N° 16 – Décembre 2006

Les Cahiers du CESA

Revue pédagogique du Centre d'études stratégiques aérospatiales

Nouvelles réalités du renseignement

Les défis du renseignement moderne

L'utilisation croissante des drones dans la manœuvre du renseignement militaire

La montée en puissance de l'intelligence économique

Enseignement militaire supérieur air du 2e degré

www.cesa.air.defense.gouv.fr

Les Cahiers du CESA
Enseignement militaire supérieur air du 2e degré

N° 16
Décembre 2006

Nouvelles réalités du renseignement

Numéro réalisé en collaboration avec le Centre français de recherche sur le renseignement (CF2R)

Directeur de publication : Gba Guillaume Gelée

Rédacteur en chef : Lcl Julian Alvarez / Rédacteurs en chef techniques : Cdt Cyril Marchand, Ltt Muriel Berger / Maquette : M. Emmanuel Batisse, M. Philippe Bucher / Diffusion : M. Pierre d'Andre, Sgt Audrey Lahon, Avt Julien Biguine

Impression : Atelier de photographie et de reproduction de l'armée de l'air (APRAA)
26, boulevard Victor - 00460 ARMÉES

Centre d'études stratégiques aérospatiales : 1 place Joffre - B.P. 43 - 00445 ARMÉES
Tél. : 01 44 42 80 64 - MTBA : 821 753 80 64 - Fax : 01 44 42 80 10 - www.cesa.air.defense.gouv.fr

Tirage 3 600 exemplaires - ISSN 1770-9342

Avant-propos

Le renseignement est depuis cinq ans à la pointe de la lutte contre le terrorisme djihadiste. D'où l'intérêt nouveau que lui portent les médias, les politiques et l'opinion publique. L'association renseignement/terrorisme masque cependant le fait que cette discipline a connu, depuis la fin de la guerre froide, un renforcement considérable de son rôle dans tous les domaines de la sécurité nationale (défense, sécurité intérieure, lutte contre la criminalité, etc.), mais aussi dans la vie des entreprises (compétition économique).

Au cours de la décennie écoulée, le monde du renseignement a été en effet confronté à une triple évolution :

– modification des champs d'intérêts traditionnels ; la sphère d'activité des services de renseignement ne cesse de s'étendre sous l'effet de l'imbrication croissante des enjeux politiques, économiques et militaires ;

– bouleversement des méthodes de travail ; lutter contre des menaces transnationales non étatiques a entraîné une évolution notable de la manière dont s'organisent et opèrent les professionnels du renseignement.

– révolution technique ; l'apparition des nouvelles techniques de l'information (acquisition, transmission, cryptage, stockage et traitement automatique des données) offre de nouvelles possibilités et pose de nombreux problèmes inédits aux organismes de renseignement.

C'est l'objectif de ce numéro des *Cahiers du CESA* de présenter aux cadres de l'armée de l'air les évolutions récentes du renseignement en termes généraux comme dans les domaines proches de leurs préoccupations.

Bonne lecture !

Les défis du renseignement moderne

La disparition de l'URSS et les attentats du 11 septembre 2001 ont entraîné une remise en question radicale des cibles et des méthodes du renseignement en vigueur depuis plusieurs décennies. En moins de dix ans s'est produite une profonde évolution de la manière dont s'organisent et opèrent les professionnels du renseignement.

À partir de 1989, l'évolution de la situation internationale a amené la communauté occidentale du renseignement à reconsidérer son action en fonction de nouveaux paramètres. Avec la disparition de la menace fondamentale que faisait peser jusqu'alors l'Union soviétique, le monde a évolué vers une forte instabilité. D'idéologique, la scène compétitive est devenue générale et l'imbrication des enjeux politiques, économiques et militaires s'est affirmée comme la caractéristique majeure du nouvel environnement international. En conséquence, les services de renseignement ont dû abandonner les grilles de lecture qui prévalaient depuis plusieurs décennies. **Les attentats du 11 septembre et la montée en puissance du terrorisme djihadiste ont encore accru la remise en cause du métier.** En l'espace d'une dizaine d'années, le monde du renseignement a connu une véritable révolution culturelle.

La nouvelle insécurité mondiale

L'évolution que le monde a connue depuis la chute du mur est beaucoup plus lourde de conséquences pour les milieux du renseignement que celle qui survint à la fin du second conflit mondial avec la défaite de l'Allemagne. Car avant même la fin des hostilités, un nouvel ennemi – le communisme soviétique – était très clairement apparu et l'ensemble du dispositif mis en place pour lutter contre le nazisme put être aussitôt redéployé contre Moscou. **Depuis 1989 une nouvelle logique s'est progressivement imposée :** la disparition d'une menace bien identifiée, probable, a cédé le pas à la diversification des enjeux et à la dispersion géographique des crises.

