entre d'une part la protection de la vie privée et d'autre part les impératifs de sécurité et d'ordre public qui fondent la mission des services de renseignements et de sûreté.[144]

Au niveau du Conseil de l'Europe, le Comité des ministres a adopté le 7 février 1995 une recommandation proposant des règles communes pour la protection de la vie privée des usagers des services téléphoniques. Cette recommandation concerne l'ensemble des services mis à disposition des usagers par les télécommunications pour communiquer ou correspondance: téléphone, vidéotex interactif, transmission de textes ou d'images par fax, consultation électronique de bases de données, télémétrie. Elle n'autorise pas l'ingérence des autorités publiques, sauf dans les cas autorisés par la loi et si le fonctionnement de la société démocratique l'exige et invite les gouvernements à tenir compte de leurs droits et pratiques internes, des principes suivants: le respect de la vie privée des utilisateurs, du secret de la correspondance et de la liberté de communication; à l'information des abonnés aux services de télécommunications au sujet des catégories de données personnelles collectées et traitées, du fondement juridique de la collecte, des finalités de la collecte et du traitement, de l'utilisation et des durées de conservation desdites données; à la subordination de la communication de données personnelles au consentement exprès, éclairé et écrit de l'abonné.[145]

Mais c'est surtout le droit communautaire de l'Union Européenne qui retiendra notre attention.

L'article 6.2 du TUE dispose que *l'Union respecte les droits fondamentaux tels qu'ils sont garantis par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (....)*, ce qui concerne évidemment les dispositions mentionnées aux points (2) et (3) supra. L'article 286.1, introduit dans le TCE par le traité d'Amsterdam, dispose qu'*à partir du 1er janvier 1999, les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes institués par le présent traité ou sur la base de celui-ci*. Enfin, la Charte des droits fondamentaux, adoptée lors du Sommet de Nice, réaffirme toute une série de libertés fondamentales, destinées – selon toute vraisemblance – à être intégrées dans une future Constitution européenne telle que proposée par la « Convention sur l'avenir de l'Europe ».

En outre, le droit communautaire dispose déjà d'une vaste législation qui réaffirme le droit à la vie privée, tout en intégrant la dimension « sécurité ».

Ainsi, le Conseil a adopté le 17 janvier 1995, une résolution visant à faciliter les écoutes téléphoniques. Si elle détaille les conditions techniques nécessaires à l'interception des télécommunications, elle n'en détermine toutefois pas les conditions de réalisation. La résolution prévoit une obligation dans le chef des opérateurs de réseaux ou des fournisseurs de services de fournir en clair aux « services autorisés » les données interceptées : appels téléphoniques mobiles ou non, courriers électroniques, télécopies et messages télex, flux de données Internet, tant au niveau de la prise de connaissance du contenu des télécommunications que des données de trafic, mais également tout signal émis par la personne faisant l'objet de la surveillance, ou la localisation géographique de l'utilisateur mobile.[146]

Afin de garantir la libre circulation des informations au sein de l'Union et d'appliquer des critères identiques dans ses relations avec les Etats tiers, en respectant le droit à la vie privée des personnes physiques, le Conseil a adopté le 24 octobre 1995 la directive 95/46 relative à la protection des personnes physiques en ce qui concerne le traitement de données à caractère personnel et la libre circulation de ces données.[147] Pour ce qui concerne le travail des SR, on notera que le traitement de données *mis en oeuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire comme la sécurité publique, la défense ou la sûreté de l'Etat* est explicitement exclu. A titre complémentaire, le règlement (CE) 45/2001 du 18 décembre 2000 traite de la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de la Communauté et la libre circulation de ces données. Il vise à assurer la protec-

144. Ibid.
145. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1996.
146. Rapport d'expertise rédigé à l'attention du Comité permanent de contrôle des services de renseignements le 7 mars 2000.
147. Journal officiel L 281, 23.11.1995

tion des données à caractère personnel dans le cadre des institutions et des organes de l'UE.[148]

Le 3 mai 1999, le « Groupe de protection des personnes à l'égard du traitement des données personnelles » a adopté une recommandation concernant le respect de la vie privée dans le contexte de l'interception des télécommunications. La recommandation insiste sur les obligations des opérateurs et fournisseurs de télécommunications de prévoir toutes les mesures de sécurité ainsi que le cryptage systématique des messages afin de rendre techniquement difficile ou impossible en l'état actuel des techniques, l'interception des télécommunications par des instances non autorisées par la loi. Le groupe souligne à cet égard que la mise en oeuvre de moyens efficaces d'interception des communications à des fins légitimes ne doit pas conduire à un abaissement du niveau général de confidentialité des communications et la protection de la vie privée des individus. La recommandation énumère les conditions d'interception de télécommunications : les autorités habilitées à permettre l'interception légale des télécommunications, les services habilités à procéder aux interceptions et la base légale de leur intervention; les finalités selon lesquelles de telles interceptions peuvent avoir lieu, qui permettent d'apprécier leur proportionnalité au regard des intérêts nationaux en jeu; l'interdiction de toute surveillance exploratoire ou générale de télécommunications sur une grande échelle; les circonstances et les conditions précises auxquelles sont soumises les interceptions, dans le respect du principe de spécificité auquel est soumise toute ingérance dans la vie privée d'autrui; le respect de ce principe de spécificité, corollaire de l'interdiction de toute surveillance exploratoire ou générale, implique en ce qui concerne plus précisément les données de trafic que les autorités publiques ne peuvent avoir accès à ces données qu'au cas par cas; les mesures de sécurité en ce qui concerne le traitement et le stockage des données, et leur durée de conservation; en ce qui concerne les personnes impliquées de façon indirecte ou aléatoire dans les écoutes, les garanties particulières apportées au traitement des données à caractère personnel; l'information de la personne surveillée, dès que possible; les types de recours que peut exercer la personne surveillée; les modalités de surveillance de ces services par une autorité de contrôle indépendant; la publicité – par exemple sous forme de rapports statistiques réguliers – de la politique d'interception des télécommunications effectivement pratiquée; les conditions précises auxquelles les données peuvent être communiquées à des tiers dans le cadre d'accords bi- ou multilatéraux.[149]

En mars 2002, le Parlement européen et le Conseil ont adopté un nouveau dispositif législatif (« paquet télécom ») appelé à encadrer le secteur des communications électroniques. Ce nouveau dispositif, qui se compose d'une directive générale (directive-cadre) et de quatre autres directives particulières (directives « autorisation », « service universel », « accès et interconnexion » et « protection de la vie privée »), a pour principal objectif de rendre le secteur plus concurrentiel. Dans le cadre de la présente étude, nous nous limiterons à examiner la directive 2002/58/CE du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques »).[150] Elle aborde un certain nombre de thèmes sensibles, tels que la conservation des données de connexion par les Etats membres à des fins de surveillance policière (rétention des données), l'envoi de messages électroniques non sollicités, l'usage des témoins de connexion et l'inclusion des données personnelles dans les annuaires publics. En matière de confidentialité des communications, la directive rappelle, comme principe de base, que les Etats membres doivent garantir, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications électroniques. En particulier, ils doivent interdire à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications sans le consentement des utilisateurs concernés. Pour ce qui est de la rétention des données, la directive stipule que les Etats membres ne peuvent lever la protection des données que pour permettre des enquêtes criminelles ou préserver la sécurité nationale, la défense et la sécurité publique. Une telle mesure ne peut être adoptée que lorsqu'elle constitue une *mesure nécessaire, appropriée et proportionnée dans une société démocratique*. Enfin, la directive prévoit que les utilisateurs doivent avoir la possibilité de refuser qu'un témoin de connexion

148. Journal officiel L 8, 12.01.2001

149. Rapport d'expertise rédigé à l'attention du Comité permanent de contrôle des services de renseignements le 7 mars 2000.

150. Journal officiel L 201 du 31 juillet 2002. Elle abroge la Directive 97/66/CE du 15 décembre 1997

(« cookies ») ou qu'un dispositif similaire soit placé sur leur équipement terminal.

En septembre 1998, le « groupe de travail sur la coopération policière » au sein de l'UE a débattu puis approuvé une nouvelle liste de « requirements » afin de couvrir les communications satellites et Internet. Les résultats prirent le nom d'ENFOPOL 98 et furent connus du grand public grâce à des fuites largement diffusées sur Internet, contraignant les autorités à mettre cette initiative sous le boisseau jusqu'en mai 2001, lorsque le Conseil de l'UE approuva un rapport explicatif des conséquences des « requirements ». Bien qu'il mette en place des mesures encadrant les interceptions (dont la surveillance en temps réel), ENFOPOL 29 reste limité par la nécessité d'obtenir un ordre spécifique autorisant l'écoute sur un sujet précis.[151]

Au sujet d'Internet, on notera la décision 276/99/CE du 25 janvier 1999, adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux. Dans le cadre de la présente étude, on notera en particulier que le « contenu illégal » porte sur une large variété de problèmes, relevant – en tout ou en partie – des missions des SR, comme la sécurité nationale; la sécurité économique; ou la protection de l'information.[152]