La principale conséquence de la disparition de la rivalité Est-Ouest a été **le renforcement du rôle de l'économie comme domaine principal de compétition entre les nations.** La guerre pour les parts de marché que se livrent, dans tous les secteurs, les États est devenue un fait déterminant. Ce conflit est d'une intensité sans cesse croissante et ses lignes de force orientent l'action des gouvernements et de leurs services, l'objet de cet affrontement étant, pour chaque pays, de créer chez lui, ou à son profit, des emplois, des revenus et d'augmenter ses ressources.

Un autre effet de la nouvelle situation internationale est **l'apparition de nouveaux acteurs non étatiques qui développent des stratégies indépendantes de tout contrôle gouvernemental** (ONG, mafias, mouvements religieux radicaux, diasporas ethniques, etc.). En conséquence, des dangers nouveaux, provenant d'organisations transnationales du crime, du terrorisme ou de la fraude, sont apparus.

Surtout, depuis cinq ans, le **terrorisme djihadiste s'affirme comme la menace principale contre la sécurité internationale.** C'est un terrorisme planétaire, mené par une nébuleuse de groupes radicaux ultraviolents, agissant de manière non coordonnée.

Ces mouvements puisent leur légitimité dans les frustrations des sociétés musulmanes comme dans l'exaspération provoquée par la politique américaine au Moyen-Orient, notamment l'intervention en Irak.

L'organisation du renseignement subit le contrecoup de ces évolutions internationales. La diversification des menaces, l'apparition de nouveaux acteurs, l'affirmation du terrorisme islamique et la révolution des techniques de l'information entraînent une transformation profonde des méthodes de travail.

Les nouvelles conditions d'acquisition, de traitement et d'exploitation des données

Les enjeux contemporains demandent des connaissances et des renseignements de plus en plus étendus et précis. Dans la nouvelle situation mondiale, caractérisée par l'interdépendance, toutes les zones stratégiques doivent être connectées et aucun secteur de l'activité humaine ne doit être négligé. Plus la civilisation est évoluée, plus les informations qu'une nation doit obtenir sur les activités de ses adversaires et alliés sont étendues et complexes.

Conséquence directe de la révolution de l'information et de la multiplication des sources ouvertes, **dans tous les domaines, la masse des données à exploiter ne cesse de croître**, souvent dans des proportions considérables. L'information essentielle est de plus en plus noyée dans une surabondance de données secondaires. Les capacités de traitement revêtent désormais une importance déterminante, comparable à celle de la recherche du renseignement lui-même. **Les défis majeurs sont devenus l'analyse, la validation et la diffusion des informations** en temps réel aux organismes qui ont besoin d'en connaître. Cela exige un très grand nombre d'experts qui ne peuvent être basculés indifféremment d'un domaine à un autre : du militaire au financier, de l'industriel au diplomatique, du scientifique au criminel.

Par ailleurs, les services ne peuvent plus prétendre tout traiter seuls. Cela rend impérative l'amélioration des échanges et de la coordination entre les services de sécurité intérieure et extérieure, et nécessaire une collaboration accrue entre ces services spécialisés et les organismes, publics ou privés, agissant dans le domaine du traitement de l'information ouverte. La recherche de la complémentarité, bien que difficile, s'avère indispensable.

Aujourd'hui, une partie très importante des informations peut être obtenue par des moyens techniques (ELINT, SIGINT, COMINT, IMINT)*, ainsi que par les sources électroniques (réseaux Internet et bases de données). Mais, si des solutions techniques de plus en plus perfectionnées existent, les performances d'un service de renseignement tiennent d'abord aux connaissances et au professionnalisme des femmes et des hommes qui le composent. **La guerre du Golfe a montré les limites physiques du renseignement technique** : malgré les considérables moyens mis en œuvre, les Américains n'eurent jamais assez de traducteurs ni d'analystes pour digérer la totalité des informations obtenues grâce à l'interception des communications irakiennes. En dépit des performances sans cesse améliorées des moyens d'interception, d'obser-

* Voir glossaire p. 32.

vation et de traitement automatique des données, **l'intuition et l'interprétation humaines demeurent irremplaçables, en particulier dans des domaines tels que l'analyse ou la recherche secrète.**

Enfin, **la notion de secret elle-même évolue** avec l'accélération des découvertes et la multiplication des sources d'information. Il devient de plus en plus difficile de protéger un secret à l'âge de l'information. Aujourd'hui, grâce à la performance des moyens de communication et à la rapidité avec laquelle doivent se prendre les décisions, la vitesse d'exploitation s'affirme comme la meilleure sécurité, et l'avantage opérationnel est passé dans le camp de ceux qui exploitent rapidement et systématiquement le renseignement.

La remise en question des méthodes de travail

L'efficacité du renseignement se trouve également remise en cause par la structuration originale et les méthodes nouvelles de la nébuleuse terroriste Al-Qaida. **En effet, rien n'est plus difficile que de lutter contre une organisation virtuelle, qui n'a ni territoire, ni base arrière, qui fonctionne quasiment sans centre de commandement** et qui est entièrement décentralisée. En particulier, l'organisation d'Oussama ben Laden est extrêmement difficile à infiltrer, du fait de la base nationale ou tribale de ses différentes composantes.

La nouvelle menace djihadiste a conduit les services occidentaux et arabes à remettre en question leurs modes de fonctionnement hérités de la Guerre froide, pour s'adapter à ce nouveau danger. Cela s'est traduit par plusieurs nouveautés en matière de recherche du renseignement :

– **la nouvelle primauté du renseignement intérieur** : la lutte contre le terrorisme est un combat qui commence d'abord sur le territoire national. C'est une lutte de l'intérieur vers l'extérieur ;

– **la part grandissante du travail effectué en coopération internationale** : une investigation contre un réseau djihadiste est nécessairement transfrontalière, car le terrorisme ne connaît pas de frontières. Les enquêtes se font en coopération internationale, afin d'obtenir une vue d'ensemble des activités d'un réseau. Une nécessaire évolution des mentalités doit avoir lieu, notamment dans la coopération avec les services de renseignement du Moyen-Orient, dont l'expertise et le niveau démocratique sont différents des nôtres. En effet, face à la prolifération tous azimuts du terrorisme, une grande partie des opérations repose désormais sur les polices et les services de sécurité locaux, dans des pays où les terroristes sont parfaitement intégrés au sein de la population ;

– **la redécouverte du renseignement secret** : l'information critique recherchée pour empêcher un acte terroriste est extrêmement difficile à obtenir, car rare et protégée. Le renseignement recherché se trouve dans la mémoire d'un individu, dans un appartement, dans un ordinateur non connecté à Internet, etc. C'est une différence essentielle avec la période de la Guerre froide, pendant laquelle les services de renseignement cherchaient

à identifier des objectifs de beaucoup plus grande taille (divisions blindées soviétiques, sites de missiles ou bases aériennes), sur lesquels diverses approches pouvaient apporter des résultats. Aujourd'hui, les secrets adverses sont de plus en plus protégés – donc difficiles d'accès – et les « structures utiles » à pénétrer de plus en plus difficiles à identifier ;

– **la relativisation du renseignement technique** : la technique, si puissante soit-elle, a beaucoup de mal à suivre l'accroissement exponentiel des communications et à décoder rapidement les dispositifs de cryptage utilisés par les terroristes. Les nouvelles techniques de l'information et de la communication – notamment la numérisation des données – imposent de nouvelles spécialités techniques qui n'existaient pas quelques années auparavant ;

– **l'exigence de transparence démocratique** : un défi auquel est désormais confronté le renseignement est le besoin de transparence et d'information du public. C'est aussi un enjeu important pour les services eux-mêmes, car il est important d'expliquer à l'opinion publique ce qui se passe afin de pouvoir la mobiliser, d'être soutenu et de recruter. Toutefois, le secret doit être reconnu comme éthique par le public, les médias et les politiques. Il doit être considéré comme essentiel à la protection des opérations et à la sécurité du pays. En revanche, la violation du droit international et le développement de méthodes coercitives (Guantanamo, Abou Ghraïb) – qui sont d'une inutilité reconnue par les spécialistes – choquent profondément nos sociétés démocratiques ayant une exigence éthique sans cesse croissante.

Vers un nouveau paradigme ?

La remise en cause de l'ordre politique international a imposé aux services de renseignement des défis d'une nature et d'une dimension nouvelles. **La profession, qui avait déjà beaucoup évolué après la chute de l'URSS, s'est transformée dans des proportions encore plus marquantes depuis septembre 2001.** La sphère d'activité des agences de renseignement ne cesse de s'étendre, car, en raison de la diversification des menaces, les services spécialisés ont élargi le champ traditionnel de leurs investigations.

L'importance du renseignement reste par ailleurs prépondérante lors des interventions militaires extérieures, lesquelles se font systématiquement dans un cadre international, comme on a pu l'observer lors de la guerre du Golfe, en Somalie, au Cambodge, en Bosnie et au Kosovo. Il semble ainsi que l'on se dirige vers une inévitable coopération multilatérale en matière de renseignement, soit par des échanges d'informations, soit par un partage des tâches. Toutefois, en raison de la compétition économique et culturelle accrue entre les anciens alliés, pour chaque pays se posent le problème de l'indépendance des moyens d'acquisition et la délicate équation indépendance/coopération qui en résulte. Les pays européens devraient prendre conscience en cette occasion de la primauté américaine en matière de renseignement. Cela devrait permettre de bâtir un outil commun, capable de conférer à l'Europe l'autonomie nécessaire.