Dans le domaine de la cryptologie, la Commission a élaboré en 1996 un Livre vert sur une protection juridique des services cryptés dans le marché intérieur.[153] Sur cette base, l'UE s'est dotée de la directive 98/84 CE sur la protection juridique des services à accès conditionnel et des services d'accès conditionnés, par laquelle les Etats membres ont l'obligation d'interdire et de sanctionner toutes les activités commerciales liées à l'accès non autorisé à ce type de services (services de la société de l'information fournis à distance par voie électronique à la demande individuelle d'un destinataire de service.[154] D'autre part, le 8 octobre 1997, la Commission a publié une communication intitulée « Assurer la sécurité et la confiance dans la communication éléctronique - Vers un cadre européen pour les signatures numériques et la cryptographie ». Cette communication propose d'établir un cadre européen pour les signatures numériques et le chiffrement Elle souligne d'une part l'importance des techniques cryptographiques, comme le chiffrement[155] et les signatures numériques,[156] mais elle constate d'autre part que des pratiques restrictives ou l'adoption de règles différentes dans les Etats membres, voire l'absence de règles, pourraient constituer des entraves au bon fonctionnement du marché unique.[157] Sur cette base, la directive 1999/93 relative à la signature électronique établit un cadre juridique communautaire, tant pour la reconnaissance légale des signatures électroniques et leur recevabilité comme preuve en justice, que pour l'activité des prestataires de services de certification.[158]

L'acquisition de renseignement SIGINT intéresse également au premier chef les forces armées. Pour ce qui concerne les moyens militaires dont disposent les armées de l'UE, on distinguera les vecteurs aériens des capacités spatiales. Les « vecteurs aériens » sont en général, des avions de transport et d'avions rapides qui assurent l'interception des émissions radioélectriques, ainsi que leur identification et leur localisation. Les armées des Etats membres de l'UE comptent une vingtaine d'appareils en charge de la reconnaissance électromagnétique. L'Allemagne possède des Breguet 1150 Atlantic datant des années soixante-dix, et modernisés à deux reprises. Outre ses Falcon 20 et ses Tornado, le Royaume-Uni peut compter sur sept Sen-

151. BUNYAN Tony, « *Surveillance des télécommunications : fin de partie* », cultures & conflits, automne 2002, http://conflits.org
152. Journal Officiel L 33, 6 février 1999
153. COM (96) 76 final -non publié au Journal officiel
154. JOCE 1998 L 320/54. Voyez aussi DEHOUSSE Franklin et ZGAJEWSKI Tania, « *L'Europe et la société de l'information* », Studia Diplomatica, Vol LIII : 2000, n°4, Institut Royal des Relations Internationales
155. Le chiffrement garantit que le message ne soit pas compréhensible par des tiers autres que l'expéditeur et le destinataire Seul l'expéditeur peut crypter le message et seul le destinataire peut le déchiffrer. Il s'agit d'un élément qui est vital sur les réseaux ouverts afin de se préserver contre toute opération illicite. Il existe dans le commerce de nombreux produits cryptographiques «préfabriqués». (Source : DEHOUSSE Franklin et ZGAJEWSKI Tania, « *L'Europe et la société de l'information* », op. cit.)
156. Les signatures électroniques permettent au destinataire de données transmises électroniquement de vérifier l'origine des données (authentification de l'origine des données) et de vérifier que les données sont complètes, n'ont pas été altérées pal des tiers ou accidentellement (intégrité des données). (Source : DEHOUSSE Franklin et ZGAJEWSKI Tania, « *L'Europe et la société de l'information* », op. cit.)
157. COM (97) 503 final - non publié au Journal officiel . Voyez aussi DEHOUSSE Franklin et ZGAJEWSKI Tania, « *L'Europe et la société de l'information* », Studia Diplomatica, Vol LIII : 2000, n°4, Institut Royal des Relations Internationales
158. JOCE 1999, L 13/12. Voyez aussi DEHOUSSE Franklin et ZGAJEWSKI Tania, « *L'Europe et la société de l'information* », op. cit.

try AEW.I (E-3D AWACS) et trois Nimrod R.1 (entrés en service en 1974 et modernisés pour la dernière fois en 1995). La Suède utilise deux Gulfstream IV S102 B. Enfin, la France dispose de deux C-160 Transall Gabriel et d'un DC-8 Sarigue. Elle a en outre la possibilité de monter la nacelle ASTAC dédiée à la reconnaissance électromagnétique sur des avions de combat ou des drones.[159]

Contrairement à l'imagerie, que nous évoquerons infra, l'écoute fait figure de parent pauvre du renseignement spatial européen. Tout juste peut-on relever quelques projets nationaux encore au stade expérimental, à l'instar des programmes français Cerise et Clémentine qui ont respectivement accompagné les lancements d'Hélios 1A en 1995 et d'Hélios 1B en 1999. L'un comme l'autre recueillent des signaux électromagnétiques dans un spectre de fréquences utilisé par les radiocommunications tactiques et les téléphones cellulaires. Sans être en mesure de soutenir la comparaison avec les satellites SIGINT américains, ils devraient être complétés à l'horizon 2003-2004 par quatre satellites Essaim spécialisés dans le COMINT.[160] L'Assemblée de l'UEO note toutefois que *l'ensemble pourrait s'inscrire à terme dans un système européen de renseignement électromagnétique depuis l'espace, qui viendrait utilement compléter le dispositif d'observation. Mais, comme dans le domaine du IMINT, une réelle coopération technique ne pourrait être menée qu'à travers la création d'une véritable agence européenne de renseignement.*[161]

En guise de conclusion (partielle), trois éléments doivent selon nous être mis en exergue.

Premièrement, le développement des techniques d'interception – que l'accélération des technologies du « Information Age » rend inéluctable – devra se faire conformément aux traditions démocatiques des Etats membres et donc être strictement encadré. Toutefois, les disparités actuelles dans les prescrits nationaux en vigueur pourraient être de nature à entraver la coopération entre SR. Si une uniformisation/harmonisation du droit des Etats membres n'est sans doute pas réaliste à court terme, il serait toutefois souhaitable que l'UE poursuive son travail de « convergence » des différentes dispositions nationales afin de concilier harmonieusement l'approfondisement de la coopération entre ses SR, le respect de ses principes les plus fondamentaux et l'adhésion de ses citoyens.

Deuxièmement, pour utiles qu'elles soient, les techniques SIGINT ne doivent pas être surévaluées, car leurs limites sont évidentes. Une simple retranscription écrite d'une conversation téléphonique ne sera que de peu d'utilité à un analyste chevronné, qui s'interrogera, au-delà des mots couchés sur le papier, à d'autres paramètres tels la langue utilisée (y compris les dialectes), les accents et intonations (lecture d'un texte pré-écrit, etc), le ton (est-il autoritaire, hésitant, … ?), soit autant de données fondamentales bien connues des services de police lorsqu'ils doivent négocier une prise d'otages ou une demande de rançon. Ce n'est pas un hasard si, dans de tels cas de figure, appel est fait à des psychologues, à des linguistes, etc. La masse de données recueillies par des interceptions indifférenciées, opérées « tous azimuths », rend une telle analyse approfondie systématique quasi impossible – ou alors dans des délais rendant l'information recueillie obsolète. La commission d'enquête américaine déjà évoquée constate d'ailleurs que *avant le 11 septembre, l'Intelligence Community n'était pas préparée à gérer le défi que représentait la traduction du volume d'informations en langues étrangères collectées pour la lutte antiterroriste. Les agences composant l'Intelligence Community ont dû faire face à des accumulations de matériaux à traduire restant en souffrance, à une pénurie de linguistes qualifiés et d'agents possédant les compétences linguistiques indispensables, avec une réserve couvrant seulement 30% des besoins pour les langues les plus utilisées par les terroristes*.[162]

Enfin, troisièmement, le SIGINT nécessite de lourds investissements en matériel et en technologie. Si bien entendu, les grands services ont, à cet égard, plus de capacités que d'autres, une approche européenne coordonnée en matière de recherche-développement permettrait d'appréciables économies d'échelle. Or, le bilan de la coopération européenne est à l'heure actuelle assez maigre, comme le note un rapport de l'Assemblée de l'UEO qui conclut qu'en matière d'interception électronique, *force est de constater qu'il n'existe pour l'heure aucune véritable coopération technique dans ce do-*

159. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
160. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
161. Ibid.
162. Traduction disponible dans Le Monde, 26 juillet 2003

maine, chaque Etat considérant que la maîtrise de la situation électromagnétique sur une zone ressortit à sa souveraineté. Dès lors, le potentiel européen se réduit à la juxtaposition de moyens et démarches purement nationaux et quasi embryonnaires au niveau spatial.[163] Et les perspectives telles que dégagées par l'Assemblée Nationale française restent limitées : *un système européen ne peut guère être envisagé mais deux possibilités restent concevables, l'une pour la gestion des clés, l'autre dans l'élaboration de standards et de logiciels communs afin d'éviter les intrusions dans les systèmes. Les limites d'une politique commune sont liées à la nécessité d'effectuer des investissements importants et d'inciter les utilisateurs à privilégier ces nouveaux équipements. La gestion commune des systèmes de clés se heurte à la forte concurrence entre entreprises des différents pays et au maintien des particularismes nationaux. L'amorçage d'une politique commune pourrait venir d'une coopération bilatérale entre la France et l'Allemagne qui attirerait ensuite les pays intéressés notamment la Grande-Bretagne et les pays scandinaves. Les capacités technologiques et financières existent, la volonté politique paraît moins acquise.*[164]

5.4. IMINT (Imagery Intelligence)

Certains auteurs distinguent, au sein de l'IMINT, un certain nombre de sous-catégories[165] : le VISINT (Visual Intelligence), les images visuelles; le PHOTINT (Photographic Intelligence), les photographies; le VIDINT (Video Intelligence), les images vidéos ; l'OPTINT (Optronic Intelligence), les images thermiques ou infrarouges. D'autres sources distinguent l'imagerie recueillie par les satellites d'observation, selon qu'elle relève de moyens optiques (IMINT) ou de moyens électroniques (RADINT).[166] Enfin, notons qu'il existe plusieurs catégories de satellites d'observation que leurs atouts et leurs points faibles rendent complémentaires. En effet, tandis que les satellites optiques, qui offrent une bonne résolution, sont « aveugles » la nuit et par temps couvert, les satellites radar, d'une résolution moindre, disposent d'une capacité « tous temps ». Les capteurs infrarouges, qui enregistrent une partie non visible du spectre optique et créent des images à partir des variations de température, permettent une vision de nuit.[167]