Éric Denécé
Directeur du Centre français de recherche sur le renseignement

Les limites des politiques d'interception satellitaires face aux nouveaux modes opératoires terroristes

Le développement des interceptions satellitaires pratiquées par les services occidentaux a conduit les terroristes à abandonner les moyens de communication modernes. En utilisant les transmissions en ondes courtes combinées à Internet, ils ont développé un mode de communication fiable et original qui échappe aux écoutes dirigées contre eux.

En pleine guerre ouverte contre le terrorisme international, il est difficile d'évoquer les interceptions sans imaginer immédiatement de grandes paraboles dressées vers le ciel, écoutant les satellites de communication orbitant autour de la terre.

Dans ce contexte, parler de transmissions en ondes courtes (ou ondes HF) au XXIe siècle peut paraître pour le moins désuet. Alors que tout le monde surfe sur Internet, envoie des *e-mails* sur toute la planète, le téléphone portable collé à l'oreille, nous serions en droit de croire que les procédés de transmission utilisant les ondes courtes sont devenus obsolètes. D'autant que **les services étatiques d'interception ne parlent plus que d'interceptions satellitaires par lesquelles transiteraient la majorité des communications privées, professionnelles ou encore officielles mondiales.** D'ailleurs ceux qui ont eu l'occasion d'approcher des installations d'écoutes, en Europe comme aux États-Unis, ont pu observer le changement rapide des antennes qui ne sont plus composées que de paraboles et autres radômes. Un signe qui ne peut tromper un œil averti.

Pourtant certaines analyses tendent à mettre en lumière les limites de cette évolution. Elles font apparaître que les services chargés des interceptions se sont probablement trop engagés en misant sur le « tout satellite ».

La persistance des communications clandestines en ondes courtes (HF)

À titre d'exemple, souvenons-nous du cas de cette analyste américaine de la *Defense Intelligence Agency* (DIA) américaine arrêtée par le FBI, le 21 septembre 2001. Ana Belen Montes, 44 ans, avait rejoint la DIA en 1985. D'après les enquêteurs, elle fournissait des renseignements aux services cubains depuis 1996. Le résultat de l'enquête menée après son arrestation a montré qu'elle recevait ses instructions grâce à un récepteur radio à ondes courtes :

Authorities declined to say what led them to focus on Montes or how they believed she became associated with the Cuban government. They said she communicated with her Cuban handlers via *shortwave radios, computer diskettes and pagers, methods employed by a Cuban spy ring based in Florida – known as the Wasp Network – that attempted to infiltrate Cuban exile organizations and U.S. military installations*[1].

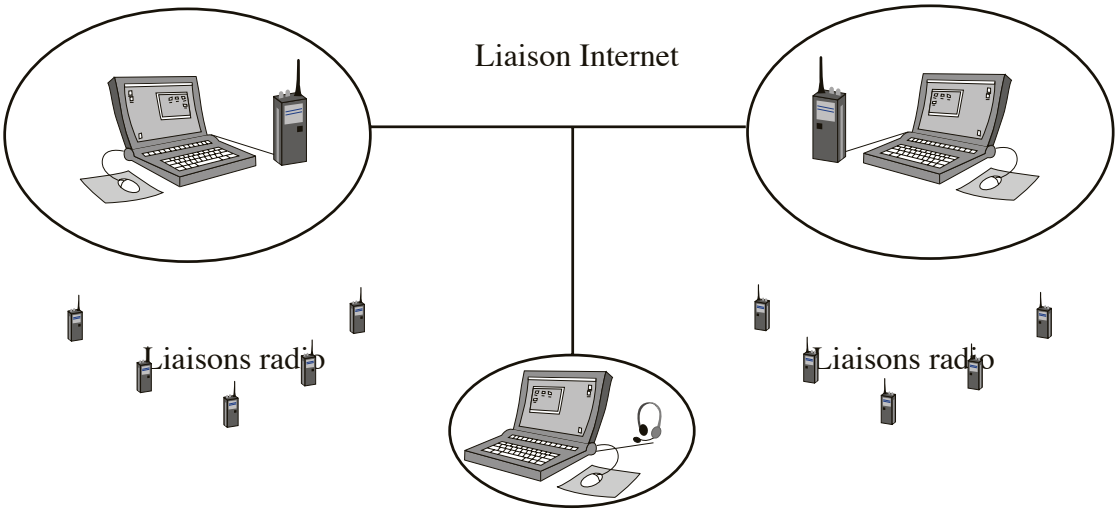
1. *Washington Post*, 22 septembre 2001.

Avant l'ère du satellite, ce type d'émission, constituée par la diffusion de groupes de chiffres énumérés par une voix synthétique, a été longtemps une des priorités des services d'écoutes de tous les pays. Il était clairement établi que ces émissions chiffrées étaient destinées aux agents clandestins infiltrés en pays ennemis. Durant la Guerre froide, ce type de transmission foisonnait. D'ailleurs on pouvait fréquemment les entendre dans différentes langues allant du russe à l'allemand, en passant par le roumain, le bulgare, le tchèque, l'anglais et même le français. Le système permettait à l'agent infiltré de recevoir, en toute discrétion, directives et autres messages de sa centrale. Avec la disparition de l'Union soviétique, ces émissions cessèrent. Les services d'écoutes occidentaux, dont l'objectif principal était le monde communiste, durent revoir leurs priorités.

À la même époque, le grand public apprit l'existence du réseau anglo-américain *Echelon*, capable d'intercepter toutes les communications téléphoniques et courriers électroniques mondiaux. L'exemple américain fut immédiatement suivi par de nombreux États. Après l'attribution des crédits nécessaires, de nouvelles antennes se déployèrent et se mirent à traquer les satellites gravitant autour du globe. **Petit à petit les ondes HF furent donc délaissées**.

Or, de plus en plus fréquemment, des radioamateurs passionnés par ce type de communication, rapportent que **les transmissions de chiffres – appelées outre-Atlantique *Numbers Stations* – reprennent leurs activités. Terroristes et criminels figureraient parmi les utilisateurs de ce mode de communication.** Mais cela ne suffit pas, semble-t-il, à changer les orientations techniques des grands services SIGINT, d'autant qu'une partie du matériel HF a été remisé. Pourtant, le cas Ana Beles Montes démontre, une nouvelle fois, que suivre aveuglément l'exemple américain n'est pas forcément un gage de réussite.

Les communications terroristes par ondes courtes



DR

Comment Al-Qaida déjoue les interceptions américaines ?

La lutte contre le terrorisme est un bon exemple d'une certaine inadaptation des politiques d'interception actuelles. **Non seulement le fait d'avoir sur écoute tous les téléphones de la planète n'a pas permis aux Américains de capturer Oussama ben Laden[2], mais cela a encouragé les terroristes à éviter ce type de transmission au profit de moyens radioélectriques traditionnels** (spectre HF), aujourd'hui délaissés par les grands services d'interception.

Un des premiers à l'avoir signalé est Georg Klingenfuss, un ressortissant allemand, spécialiste de l'écoute radio, qui publie régulièrement des recueils de fréquences et autres manuels de codes. Sur son site Internet, il n'hésite pas à indiquer, capture d'écran à l'appui, que **les réseaux terroristes tels qu'Al-Qaida communiquent grâce aux ondes courtes.** Il cite, pour exemple, les nouveaux systèmes de transmission permettant l'acheminement d'*e-mails* par radio, utilisés par les ONG, notamment le Comité international de la Croix-Rouge (CICR). Or, certaines ONG opérant en Afrique et en Asie se seraient fait dérober plusieurs de ces émetteurs. Par ailleurs, la radio bulgare a fait état, par le passé, d'une information selon laquelle **des membres d'Al-Qaida se seraient procuré, au Japon, du matériel performant de radiocommunication HF.**

Un nouvel élément vient corroborer cette théorie. Il a été publié le 2 janvier 2006 par la presse privée algérienne. Il s'agit de la capture d'Abou Billel El-Oulbani, présumé représentant d'Al-Qaida pour la région Afrique/Maghreb. Lors de son arrestation par les forces de sécurité algériennes, il a été découvert une « station radio UHF ultrasophistiquée » installée dans une maison abandonnée au sommet d'une colline. Celle-ci aurait été utilisée pour communiquer avec les différents réseaux d'Al-Qaida en Afrique.

Il est important de noter qu'il s'agit d'une station UHF (*Ultra High Frequency*, ou ultra haute fréquence), c'est-à-dire utilisant des fréquences qui, en fonction de la topographie et des puissances utilisées, offrent une portée dépassant rarement la centaine de kilomètres. Si cette station était bien utilisée pour transmettre sur de plus longues distances, cela indiquerait l'utilisation d'un procédé bien connu des radioamateurs : **il s'agit d'un système alliant Internet et la radio**, hypothèse rendue encore plus vraisemblable quand on sait que parmi les objets saisis figurent trois ordinateurs portables. **Il suffit alors pour transmettre de relier la radio à un ordinateur équipé d'un logiciel spécifique.** De tels programmes existent et sont même gratuits. Développés par des radioamateurs, ils permettent de communiquer dans le monde entier à travers des réseaux privés reliés à Internet et connectés entre eux. Ce système permet de transmettre de deux manières : soit à partir d'un ordinateur connecté à Internet qui activera un émetteur-récepteur implanté n'importe où dans le monde ; soit à l'inverse, grâce

2. On se souvient de l'information, largement médiatisée, selon laquelle la *National Security Agency* (NSA) écoutait le téléphone satellitaire d'Oussama ben Laden, notamment lorsqu'il prenait des nouvelles de sa mère, alors hospitalisée.

DR

Des terroristes pourraient communiquer entre eux par cybercafés pour se donner des informations ou même des ordres d'exécution sans se faire repérer par les services de renseignement.