L'importance du secteur spatial dans l'acquisition du renseignement n'est plus contestée. Ainsi, un rapport de l'Assemblée de l'UEO souligne que *dans l'environnement géostratégique actuel, il est difficile de connaître avec précision le lieu, l'espace géographique, la nature et le niveau de menace d'une crise qui peut être déclenchée à tout moment, parfois avec un faible préavis. Toute erreur d'évaluation d'une situation peut avoir de graves conséquences tant au plan politique que pour l'emploi des forces. C'est pourquoi l'utilisation de l'espace est un élément majeur de la politique militaire des nations modernes. Les systèmes spatiaux sont devenus des moyens essentiels de recueil, d'analyse et de distribution de l'information à une échelle planétaire. L'espace joue en permanence un rôle majeur de maîtrise de l'information dans l'analyse, le suivi et la gestion des crises. Les applications spatiales concourent, en complément d'autres moyens, à fournir aux hautes autorités civiles et militaires les éléments indispensables à la conduite d'une véritable politique de sécurité et de défense européenne*.[168] Pour l'Assemblée de l'UEO, *l'importance stratégique de l'espace n'est plus à démontrer. C'est un lieu de déploiement de systèmes de télécommunication (télévision, liaisons téléphoniques), de renseignement (météréologie, observation de la terre) et de navigation, au profit des pouvoirs politique, économique et militaire. Pour l'Europe, le développement spatial peut constituer un outil lui permettant d'atteindre ses principaux objectifs en matière de sécurité et de défense*.[169] *(...) l'utilisation de l'espace est devenue un élément primordial de la politique militaire des grandes nations. Pour que les décideurs aient à leur disposition, à tout moment, une vision actualisée et complète de la situation, l'Union Européenne doit notamment se doter des systèmes spatiaux appropriés permettant de recueillir et d'analyser l'information. C'est*

163. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
164. Assemblée Nationale, Rapport d'information n°2623, op. cit.
165. WALDEN Alexander, op. cit.
166. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1998
167. Ibid.
168. Assemblée de l'UEO, « *Le développement d'une capacité européenne d'observation spatiale pour les besoins de la sécurité de l'Europe* », rapport présenté au nom de la commission technique et aérospatiale par L. O'Hara, rapporteur, et M. Cherribi, rapporteur associé
169. Cf le rapport des « trois sages » (Carl Bildt, Jean Peyrelevade et Lothär Spath) sur la politique spatiale européenne : « *Towards a space agency for the European Union* », rapport réalisé à la demande d'Antonio Rodota, Directeur général de l'ESA.

pourquoi non seulement la possession de satellites est indispensable, mais l'accès à l'espace est primordial : l'autonomie dans le domaine spatial repose sur la capacité de lancer et de concevoir des satellites.[170]

En effet, le rôle des satellites est essentiel pour l'acquisition du renseignement nécessaire à la prévention et à la gestion des crises, qu'il s'agisse de l'appréciation générale de la situation, de l'évaluation des forces en présence ou des mouvements de réfugiés, de la surveillance des embargos, de la préparation des activités humanitaires ou des interventions militaires. En outre, ils sont le seul moyen permanent de surveillance de la prolifération des armes de destruction massive et du respect des traités de désarmements. Actuellement dévolue au renseignement stratégique et opérationnel, l'observation satellitaire devrait aussi offrir dans le futur des possibilités d'exploitation au niveau tactique grâce à des constellations de petits satellites d'observation bon marché, à orbite très basse et donc à durée de vie courte. Enfin, l'imagerie satellitaire permet d'acquérir des informations dans des zones inaccessibles à d'autres sources ou lorsque l'utilisation de sources humaines présente des risques excessifs.[171]

Enfin, pour ce qui concerne le « renseignement de défense », deux experts canadiens, Mark Stout et Thomas Quiggin, relèvent les applications de l'imagerie spatiale en situation de combat : *même si l'imagerie commerciale à haute résolution ne révolutionnera pas probablement la conduite de la guerre, elle a le potentiel pour servir de « multiplicateur de force » important pour certains consommateurs. Presque toutes les étapes de préparatifs en vue d'une opération par un pays ou par une faction belliqueuse contre des forces ou des infrastructures mécanisées trouveront une application à l'imagerie accessible au public. (…) Judicieusement agencée avec d'autres sources d'information, l'imagerie accessible au public offre la possibilité d'influencer substantiellement les cycles de prise de décision des leaders politiques et militaires. Les applications les plus évidentes seraient le choix des cibles à attaquer et les opérations de planification. La capacité de voir une installation du haut des airs (un réacteur nucléaire, un barrage hydroélectrique ou une garnison militaire) constitue un important avantage dans le processus de planification des opérations d'offensive. Les routes d'infiltration et d'exfiltration pour les attaquants dans la guerre de type guérilla peuvent être mieux planifiées, et une opération intensive d'imagerie pourrait permettre d'identifier des activités normales, des niveaux d'équipement, voire même des dispositifs et des routes de patrouille.*[172]

Des photos prises par satellites civils deviennent disponibles pour le grand public avec des degrés de résolution presque aussi élevés que ceux des satellites militaires et à des prix qui deviendront de plus en plus abordables au fur et à mesure du développement de la concurrence commerciale. Les images commerciales les plus performantes sont fournies par le satellite américain Ikonos, et commercialisées par la société américaine Space Imaging. Des sociétés concurrentes telles que Orbital Imaging (USA), Kiberso (Russie) et Spot Image (Europe) fournissent des images d'une résolution plus basse. Mais les satellites commerciaux non-américains progressent eux aussi vers des résolutions plus fines, aux alentours de deux mètres. Le satellite israélien Eros s'approche de la résolution métrique avec une résolution de 1.8 mètres. Spot 5 offre une résolution de 2.5 mètres. Rocsat pour la Corée et Alos pour le Japon, dont les lancements sont prévus respectivement pour 2003 et 2004, auront tous les deux une résolution proche de 2 mètres en mode panchromatique. La compagnie russe SovinformSpoutnik semble posséder actuellement un système opérationnel d'une résolution de 2 mètres.[173]

L'état du marché satellitaire ne manque pas bien sûr de susciter des réticences et des débats au sein du gouvernement américain qui craint la diffusion de pareilles images à des pays belliqueux ou à des éléments hostiles. Ainsi, celui-ci exige que les constructeurs américains puissent contrôler l'obturateur de tout satellite d'observation vendu à des pays étrangers ou exploité pour eux. Les industriels, globalement soutenus par le Département du commerce sont favorables à une libéralisation du marché, tandis que le Départe-

170. Assemblée de l'Union de l'Europe Occidentale, « *La coopération entre les industries aérospatiales européenne et russe* », Document A/1821, 4 juin 2003, quarante-neuvième session, rapport présenté au nom de la commission technique et aérospatiale par M. Le Guen, rapporteur.
171. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1998
172. STOUT Mark & QUIGGIN Thomas, « *L'exploitation de la nouvelle imagerie satellitaire de haute résolution : des impératifs darwiniens ?* », in Commentaire n° 75, Publication du Service Canadien du Renseignement de Sécurité, été 1998, disponible sur le site www.csis-scrs.gc.ca
173. Comité permanent de contrôle des services de renseignement, rapport d'activité 2000

ment d'Etat et le Pentagone y sont hostiles. Au cours de ces dernières années, les industriels n'ont cessé de marquer des points mais il est certain que le gouvernement américain conserva toujours la possibilité d'interdire la vente d'images de certaines zones sensibles des Etats-Unis ou de ses alliés, de poser des limitations techniques (notamment sur les angles de prises de vues) ou de couper à tout moment le flot d'images. Jusqu'à présent, seul le territoire d'Israël ferait l'objet d'une telle restriction de la part de Washington. Un événement récent illustre cette problématique. A l'automne 2001, lors du déclenchement de l'opération « Enduring Freedom » en Afghanistan, l'Administration Bush voulut s'assurer que ces images de la compagnie Space Imaging et de son satellite Ikonos ne pouvaient tomber entre des mains hostiles, susceptibles d'en faire un usage militaire. Un accord commercial fut conclu entre la compagnie Space Imaging et la National Imagery and Mapping Agency (NIMA), accordant à cette dernière une exclusivité sur les images prises de l'Afghanistan. Signé le 5 octobre pour une durée d'un mois (pour un coût de 1.9 millions de dollars), l'accord fut prolongé le 5 novembre pour un second mois. Ensuite, la NIMA a poursuivi ses commandes sans clause d'exclusivité.[174]

Comme le note le Comité R, *la crainte demeure donc que n'importe quel Etat, qu'il soit pacifique ou belliqueux, et même que n'importe quelle entreprise criminelle ou organisation hostile, puisse bientôt se procurer les moyens d'observer depuis l'espace les systèmes de défense et de sécurité des Etats de droit démocratiques*.[175] Des experts canadiens pointent eux aussi les conséquences potentielles d'un « détournement » de la technologie IMINT : *la grande disponibilité de l'imagerie commerciale à haute résolution pourrait potentiellement avoir la capacité d'influencer considérablement les opérations de sécurité et les guerres, un peu partout dans le monde. Les insurgés, les terroristes et les forces militaires disposant de ressources mécanisées réduites et qui ont la volonté et l'habileté d'exploiter cette nouvelle technologie ont certainement le plus à gagner. En même temps, cette révolution de l'imagerie est susceptible de faciliter le rôle notoirement difficile des forces de maintien de la paix. À la fin, on ne sait pas vraiment si la cause de la paix ne sera pas servie par l'utilisation de ce nouveau produit. Cependant, nous croyons, intuitivement, que chaque pays et les forces infranationales, face à l'impératif darwinien d'exploiter tous les avantages qui leur sont offerts, feront un usage plus efficace de l'imagerie et beaucoup plus rapidement que ne le feront les imposantes bureaucraties aux vues étroites, comme l'Organisation des Nations Unies.*[176]