DR

à un émetteur-récepteur, il est possible de se connecter à un ordinateur relié à Internet qui fera transiter la communication à l'autre bout de la planète, si besoin est.

Concrètement, **Ben Laden pourrait très bien donner ses instructions au Groupe salafiste pour la prédication et le combat (GSPC) algérien à partir d'un cybercafé de Jalalabad, sa voix étant retransmise par un émetteur situé sur les hauteurs d'Alger,** et cela avec très peu de moyens et de en toute discrétion, puisque la majeure partie des services d'écoutes étatiques, suivant l'exemple américain, a délaissé les traditionnelles écoutes radio, au profit de l'interception satellitaire.

Un procédé particulièrement discret

Ce système de transmission a la particularité d'utiliser différents procédés. Tout d'abord, la partie transitant par Internet allie la technique dite *Peer to Peer* et la téléphonie IP*, rappelant à la fois les techniques utilisées pour le partage des fichiers audios (MP3 et autres) et la téléphonie *via* Internet. Sachant qu'actuellement les services officiels en sont à la définition des normes d'interception de telles communications, et qu'ils ont fixé un délai de 18 mois aux fournisseurs d'accès pour leur fournir la possibilité technique de procéder à des interceptions légales, il ne fait aucun doute que **ce procédé offre une grande sécurité pour ses utilisateurs.**

La seconde partie utilise les ondes radioélectriques traditionnelles. Bien que les interceptions radio aient considérablement diminué, le risque d'être écouté demeure. Cependant, si l'émission radio sert uniquement à donner des instructions à des activistes déployés sur le terrain, elle peut se faire à partir de stations isolées ne comportant qu'un ordinateur et une radio, un ensemble totalement autonome. D'ailleurs, en ce qui concerne la découverte opérée par les forces algériennes, l'installation se trouvait dans une maison abandonnée. On peut facilement imaginer que les terroristes utilisent plusieurs stations relais. Seuls ces émetteurs sont susceptibles d'être détectés par les services d'écoutes, les destinataires pouvant se borner à recevoir leurs instructions sans émettre eux-mêmes. De plus, de nouvelles stations radio associées à un ordinateur portable peuvent être facilement et rapidement déployées. Il est donc aisé pour les logisticiens de remplacer une installation découverte par les forces de sécurité et de maintenir ainsi une infrastructure de communications opérationnelle, relativement sûre et discrète.

* Voir glossaire p. 32.

Ce procédé permet ainsi à tout leader d'Al-Qaida disposant d'une connexion Internet de s'adresser par radio à des terroristes répartis dans le monde entier. L'individu n'ayant besoin d'aucun matériel spécifique, il peut être très mobile et déjouer ainsi toute surveillance éventuelle. Il sera donc très difficile pour un service spécialisé d'intercepter ses communications

Cette découverte confirme qu'**Al-Qaida utilise des moyens de communications radio traditionnels, des moyens maintenant abandonnés par la plupart des organismes officiels, y compris les services d'écoutes.** Preuve en est le dernier scandale des écoutes illégales ordonnées par George Bush dans le cadre de la lutte antiterroriste. Il s'agit presque exclusivement d'écoutes téléphoniques, procédé qui ne semble plus avoir la faveur des terroristes. Le fait de délaisser les écoutes radioélectriques classiques au profit de l'interception par satellites a ouvert une faille dans laquelle semble s'être engouffrée Al-Qaida.

L'utilisation offensive des interceptions

Il existe cependant quelques services qui, s'ils sont toujours un peu sourds lorsqu'il est question d'écouter les ondes courtes, ont su **utiliser l'interception des téléphones cellulaires ou des communications par satellites à des fins beaucoup plus offensives que la simple écoute.**

Citons pour exemple les services israéliens qui, en 1996, ont éliminé l'artificier du Hamas, Yeyia Ayache, grâce à son GSM. Après avoir mis hors service sa ligne fixe, les Israéliens l'ont forcé à utiliser son portable préalablement piégé. Après avoir identifié sa voix, ils ont déclenché à distance l'explosion de son appareil, le tuant sur le coup[3].

Les Russes ne sont pas en reste, puisque, quelques mois plus tard, ce fut au tour du président indépendantiste tchétchène, Djokhar Doudaev, de subir un sort semblable. Utilisant un téléphone satellitaire, il fut localisé par les services de Moscou qui déclenchèrent aussitôt un raid aérien sur sa position. Il fut tué lors de cette attaque[4].

Gageons que si la chute de l'Union soviétique a révolutionné la politique mondiale des interceptions, le 11 septembre 2001 aura un effet similaire. Espérons que ce tragique événement ouvre un peu plus les yeux des décideurs et les encourage à prendre en compte l'avis des spécialistes confrontés quotidiennement à la réalité du terrain.