Laurence Nardon met en exergue les différentes options qui s'offrent à Washington : *l'achat de toutes les images produites serait sans doute coûteux et aléatoire. Quant aux entreprises étrangères, quel que soient leur nombre et la résolution de leurs images, il est peu probable qu'elles acceptent les propositions d'achat exclusif d'une agence de renseignement américaine comme la NIMA. (...) Le buy-to-deny a été une solution de court terme. De l'aveu des responsables de l'actuelle administration, il n'est pas non plus pensable de revenir au shutter control. L'administration doit donc maintenant s'attacher à trouver un nouveau mécanisme de contrôle. Au lendemain de l'opération Enduring Freedom, l'administration Bush repense son approche. Elle doit accepter la possible diffusion de l'imagerie spatiale. Les solutions explorées passent par un dialogue très en amont avec les producteurs américains et étrangers, une utilisation de l'imagerie meilleure et plus rapide que l'ennemi pendant les crises, la préparation dès à présent des ripostes à la diffusion de l'imagerie.*[177]

Quel est, en la matière, l'état de la coopération européenne ?

De la guerre du Golfe au conflit en Afghanistan ou en Irak, en passant par les Balkans, toutes les crises récentes ont confirmé l'importance de l'observation spatiale. Elles ont aussi révélé la domination sans partage des Etats-Unis dans ce domaine en même temps que la dépendance et les carences de l'Europe. Aussi les ministres de l'UE, réunis à Laeken en novembre 2001, ont-ils déclaré qu'il convenait de consentir un réel effort au profit des programmes d'imagerie spatiale de haute résolution afin que l'Europe accède à la maîtrise du renseignement stratégique.[178] Dans son Livre Vert sur la politique spatiale européenne, publié en janvier 2003, la

174. NARDON Laurence, « *Le contrôle de l'imagerie commerciale : après la campagne d ' Afghanistan* », Le Centre français sur les Etats-Unis (CFE), Institut français des relations internationales, Juin 2002

175. Comité permanent de contrôle des services de renseignement, rapport d'activité 2000

176. STOUT Mark & QUIGGIN Thomas, op. cit.

177. Ibid.

178. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

Commission n'élude pas la dimension militaire du secteur : le développement rapide de la PESC/PESD *appelle une attention particulière.*[179] L'analyse de la Commission révèle que l'industrie spatiale est porteuse d'une triple dimension : stratégique, parce qu'elle assure à l'Europe l'indépendance dans l'essentiel des secteurs de l'espace; duale, puisqu'elle intervient à la fois sur les marchés civils et de défense; et de catalyseur, puisqu'elle agit au delà du spatial, notamment pour l'industrie des équipements électroniques grand public et de la distribution télévisuelle. La Commission souligne le défi en ces termes : *la question fondamentale est celle de l'ambition européenne. Aucune des nations européennes ne saurait conduire de manière indépendante une politique spatiale à la hauteur des enjeux. Le fait que les Etats-Unis consacrent six fois plus de ressources publiques à l'espace que l'ensemble des pays européens ne peut laisser l'Europe indifférente si elle veut jouer un rôle dans le monde sur ces questions.* Mais la Commission admet que certains sujets sont délicats : *il s'agit par exemple du degré d'indépendance dont veut disposer l'Europe dans ce domaine stratégique ; de la capacité à traiter globalement la dimension de sécurité et du niveau, du mode et de la cohérence d'investissements qu'elle est prête à consentir.* Enfin, elle note que *les systèmes spatiaux forment le principal outil de collecte, transmission et distribution d'information sur un plan global et le seul qui soit physiquement non-intrusif, grâce aux capacités offertes par exemple par les systèmes de communications large bande et d'imagerie à base optique, infra-rouge ou radar, dont les performances connaissent des progrès spectaculaires. Une composante spatiale en soutien à une capacité de prise de décision rapide contribuerait à rendre crédible et efficace la PESC.*[180]

Un exemple concret de la politique spatiale de l'UE est le développement du système de radiopositionnement par satellites GALILEO, dont les applications en matière de renseignement ne sont que très indirectes, et qui ne sera donc pas traité ici.

En matière d'imagerie satellitaire, les coopérations entre Etats membres se font essentiellement sur base bi- ou multilatérale.

Le programme Hélios 1, auquel participent la France (à hauteur de 78,9%), l'Italie (pour 14,1%) et l'Espagne (7%), s'appuie sur deux satellites militaires optiques Hélios 1A et 1B, mis en orbite depuis Kourou, respectivement en juillet 1995 et en décembre 1999. La composante sol du système comprend des centres principaux à Creil (région parisienne), Patricia di Mare (près de Rome) et Torrejón (près de Madrid), mais aussi des centres de réception des images à Colmar (France), Lecce (Italie) et Maspalomas (Espagne) ainsi qu'une station de théâtre transportable française (STT). Cette coopération est fondée sur le principe d'une exploitation en commun, et non sur un simple accord pour l'échange d'informations entre services alliés. Chaque pays dispose du droit de réaliser des prises de vues au prorata de sa participation financière au programme. Des règles de programmation quotidienne sont établies conjointement par les Etats-Majors et les SR des trois pays. Nous rejoignons l'opinion de l'Assemblée de l'UEO, pour qui *l'exemple de la coopération tripartite autour du système Hélios 1 tend à démontrer qu'une coopération sur les moyens techniques d'acquisition du renseignement favorise une relative harmonisation des politiques et stratégies de renseignement des pays participants*.[181] En 1994, il a été envisagé de lancer, en coopération européenne, le projet Hélios Il, qui devrait offrir des capacités d'observation supérieures à Hélios I, notamment en matière d'observation de nuit grâce à des moyens infrarouges, à une transmission plus rapide des renseignements recueillis et à une précision accrue de ses images pour détecter des cibles tactiques. La France et l'Allemagne ont donc signé le 7 décembre 1995 un accord pour la construction en commun des satellites d'observation Hélios Il et Horus. La France devait être le maître d'oeuvre d'Hélios Il et l'Allemagne, celui d'Horus. Cependant, en avril 1998, l'Allemagne décidait de se retirer du projet Horus. Hélios II – auquel s'est aussi associé la Belgique à hauteur de 2.5% – est considéré comme un saut technologique très important. Ses progrès les plus significatifs sont la reconnaissance de tout objectif d'intérêt militaire, alors qu'Hélios l ne permet la détection que de 80% de ces objectifs, par une amélioration de la résolution ; un service au plus près des utilisateurs, notamment ceux des forces qui auront un accès direct aux images d'archives, à la programmation du système et aux prises de vues réalisées à leur profit. Cette évolution est rendue possible parce que la capacité de production de

179. « *Livre vert – Politique spatiale européenne* », Commission européenne, COM (2003) 17, 21 janvier 2003.
180. Ibid.
181. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

prises de vues est multipliée par trois par rapport à Hélios I. Les images d'Hélios II fourniront les données de géographie numérique nécessaires aux vecteurs et armes de nouvelle génération (Rafale, Tigre, NH 90, Mirage 2000, Apache AP, Scalp EG, AASM, etc.) pour permettre le recalage et la désignation d'objectifs ; une capacité infrarouge, permettant l'observation de nuit par temps clair ainsi que le recueil d'activités de jour et de nuit ; une capacité de prise de vues en très haute résolution ; une division par deux des délais d'acquisition et de mise à disposition de l'information.[182] Pour le maître d'œuvre du projet, la Direction Générale de l'Armement (DGA), *Helios 2 se veut un élément central d'un futur système européen d'observation par satellite. En effet, la France est convaincue que l'avenir réside dans la mise en commun au niveau européen des moyens spatiaux opérationnels et, à ce titre, l'état-major des armées a mis au point un « Besoin opérationnel commun » aujourd'hui partagé par de nombreux pays européens.*[183] Comme le relève l'Assemblée de l'UEO, *cette association n'est pas une fin en soi mais un point de départ vers le développement d'une véritable capacité d'observation européenne avec l'aide de nouveaux partenaires qui pourra prendre forme le plus rapidement possible en s'appuyant sur les acquis existants.*[184]

Après la crise du Kosovo, l'Allemagne décida de développer seule le programme d'observation radar SAR Lupe. Cependant, l'évidente complémentarité des ressources optiques et radar a conduit la France et l'Allemagne à se rapprocher pour échanger des données optiques Hélios II contre des données radar SAR Lupe. L'accord d'échange de capacités passe par l'acquisition d'un «segment sol utilisateur » SAR Lupe en échange d'un accès de l'Allemagne à celui d'Hélios II, ou encore par le développement d'un segment sol commun aux deux systèmes. Il s'agit seulement d'échanger des données existantes ou pouvant être commandées : il n'est pas prévu d'accorder à l'un des deux pays la capacité de programmer les observations réalisées par le satellite de l'autre pays, et vice versa.[185]

Parallèlement au développement de la constellation SAR Lupe, l'Allemagne coopère, depuis 1997, avec la Grande-Bretagne sur le projet InfoTerra/TerraSAR. Ce programme prévoit le lancement vers 2005 de deux satellites radar haute résolution pour l'observation de la terre. Il vise à fournir une capacité d'observation duale, combinant des applications civiles (agriculture, déforestation, cartographie, exploration, géologie et gestion des risques environnementaux) et des applications militaires (prévention et gestion des crises, suivi des conflits, etc.).[186]

L'accord signé entre la France et l'Italie, à l'occasion du sommet de Turin de janvier 2001, définit les principes de la coopération devant régir un grand système multi-capteurs s'appuyant sur de petits satellites pour des missions optiques et radar. Ce système repose sur deux programmes civilo-militaires de satellites dont la mise en place doit se dérouler entre 2003 et 2006. Le programme italien Cosmo Skymed prévoit quatre satellites radar, et le programme français Pléïades, deux satellites optiques haute résolution. Outre les échanges d'informations d'origine satellitaire, l'accord concerne porte également sur le segment sol qui sera développé en commun par les deux parties.[187]

La DGA française a en outre lancé début 2002 le développement du programme « système sol d'observation » (SSO) qui offrira un accès aux images des satellites militaires développés par divers pays européens : images radar des satellites italiens COSMO-Skymed et allemand SAR-Lupe, complétant les images optiques des satellites français HELIOS 2 et PLEIADES (satellite civil).[188]

Mais c'est certainement le Centre satellitaire de l'UE (CSUE) qui est porteur de la dimension la plus européenne ». Depuis l'adoption de l'action commune du Conseil de l'Union européenne du 20 juillet 2001, le CSUE est une agence indépendante. Situé à Torrejon, près de Madrid. Il est opérationnel depuis le 1er janvier 2002 et, si son infrastructure est fournie par l'UEO, il est en fait placé sous le contrôle politique du COPS et la direction opérationnelle du HR/PESC. Le

182. Assemblée de l'UEO, « *Le développement d'une capacité européenne d'observation spatiale pour les besoins de la sécurité de l'Europe* », op. cit.
183. « *Les programmes d'observation, de télécommunication et de systèmes d'information de la DGA : décupler l'efficacité de la décision d'engagement militaire* », site de la Délégation Générale à l'Armement, www.defense.gouv.fr/dga/
184. Assemblée de l'UEO, « *Le développement d'une capacité européenne d'observation spatiale pour les besoins de la sécurité de l'Europe* », op. cit.
185. Ibid.
186. Ibid.
187. Ibid.
188. « *Les programmes d'observation, de télécommunication et de systèmes d'information de la DGA : décupler l'efficacité de la décision d'engagement militaire* », site de la Délégation Générale à l'Armement, www.defense.gouv.fr/dga/

Centre ne dispose pas de satellite propre, et n'est pas une station réceptrice d'images satellitaires. Il s'agit d'un centre d'analyse et d'interprétation. Dans une première phase expérimentale, le centre satellitaire travaillait uniquement avec des images acquises sur une base commerciale auprès de diverses sources européennes et étrangères. Cependant, il intègre à présent des sources ouvertes (images de satellites commerciaux) et des sources classifiées (images de satellites militaires américains et du satellite Hélios I). Le Centre utilise actuellement des images commerciales optiques des satellites Spot 1,2 et 4 (France) ; Landsat 4, 5 et 7 (Etats-Unis) ; IRS l-C et D (Inde) ; KVR, DKl (Russie) ; Ikonos et Quickbird (Etats-Unis), et Eros (Israël). Les images radar correspondent aux satellites ERS 1 et 2 (Agence spatiale européenne) et Radarsat (Canada). Quant aux sources non commerciales, le Centre utilise des images Hélios (France, Italie et Espagne). Le CSUE est chargé de l'exploitation des images issues de l'observation spatiale au profit du Centre de situation ou de l'Etat-major de l'UE en vue de l'élaboration des options stratégiques. A ce titre, il appartient à l'EMUE, et plus particulièrement à sa division Renseignement, d'orienter les recherches du Centre concernant les questions de sécurité et de défense en lui faisant part de ses besoins. Par ailleurs, au niveau de la conduite de l'intervention militaire, l'état-major de l'opération devra être mis en liaison directe avec le Centre de Torrejón. Soixante-huit personnes et trois experts détachés travaillent au CSUE, dont le budget s'élève à 9.3 millions d'Euro.[189]

En dépit des progrès réalisés, le bilan du Centre reste modeste, et l'Assemblée de l'UEO en a relevé les limites : *il reste encore des progrès à accomplir au Centre satellitaire afin d'atteindre le niveau d'efficience des centres militaires nationaux d'exploitation de l'imagerie spatiale. En effet, le Centre de Torrejón étant de nature largement civile et dépourvu d'un personnel suffisant et adapté (interprètes d'images à statut militaire), il peine à assurer le traitement des images en temps quasi réel qui est nécessaire à la conduite des opérations militaires au cours d'une crise. Il s'agit donc de créer en son sein même une véritable division militaire du renseignement, dotée de personnels militaires détachés des divers pays membres, capables de travailler sans limites d'horaires et pouvant être réquisitionnés en temps de crise*. De plus, l'Assemblée de l'UEO estime qu'*afin de délivrer des dossiers images complets, le Centre ne doit pas se limiter à l'analyse des seules images d'origine spatiale, mais doit pouvoir intégrer également les images d'origine aérienne (aéronefs pilotés ou drones) et les corréler ensemble. A terme, il doit devenir une véritable agence européenne de l'imagerie*. [190] Un analyste américain porte un jugement plus sévère : (…) *the Satellite Center's overall utility in a CIP is limited. Its satellite intelligence is useful mainly for background information on such areas as infrastructure. Since the Center does not control its own satellites, it cannot guarantee that it will receive imagery when requested from commercial or foreign suppliers. The time required to access and analyze the imagery is too slow for tactical demands or a fast-moving crisis. It still takes a week to produce a detailed report. Thus, while the Satellite Center has made a small contribution to European intelligence cooperation, it has little to add in its current form.*[191]

L'Assemblée de l'UEO conclut que *l'avenir du Centre dépend, bien entendu, des moyens que l'UE sera prête à lui octroyer, mais aussi du réalisme des missions qui lui seront confiées. (...) le Centre devrait avoir une structure duale, orientée vers le marché mais disposant de compétences militaires. Les sources commerciales serviraient à des missions ordinaires de renseignement à moindre coût. L'utilisation de sources militaires européennes servirait à répondre à des missions extraordinaires, demandant des temps de réaction très courts et des données parfaitement sécurisées. L'UE devra, d'une part, prendre conscience que l'association du Centre à la PESD exigera un élargissement de ses capacités à un environnement militaire et, d'autre part, convenir que l'observation de la terre n'est pas sa seule mission mais qu'il convient d'y ajouter les transmissions, l'alerte avancée, l'écoute électronique et la navigation. Le Centre devra rechercher l'adéquation optimale que la coexistence de systèmes civils performants et d'outils militaires spécialisés autorise.*[192]

189. Assemblée de l'UEO, « *Le développement d'une capacité européenne d'observation spatiale pour les besoins de la sécurité de l'Europe* », op. cit.

190. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

191. VILLADSEN Ole, op. cit.

192. Assemblée de l'UEO, « *Le développement d'une capacité européenne d'observation spatiale pour les besoins de la sécurité de l'Europe* », op. cit.

Par ailleurs, les forces armées des Etats membres de l'UE disposent de capacités non négligeables en termes d'acquisition de renseignement IMINT.

Pour ce qui concerne les avions de reconnaissance, la plupart des forces aériennes des Etats membres disposent d'une composante pilotée spécialisée dans la reconnaissance aérienne, à la fois photographique, infrarouge et radar. La France dispose dans ce domaine d'un large éventail de vecteurs (deux escadrons ou 40 appareils Mirage F1 CR et Mirage IV P) et de capteurs (nacelles photo avec résolution d'environ un mètre, infrarouge et radar). La France dispose en outre de ses Super-Etendard modernisés à bord de porte-avions. L'ensemble de ces appareils sera remplacé par le Mirage 2000-N (équipés des nacelles de reconnaissance de nouvelle génération RECO-NG, à capacité optique et infrarouge, utilisant la technologie numérique) à l'horizon 2005-2006. S'agissant de la surveillance aéroportée du ciel, la future Force de réaction rapide de l'UE pourra s'appuyer sur les AWACS fournis par le Royaume-Uni et la France (un ou deux chacun). Pour la surveillance aéroportée du champ de bataille, si elle ne dispose pas de système semblable aux J-STARS américains (*Joint Surveillance Target Attack Radar System)*, l'UE pourra compter sur le système français héliporté de théâtre HORIZON et, à partir de 2006, sur le système aéroporté britannique ASTOR (*Airborn Stand-Off Radar*).[193]

Les Etats membres de l'UE disposent également de capacités en matière de drones. Les drones (lents) de courte portée satisfont à des besoins tels que « voir derrière la colline », désigner des objectifs avec précision, contrôler en temps réel l'efficacité des feux ou brouiller localement les radiocommunications adverses. En ce domaine, l'UE dispose des drones FOX et CRECERELLE de la France, du BREVEL et du TAIFUN allemand. La Grande-Bretagne développe le système PHOENIX, l'Italie met en oeuvre le MIRACH 26 et l'Espagne le drone SIVA. Les Pays-Bas ont commandé quatre escadrons de drones SPERWER à la société française Sagem. Pour ce qui concerne les drones rapides, destinés à remplir des missions de renseignement tactique au profit des armées de terre dans la profondeur du dispositif adverse, l'UE peut compter sur le drone CL-289 utilisé par la France et l'Allemagne, ainsi que sur le drone italien MIRACH 150. Par contre, l'Europe ne dispose que d'un nombre très limité de drones de longue endurance MALE (seule la France dispose d'une batterie de quatre drones HUNTER israéliens et la Belgique de quatre batteries du même type), et ne dispose d'aucun drone HALE (à haute altitude et longue endurance) semblable au GLOBAL HAWK américain.[194]

Si de nombreux projets sont en cours d'étude en Europe, aucune coopération européenne organisée ne semble en cours. Aussi dans le cadre du « Plan d'action européen sur les capacités » adopté par les membres de l'Union européenne en novembre 2001, a-t-il été décidé de mener des études en commun sur les lacunes en matière de drones, sous leadership de la France.