Alain Charret
Rédacteur en chef de la lettre électronique *Renseignor*, chercheur associé au CF2R

3. *Le Point*, n° 1218, samedi 20 janvier 1996, p. 21.
4. *Le Point*, n° 1232, samedi 27 avril 1996, p. 23.

L'utilisation croissante des drones dans la manœuvre du renseignement militaire : l'exemple des États-Unis

Depuis une décennie, les drones sont de plus en plus étroitement associés aux opérations militaires. Le développement d'engins de nouvelle génération, aux capacités infiniment supérieures aux précédentes, va encore accroître leur utilisation et conduire à une modification leur doctrine d'emploi.

La guerre du Golfe ayant joué un rôle de révélateur, les drones ont été ensuite de plus en plus étroitement associés aux opérations. Sans aucune prétention à l'exhaustivité, cet article a pour ambition d'attirer l'attention des lecteurs sur quelques tactiques basées sur une utilisation innovante des *Unmanned Aerial Systems* (UAS).

Le Global Hawk*, drone aérien de tous les superlatifs*

Les capacités des engins *High Altitude, Long Endurance* (HALE) sont telles que l'expression « satellites de théâtre » a parfois été utilisée pour les évoquer ; le *Global Hawk* américain constitue à ce titre un exemple emblématique.

Son envergure de 35 mètres est supérieure à celle d'un *Boeing 737* ; il peut, en partant du territoire continental des États-Unis, rejoindre l'espace aérien bosniaque, y orbiter 24 heures d'affilée puis revenir à son point de départ, sans ravitaillement en vol : son endurance est de 41 heures pour plus de 25 000 kilomètres de distance franchissable. Lors de l'exercice *Linked Seas* en mai 2000, le quatrième prototype du drone effectua un vol transatlantique aller-retour en décollant de la base aérienne d'Englin à destination des îles Madère et du Portugal. Grâce à une liaison de données satellitaire, un *Global Hawk* peut transmettre en temps réel l'imagerie à l'autre bout du monde. **La superficie de la zone qu'un seul engin est capable de surveiller est d'environ 140 000 km², soit le quart de la surface du territoire français métropolitain.**

Photo John Schwab, *US Air Force*

Contrôle technique d'un drone *Global Hawk* à Beale AFB en Californie.

Actuellement, le programme RQ-4 se déroule tambour battant : « *Les* Global Hawk *totalisent plus de 5 000 heures de vol dans le cadre de la guerre contre le terrorisme. En action de manière quasiment ininterrompue depuis le 11 septembre 2001, les drones de ce type ont accompli 233 missions en soutien des opérations en Irak et en Afghanistan. Sur ces 233 missions, 157 ont été accomplies par un seul* Global Hawk *(...). La synthèse des opérations de combat indique que les RQ-4 ont procuré l'imagerie de 55 % des cibles militaires pendant la phase initiale du conflit irakien*[5].» En novembre 2005, la société *Northrop Grumman* a du reste signé un contrat cou-

vrant le lancement de la production de 5 RQ-4B, version agrandie du RQ-4A ; le nouveau modèle emporte 1 360 kg de charge utile contre 900 pour son prédécesseur.

Photo Daniel McLain, *US Navy*

La miniaturisation des drones a induit le développement de tactiques innovantes.

Mais déjà, les autorités militaires américaines travaillent sur le successeur du *Global Hawk*. Dénommé *SensorCraft*, il volera à une altitude de près de 20 000 mètres et sera polyvalent. **L'engin pourra en effet tout à la fois surveiller l'espace aérien de manière active ou passive, jouer le rôle de radar météo, localiser, poursuivre et identifier les cibles terrestres même camouflées, intercepter les communications radio ainsi que les ondes radar, analyser les substances NRBC contaminant une zone et enfin brouiller les émetteurs adverses.** Pour ce faire, le *SensorCraft* sera avant tout un drone littéralement bâti autour de ses senseurs dont les antennes seront noyées dans la masse de la structure afin de limiter les forces de traînée aérodynamiques.

Tactiques innovantes pour drones légers

À l'autre bout de l'échelle des dimensions, **la multiplication des drones légers ouvre la voie à un foisonnement de tactiques nouvelles.**

Un système à propulsion électrique tel que le *FQM-151A Pointer* équipé d'une caméra thermique permet ainsi d'effectuer une reconnaissance discrète d'un objectif non coopératif en ambiance nocturne. Pour ce faire, l'engin prend de l'altitude à la verticale d'un point situé en dehors du périmètre de l'installation puis la survole en planant après avoir coupé son moteur.