En conclusion, un expert belge, André Dumoulin, sollicité par le Comité R, a isolé fort à propos un certain nombre d'avantages décisifs d'une autonomie satellitaire : *disposer d'instruments autonomes permettant d'évaluer de façon indépendante, précise et objective la situation générale ou des sites particuliers sur les zones observées et parfois difficile d'accès est l'apanage des satellites d'observation. Liberté de survol, relative invulnérabilité, répétitivité élevée du champ de la surveillance sont aussi associées* à *ces avantages. Ces instruments de surveillance offrent le moyen de fournir des preuves d'agression, de contrôler le respect des accords diplomatiques et de désarmement, de dissuader un Etat partie de violer ceux-ci, d'observer les zones de crises, de détecter des tensions, d'aider* à *anticiper, prévenir et désamorcer autant que faire se peut les conflits locaux, régionaux ou inter-étatiques pouvant justifier d'une intervention internationale diplomatique et militaire, d'accompagner des prépositionnements de forces, d'aider* à *la gestion des crises et de conduire les guerres (détection, ciblage) et parfois de suppléer* à *l'absence de forces prépositionnées comme outils de renseignement. Ces outils de surveillance apportent en partie la garantie de ne pas être entraîné contre son gré dans des opérations multinationales en permettant la vérification de l'argumentaire diplomatique et militaire international (exercice de contre-manipulation et de recoupement d'informations). Aussi, de facto, leur simple existence peut réduire la suspicion parfois bien présente même entre pays alliés. Le renseignement satel-*

193. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

194. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.

litaire apporte des éléments à interpréter au profit du renseignement militaire, du renseignement d'intérêt militaire et du renseignement de défense global. Il permet d'apporter certaines réponses à *certains domaines connexes* à *la sécurité comme le domaine environnemental ou bio-géographique, tout en offrant l'exemple type du multiplicateur de forces. La multiplication et la redondance des systèmes de surveillance en complémentarité avec I'HUMINT contribuent, lorsqu'ils sont bien gérés et traités, à réduire la possibilité de passer* à *côté d'indications essentielles du point de vue du renseignement militaire; quand bien même le nombre de données recueillies accroît souvent le risque de ne pas les déceler* à *temps.*[195] Mais on retiendra surtout ce constat tourné vers l'avenir : *les pays qui font l'effort de se munir de moyens satellitaires au service de leur défense et de leur diplomatie ont franchi une étape qui les différencie des autres, parce qu'ils les mettent en prise directe avec les événements se déroulant au-delà de l'horizon.*[196]

Pour ce qui concerne la coopération européenne dans son ensemble, l'Assemblée de l'UEO émet un jugement contrasté. Dans un rapport de juin 2002, elle déplore que *l'Europe spatiale est plutôt la somme d'une série de programmes nationaux que le résultat d'une vraie politique européenne, bien que notre continent puisse se prévaloir de compétences techniques très poussées, d'une communauté scientifique très forte et d'une importante industrie. Malheureusement, l'absence d'une volonté politique a, jusqu'à présent, empêché notre continent d'avoir une réelle politique spatiale.*[197] Mais dans un autre rapport – datant de la même époque - elle se veut somme toute optimiste : *en conclusion, ces coopérations techniques permettent de donner un élan à l'Europe du renseignement spatial mais ne sont pas la garantie de la mise en place future d'un véritable système commun européen. Elles se révèlent pourtant indispensables pour la simple raison qu'aucun des membres de l'Union européenne n'a les moyens de s'équiper, au niveau national, de toute la panoplie d'éléments de recueil et de traitement nécessaire en matière de renseignement. La poursuite du programme Hélios 2 avec les Belges et les Espagnols, complétée par les accords Pléïades/Cosmo Skymed et Hélios/SAR Lupe, est un signe encourageant, et on pourrait envisager à terme un système global européen d'observation de l'espace en commençant par fédérer les segments sol des différents systèmes existants*.[198]

La nécessité d'obtenir au meilleur prix des technologies toujours plus sophistiquées et donc coûteuses sera en effet un puissant levier à une coopération européenne : *dans un contexte de ralentissement économique général, toute ambition spatiale d'envergure passe désormais par une politique européenne de coopération extrêmement volontariste. Et pour dépasser le cadre actuel, jugé trop restreint, des coopérations bilatérales ou trilatérales, il faudrait pouvoir définir, dans l'ensemble des domaines spatiaux, des besoins communs aux pays de l'UE. De même, il apparaît souhaitable de confier l'expertise technique ainsi que la maîtrise d'ouvrage des programmes à un organisme mandaté par l'ensemble des pays de l'Union européenne. (...) Dans un souci de réduction de coûts, il faut également rechercher toutes les synergies civilo-militaires possibles, tant au niveau des équipements que des services, lorsqu'elles répondent au besoin opérationnel. Si les avantages que présente la dualité sont nombreux, elle a aussi ses limites. Les applications militaires sont souvent exigeantes en performances et imposent parfois des contraintes d'emploi liées à la confidentialité et à la sécurité des missions. La dualité ne peut que se renforcer ; mais se priver de satellites militaires représenterait une sérieuse régression sur les plans opérationnel et technique dans la mesure où les industriels européens ont acquis un niveau d'excellence dans de nombreux domaines qui intéressent les militaires. Quelles sont, parmi les applications du domaine spatial militaire, celles qui pourraient concourir à l'édification d'une défense européenne ? Cette démarche est-elle réaliste ?*[199]

195. Comité permanent de contrôle des services de renseignement, Rapport d'activités 1998
196. Ibid.
197. Assemblée de l'UEO, « *Le développement d'une capacité européenne d'observation spatiale pour les besoins de la sécurité de l'Europe* », op. cit.
198. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
199. Assemblée de l'UEO, « *Le développement d'une capacité européenne d'observation spatiale pour les besoins de la sécurité de l'Europe* », op. cit.

Conclusions : Relever le défi d'un nouvel environnement et d'une nouvelle finalité du renseignement

Nous rejoignons pleinement le constat de Klaus Becher, Bernard Molard, Frédéric Oberson et Alessandro Politi : *l'élaboration d'une politique européenne de renseignement peut être considérée comme nécessaire, compatible avec d'autres politiques et réalisable. Elle est nécessaire parce que, du point de vue professionnel, aucune agence européenne ne peut, à elle seule, faire face à l'explosion mondiale de l'information et aux implications de l'OSINT ainsi que du renseignement économique qui engendrerait une liste impressionnante de besoins dans le domaine de la collecte de renseignements. Une autre raison tient à la réduction des budgets. Au niveau national, les ressources bien trop limitées pour couvrir le financement de nouveaux programmes de collecte technique de renseignements ou une capacité importante d'évaluation multisource à l'intérieur et à l'extérieur des services de renseignement, voire même pour maintenir les moyens existants. Enfin, une politique semble nécessaire parce qu'elle est saine politiquement et qu'elle reconnaît les limites des Etats-nations européens indépendamment de la manière dont l'intégration européenne peut évoluer. Les renseignements qu'obtiendraient les responsables politiques grâce à une synergie européenne seraient de meilleure qualité et plus objectifs que ceux que leurs budgets limités leurs permettent d'acheter. Une telle politique serait compatible avec les liens de confiance et les alliances existants parce qu'elle se fonderait sur les conséquences de l'évolution actuelle et des décisions politiques prises à un plus haut niveau. Elle permettrait non seulement le maintien de relations privilégiées, mais pourrait également les relancer. Elle ne mettrait pas en cause les intérêts sécuritaires spécifiques, mais permettrait une coopération chaque fois que cela serait possible et souhaitable. Elle est réalisable parce qu'elle serait mesurée à l'aune des avantages concrets attendus, et parce qu'elle offrirait un cadre clair pour un effort commun afin de résoudre les anciens problèmes communs ainsi que les nouveaux défis : satellites, OSINT, renseignement économique, guerre de l'information, guerre des réseaux, formation commune et emploi d'analystes, évaluation commune du renseignement multisource. Ces éléments ainsi que les nouveaux risques sécuritaires sont des domaines possibles de coopération dans le cadre d'une politique européenne de renseignement souple, informelle, mais clairement définie.*[200]

L'environnement dans lequel évolue le monde du renseignement a changé. Le 11 septembre n'a fait que grossir des constats déjà formulés auparavant.

D'une part, comme l'a remarqué l'expert canadien Pierre Cloutier, *le renseignement n'est pas et n'est plus l'apanage exclusif des Etats et des gouvernements. Les grandes agences gouvernementales ne sont plus les seules à produire du renseignement et constitueront probablement même dans l'avenir des groupes minoritaires. Le renseignement n'est pas non plus l'apanage exclusif des organisations privées ou publiques. (...) chaque individu deviendra non seulement un consommateur mais aussi un producteur de renseignement. Le renseignement n'est plus relié exclusivement aux questions de sécurité nationale.* [201]

D'autre part, l'évolution technologique, et notamment l'explosion de réseaux d'information mondiaux, a brouillé la distinction traditionnelle entre le renseignement stratégique et le renseignement tactique, a placé les SR nationaux en situation de concurrence autant que de coopération.

Enfin, la nature même de la menace terroriste a brouillé la distinction habituelle entre « Law Enforcement » et « Intelligence », entre ce qui relève de l'ordre national et ce qui ressort de l'étranger, entre la sphère publique et le secteur privé. Comme le note Gregory Treverton, *ce genre d'intervention est peut-être la plus difficile de toutes, car elle oblige les services de renseignements de tous les pays non seulement à partager des informations entre eux, mais à travailler chez eux avec divers représentants gouvernementaux et simples citoyens, qui sont de nouveaux venus dans le domaine du renseignement et découvrent ce qu'est le renseignement et ce qu'il peut faire ou non.*[202]

On serait tenté d'évoquer une « révolution copernicienne » du renseignement, à l'instar de la « Revolution in Military Affairs ». A. Denis Clift, Président du "Joint Military Intelligence

200. POLITI Alessandro, « *De la nécessité d'une politique européenne de renseignement* » op. cit.
201. CLOUTIER Pierre, op. cit.
202. TREVERTON Gregory F., « *Remodeler le renseignement pour le partager avec « nous-mêmes* », Commentaire n° 82, Publication du Service Canadien du Renseignement de Sécurité, 16 juillet 2003 (disponible sur le site csis-scrs.gc.ca)

College", n'estime-t-il pas en effet: *The Internet era is a dynamic with an on-rush of changes both revolutionary and far more subtle to the work of intelligence: changes in the doctrine and practice of collection, analysis, and dissemination; and changes in the relationship and the mindset between intelligence and law enforcement, intelligence and the policy-maker, and intelligence and the military commander.*[203] Lors d'une autre conférence, il ajoute: *Intelligence professionals understand as never before that in this new era intelligence is the air the nation breathes, that their work must be relevant, with underlined emphasis on the importance of warning, it must be accessible when and where needed, it must be actionable, and they must accept accountability for the intelligence provided or not provided.*[204]

Plus précisément, le président du « National Intelligence Council » américain, John C. Gannon prédit une « révolution » dans cinq domaines: dans la communication avec les responsables politiques au plus haut niveau; dans la collaboration avec de nouveaux partenaires au sein même des administrations, comme avec les forces de l'ordre; dans la manière d'appréhender les nouvelles technologies; dans le recrutement et la formation d'un personnel qualifié; dans l'ouverture et la transparence au monde extérieur.[205]

Si le défi est de taille, il n'est pas pour autant insurmontable car comme le relève le Colonel EMG Baud, officier suisse et auteur d'une anthologie des SR, *les cadres des services de renseignement changent fréquemment et les structures s'adaptent relativement rapidement. A la fin de la guerre froide, c'est-à-dire jusqu'en 1997 environ, la plupart des services ont allégé leurs structures, les pays d'Europe orientale ont totalement restructuré et réorienté leurs services (souvent plusieurs fois consécutives). Puis, après de 11 septembre de nouvelles questions ont surgi et commencent à provoquer des changements profonds dans les services*.[206] Le Colonel Baud constate encore qu'*on ne s'était jamais vraiment posé la question de la finalité du renseignement et ses structures étaient davantage issues d'une évolution historique que d'une réflexion sur la manière de produire le renseignement*.[207]

Cette « nouvelle stratégie » du renseignement doit s'apprécier dans une perspective à long terme car, comme le note très justement Alexis Debat, *le renseignement obéit très peu aux principes de base de la théorie des investissements, selon laquelle tout accroissement de capacités provoque instantanément une amélioration des résultats. Et c'est encore plus vrai dans un domaine aussi complexe et aléatoire que la lutte contre les réseaux terroristes, surtout lorsque celle-ci tend vers un objectif aussi fantasmagorique que la sécurité absolue. (...) Bref, plus que des fonds ou des directives supplémentaires, le travail de terrain des soldats de l'anti-terrorisme nécessite du temps et un vivier d'expertise dont la constitution prendra plusieurs années. Plus encore, il exige une capacité à investir à long terme - c'est-à-dire la liberté de gaspiller - ses ressources dans des opérations ou au profit d'individus apparemment improductifs, mais qui peuvent, un jour ou l'autre, se révéler extrêmement fructueux.*[208]

Encore faut-il concevoir la finalité de ce processus, car le « renseignement » n'a de sens que s'il est utilisé dans un contexte d'aide à la décision (en anglais « decision support »).[209] La sensibilisation des différents acteurs est fondamentale pour que chacun se sente concerné, comme le note un autre officier de renseignement français, le Lieutenant-Colonel de Barmon : *le renseignement n'est ni une fin en soi, ni une activité strictement reservée à certains spécialistes: il concerne tout le monde à des degrés divers. Il est l'une des préoccupations majeures du chef, quel que soit son niveau, il doit permettre d'anticiper l'action de l'adversaire ainsi que ses réactions face à nos propres actions*.[210] Constat semblable pour l'Assemblée de l'UEO, qui souligne que *le renseignement offre ainsi une grille d'analyse permettant l'évaluation stratégique. Celle-ci, à terme, devra servir à présenter des options stratégiques aux décideurs*

203. CLIFT Denis, « *From Semaphore to Predator - Intelligence in the Internet Era* », Yale University Apri127, 2002
204. CLIFT Denis, « *Catching Field Mile - Intelligence and Policy in the 21th Century* », Harvard University February 20, 2003
205. GANNON John C., « *The role of the Intelligence Services in a globalised world* », .20 May-August 2001, SISDE (Servizio per le Informazioni e la Sicurezza Democratica, Rivista di Intelligence e di cultura professionale.
206. « *Le renseignement aujourd'hui: entretien avec le colonel EMG Baud* », 20 juillet 2003, checkpoint-online.ch
207. Ibid.
208. DEBAT Alexis, « *Voyage au cœur du renseignement américain* », in Politique internationale, n°95, Printemps 2002.
209. CLOUTIER Pierre, « *Renseignement et sécurité dans l'âge de l'information: les défis du Québec* », Centre de recherche sur la sécurité et le renseignement, cloutip@cam.org
210. de BARMON (Lieutenant-Colonel), *« La fonction renseignement »*, op. cit.

politiques. C'est au cours de cette phase que l'on doit permettre aux décideurs l'accès à l'ensemble des observations, évaluations et planifications réalisées afin qu'ils puissent prendre une décision et définir précisément le but de l'opération et les moyens à y consacrer. [211]

Lors de son audition devant la commission du renseignement de la Chambre des Représentants, Anthony H. Cordesman, Président de la « Arleigh A. Burke Chair for Strategy » pointe le danger de « politiser » le renseignement : *one key lesson of the Iraq War is still that it is dangerous to over-politicize intelligence and to not provide a picture of the threat and reasons for warfighting that is properly qualified. Overselling thé threat before a war leads to overreacting during a conflict, and major credibility problems in the aftermath of thé conflict that can interfère with nation building and limit domestic and international support in future conflicts.*[212] Le scandale auquel est actuellement confronté le Premier Ministre britannique Tony Blair, accusé d'avoir « manipulé » des renseignements fournis par ses experts pour sur-évaluer délibérément les capacités ADM de l'Irak, illustre cette problématique et ses conséquences.

Mais les responsabilités sont sans doute partagées, comme l'admet le Colonel Baud : *il est généralement coutume de rejeter sur la classe politique l'erreur de ne pas utiliser le renseignement et de ne pas avoir cette « culture du renseignement » que nous envions tellement à nos partenaires anglo-saxons. La réalité est un peu plus complexe et il faut se demander si le produit offert correspond aux besoins du marché…* [213]

Face à ces défis multiples, établir cette « Europe du renseignement » pourrait être une occasion unique de faire entrer les SR de plain-pied dans le XXIème siècle.

Les attentats de Madrid ont suscité de nombreuses reactions plaidant pour un renforcement du renseignement européen, sans que ces déclarations d'intention soient au demeurant très concrètes. Dans son programme d'action adopté le 18 mars 2004, la Commission propose cinq types d'action, y compris un renforcement de la coopération opérationnelle. Mais l'Exécutif précise : *This new coordination mechanism should neither be a European CIA not just a second pillar instrument. Terrorism is first and foremost an internal security matter and therefore the mechanism we suggest to establish should exchange information mostly within a third pilar umbrella. In this way, we put existing – Community, Union, international and national – networks in dialogue among themselves rather than losing time destroying existing and creating new procedurally time-consuming institutions and bodies*.[214]

Sous réserve des mesures concrètes qui pourraient être décidées au niveau européen dans les semaines et les mois à venir, force est de constater que les propositions de la Commission nous laissent perplexes :

- Placer des « réseaux en dialogue » ne changera rien à la situation actuelle : ces réseaux existent déjà, de manière informelle ou sur base de protocoles d'échange entre services. La politique du « donnant-donnant » se poursuivra, alors que l'expérience démontre qu'elle génère opacité et inefficacité.
- Au demeurant, la référence à une « CIA européenne » illustre la méconnaissance de la « communauté du renseignement » américaine, où la CIA n'est qu'un service parmi les … 14 existants ! Elle n'est la plus importante ni en budget, ni en personnel – seulement en célébrité…
- La Commission évoque une « coordination », mais que coordonnera-t-on ? les échanges de renseignements obtenus sur base de directives et de priorités nationales ? ou coordonnera-t-on la recherche de renseignements entre SR de l'UE sur base d'une « politique de renseignement européenne » ?

La Commission limite sa réflexion au seul problème du terrorisme, ce qui illustre qu'elle agit « dans l'urgence », sans embrasser l'ensemble des missions des SR. Elle considère le problème comme relevant de la « sécurité intérieure », pour laquelle une bonne partie des SR est … incompétente ! (puisqu'ils ne peuvent agir qu'en dehors de leur territoire national). Seuls seraient donc couverts les services de contre-ingérence.■

211. Assemblée de l'UEO, *« Renseignement européen : les nouveaux défis – Réponse au rapport annuel du Conseil »*, op. cit.
212. CORDESMAN Anthony H., "*Sufficiency of Inteligence in Iraq: Emerging Issuesand Lessons Learned*", Testimony before the Permanent Select Committee on Intelligence United States House of Representatives , July 24, 2003
213. « *Le renseignement aujourd'hui: entretien avec le colonel EMG Baud* », 20 juillet 2003, checkpoint-online.ch
214. MEMO/04/66 – 18 mars 2004. www.europa.eu.int

GRIP

GROUPE DE RECHERCHE
ET D'INFORMATION
SUR LA PAIX ET LA SÉCURITÉ

Fondé en 1979 à Bruxelles, le GRIP est un institut de recherche indépendant qui étudie les questions de défense, de sécurité et de désarmement. Par ses travaux, le GRIP veut contribuer à une meilleure compréhension de ces problématiques dans la perspective d'une amélioration de la sécurité internationale en Europe et dans le monde.

Adresse : rue Van Hoorde, 33
B -1030 Bruxelles
TEL: (32.2) 241.84.20
FAX: (32.2) 245.19.33
E.Mail: admi@grip.org
Website: http://www.grip.org

(bureaux ouverts du lundi au vendredi de 8h30 à 13h et de 13h30 à 17h)

LES PUBLICATIONS DU GRIP

Depuis sa fondation, le GRIP est surtout connu par son travail d'édition. Au fil du temps, les publications ont changé, tant au niveau du contenu, de la présentation que de la périodicité. Depuis l'automne 1997, elles se présentent sous trois formes :

1. Les Nouvelles du GRIP

Une lettre d'information trimestrielle de 8 pages : regard sur les grands dossiers du moment, nouvelles insolites, aperçu des activités du centre, etc.

Cette lettre est envoyée d'office à tous les **membres du GRIP** en règle de **cotisation** de même qu'aux abonnés aux « Livres du GRIP ».

2. Les Livres du GRIP

Chaque année, le GRIP publie 5 ouvrages en collaboration avec les éditions Complexe, abordant les questions internationales dans les domaines de la géo-stratégie, de la défense et de la sécurité internationale.

Ces 5 ouvrages font partie de l'abonnement aux « Livres du GRIP » ; ils sont également disponibles en librairie et au GRIP.

3. Les Rapports du GRIP

Cette nouvelle collection (format A4, sans périodicité) valorise des travaux de recherche réalisés pour la plupart au GRIP.

Ces rapports sont envoyés d'office à tous ceux qui souscrivent un abonnement de soutien ; ils peuvent aussi être commandés au GRIP.

Tarifs 2004

	Belgique	Autres Europe	Autres Monde
1. Cotisation			
Abonnement aux «Nouvelles du GRIP»	15 euros *605 FB*	16 euros *645 FB*	18 euros *726 FB*
2. Les Livres du GRIP			
Abonnement annuel aux 5 livres[1] et aux «Nouvelles du GRIP»	75 euros *3.025 FB*	85 euros *3.428 FB*	90 euros *3.630 FB*
3. Abonnement complet[2]			
Abonnement à toutes les publications (Rapports inclus)	125 euros *5.042 FB*	140 euros *5.647 FB*	150 euros *6.050 FB*
4. Abonnement de soutien	250 euros *10.084 FB*	250 euros *10.084 FB*	250 euros *10.084 FB*

1. L'abonnement couvre 5 livres (équivalant à 10 numéros), plus le trimestriel «Les Nouvelles du GRIP».

2. L'abonnement annuel complet inclut la collection des Rapports (non périodiques), avec en moyenne six parutions par année.

Vous souhaitez vous abonner ?

Vous pouvez le faire par téléphone (02/241.84.20), par fax (02/245.19.33), par Email (publications@grip.org) ou en nous envoyant votre demande d'abonnement, accompagnée de votre payement, au GRIP, rue Van Hoorde 33 B -1030 Bruxelles.

Modes de paiement : **Belgique** (virement au compte 001-1711459-67du GRIP à Bruxelles; virement au CCP 000-1591282-94 du GRIP à Bruxelles; bulletin de virement) / **France** (chèque barré; mandat postal international) / **Luxembourg** (soit verser au CCP 86464-37 du GRIP à Luxembourg; soit envoi d'un chèque au GRIP, libellé en FL) / **Autres pays** (virement au CCP 000-1591282-94 du GRIP à Bruxelles; mandat postal international / **Autre moyen de paiement** (carte de crédit - VISA, Eurocard, Mastercard - Précisez votre n° de carte et la date d'expiration.

Les Rapports du GRIP

1/97 **Ex-Yougoslavie - L'embargo sur les armes et le réarmement actuel**, Georges Berghezan, 32p., 7,44 euros.

2/97 **FN Herstal : Quel avenir pour la tradition armurière ?**, Luc Mampaey, 20p., 4,96 euros.

3/97 **Burundi : trafics d'armes et aides militaires**, Human Rights Watch, 60p., 11,16 euros.

1/98 **L'industrie belge de défense - Adaptation, consolidation et mythe de la reconversion**, Luc Mampaey, 84p., 12,39 euros.

2/98 **Kosovo : poudrière des Balkans**, Sevdi Zymberaj et Bernard Adam, 21p., 7,44 euros.

3/98 **Concepts et potentiels nucléaires 1999-2000**, André Dumoulin, 35p., 7,44 euros.

4/98 **La Belgique et les satellites de renseignement**, André Dumoulin, 23p., 4,96 euros.

5/98 **Le programme HAARP : science ou désastre ?**, Luc Mampaey, 84p., 11,16 euros.

1/99 **Les armes non létales - Une nouvelle course aux armements,** Luc Mampaey, 40p., 8,68 euros.

2/99 **La guerre du Congo-Kinshasa - Analyse du conflit et transferts d'armes vers l'Afrique centrale**, Georges Berghezan et Félix Nkundabagenzi, 54p., 9,92 euros.

3/99 **Post-Cold War Conversion in Europe - Defence Restructuring in the 1990s and the Regional Dimension**, collectif, 104p., 17,35 euros.

1/00 **La détention d'armes par les civils - Armes à feu : un enjeu en matière de Santé publique**, Sophie Nolet, 44p., 8,68 euros.

2/00 **Marquage et traçage des armes légères**, Ilhan Berkol, 72p., 14,87 euros.

3/00 **Bilan de la guerre du Kosovo : Résultat des frappes - Fin du conflit - La reconstruction - La situation en Serbie-Monténégro**, Valérie Peclow et Bernard Adam, 56 p., 9,92 euros.

4/00 **National Missile Defense - Le retour de la guerre des étoiles et les enjeux stratégiques**, Aris Roubos et Michel Wautelet, 60p., 9,92 euros.

5/00 **L'Union européenne et la prévention des conflits africains**, Félix Nkundabagenzi, 28p., 7,44 euros.

6/00 **Groupe Herstal S.A. - L'heure des décisions**, Luc Mampaey, 34p., 7,44 euros.

7/00 **La disponibilité des armes légères illicites - Comment combattre cette menace internationale**, Peter Lock, 34p., 7,44 euros.

1/01 **Le micro-désarmement - Le désarmement concret en armes légères et ses mesures associées**, Michel Wéry avec la contribution de Georges Berghezan et Félix Nkundabagenzi, 64p., 13 euros.

2/01 **Le réarmement de la Sierra Leone - Un an après l'accord de paix de Lomé**, Eric G. Berman, une étude de Small Arms Survey, 42p., 8,50 euros.

3/01 **La disponibilité des armes à feu - Quel impact sur la sécurité et la santé publique ?**, collectif, 40p., 8,50 euros.

4/01 **La conférence des Nations unies de juillet 2001 sur les armes légères - Analyse du processus et de ses résultats**, Ilhan Berkol, 58p., 11 euros.

5/01 **L'ONU face au terrorisme**, Sandrine Santo, 38p., 8,50 euros.

1/02 **La Chine et la nouvelle Asie centrale - De l'indépendance des républiques centrasiatiques à l'après-11 septembre**, Thierry Kellner, 40p., 8,50 euros.

2/02 **L'Union européenne et la prévention des conflits - Concepts et instruments d'un nouvel acteur**, Félix Nkundabagenzi, Caroline Pailhe et Valérie Peclow, 72p., 13 euros.

3/02 **L'Inde et le Pakistan - Forces militaires et nucléaires en présence**, Françoise Donnay, 40 p., 8,50 euros.

4/02 **Les exportations d'armes de la Belgique**, Bernard Adam, Sarah Bayés, Georges Berghezan, Ilhan Berkol, Françoise Donnay, Luc Mampaey et Michel Wéry, 72 p., 13 euros.

1/03 **Les relations arméno-turques - La porte close de l'Orient**, Burcu Gültekin et Nicolas Tavitian, 32p., 7 euros.

2/03 **La crise ivoirienne - De la tentative du coup d'Etat à la nomination du gouvernement de réconciliation nationale**, Claudio Gramizzi et Matthieu Damian, 45p., 9 euros.

3/03 **Enfants soldats, armes légères et conflits en Afrique - Les actions de la coopération au développement de l'Union européenne et de la Belgique**, Claudio Gramizzi, Félix Nkundabagenzi, Sophie Nolet et Federico Santopinto, 44p.

4/03 **Questions juridiques sur la régionalisation des licences d'armes**, Nicolas Crutzen, 28p., 7 euros.

1/04 **Controlling arms brokering - Next steps for EU member states**, Holger Anders, 34p., 7 euros.

2/04 **Bilan d'un an de guerre en Irak - Analyse des coûts et des éléments déclenchants**, Caroline Pailhe avec la collaboration de Valérie Peclow et Federico Santopinto, 51p., 9 euros

---

Les « Rapports du GRIP » sont peu diffusés en librairie. Avant tout disponibles au GRIP et sur www.grip.org