Utilisés par les équipes de forces spéciales infiltrées en zone contrôlée par l'ennemi, des drones légers peuvent aider à l'acquisition des cibles au profit de l'aviation d'appui-feu. C'est le cas au sein du *United States Air Force Special Operations Command* où les commandos *Special Tactics* ont désormais intégré le drone aérien miniature *Battlefield Air Targeting-Camera Autonomous MAV* (BAT-CAM) à leur *Battlefield Air Operations Kit*. À l'origine, le développement du BAT-CAM fut inauguré par des étudiants de la *Brigham Young University* qui eurent l'idée originale de concevoir un drone léger à ailes repliables. Cette particularité motiva l'intérêt de l'*Air Force Research Laboratory* : tout d'abord conçues en papier pour une envergure de 61 cm, les ailes du BAT-CAM sont maintenant en fibres de carbone et nylon pour une envergure réduite à 51 cm. Cette caractéristique intéressante s'allie à la simplicité d'emploi de l'engin qui peut se diriger automatiquement vers un point simplement

5. Jim Skeen, « *Spy planes pass 5,000 hours* », *dailynews.com*, 4 janvier 2006.

désigné sur la cartographie affichée à l'écran d'un ordinateur portable ou d'un assistant digital personnel. Équipé d'un moteur électrique, d'une caméra vidéo couleur, d'un système de navigation satellitaire et d'un autopilote miniaturisé, le BAT-CAM dans sa forme actuelle ne constitue cependant qu'une première étape. Une version ultérieure verra son envergure réduite à 30 cm ou moins ; elle emportera des senseurs chimiques, une caméra thermique de vision nocturne ou des « *tags* » (étiquettes) pour « marquer » les véhicules ennemis dont les équipes de forces spéciales désirent suivre les déplacements.

Drone propriétaire ou délégation de contrôle ?

L'un des premiers problèmes qui s'est posé en matière d'intégration d'un drone aérien au sein d'un système a été d'analyser ce que signifiait contrôler un tel engin. Cinq niveaux ont en conséquence été définis[6] :

- Niveau 1 : réception et transmission secondaires d'imagerie et de données.
- Niveau 2 : réception d'imagerie et de données provenant directement du drone.
- Niveau 3 : contrôle de la charge utile du drone, en particulier des senseurs.
- Niveau 4 : contrôle de toutes les fonctions à l'exception du décollage et de l'atterrissage.
- Niveau 5 : contrôle total des fonctions du drone.

En décembre 2003 pour la première fois, un contrôle de niveau 5 a été établi par un avion de patrouille maritime *P-3C Orion* américain sur un drone à voilure tournante *Fire Scout*. Quelles tâches pourraient ainsi être confiées à ces engins sans pilote asservis à un appareil piloté ? Pour le capitaine Steve Eastburg, officier de programme au sein du Commandement naval des systèmes aériens, il s'agit « *d'améliorer la capacité de survie de la plate-forme habitée, de diminuer le temps nécessaire aux opérations de ciblage, d'améliorer la connaissance de la situation tactique ainsi que l'acquisition des données relatives à l'évaluation des dégâts après bombardement et enfin de jouer le rôle de relais de communication au profit d'un groupe de combat naval* »[7].

Le *P-3C* peut donc, par délégation, assurer le contrôle d'un drone ; cela n'empêche nullement les Américains de développer un engin « propriétaire » : c'est le *Coyote* qui ressemble à « *un croisement entre un avion et un obus d'artillerie* »[8]. Muni d'ailes rétractables lui conférant une envergure de 76 cm lorsque dépliées, ayant une endurance de 90 minutes et une vitesse de croisière de 96 km/h, l'engin a été conçu pour pouvoir être lancé depuis les cavités cylindriques où sont habituellement logées les bouées acoustiques.

6. *http://www.globalsecurity.org/intell/systems/uav_tcs.htm*.
7. « *NAVAIR Demonstrates Control of UAV at Highest Level* », *US Naval Air Systems Command*, 22 décembre 2003.
8. Michael Peck, « *Undersized Drone Promises Extended Maritime Surveillance* », *National Defense Magazine*, janvier 2006.

Chacune des deux solutions dont il est ici question présente des inconvénients ; le couple *Orion*/*Coyote* met en évidence ceux dont pâtit la solution du « drone propriétaire ». Les impératifs techniques dictés par la cellule porteuse imposent parfois des choix difficiles. Ainsi, le *Coyote* sera considéré comme consommable car ne pouvant être récupéré par l'avion. Parallèlement, le volume dévolu aux bouées acoustiques étant à la fois intangible et limité, autonomie et capacité d'emport du drone ont été mesurées au plus juste alors même que les conditions de lancement ont imposé de concevoir d'emblée pour l'engin une structure relativement solide, donc lourde. Pourtant, la solution du drone propriétaire léger n'est pas dénuée d'intérêt : elle permet, généralement à court terme et à moindre coût, de raccourcir la boucle OODA (observation, orientation, décision, action). Outre le *Coyote*, d'autres drones propriétaires sont en cours de gestation ; mentionnons par exemple le *Wing Store UAV* qui pourra être lancé depuis un panier de roquettes M260/M261 équipant les hélicoptères d'attaque américains.

La délégation de contrôle, un impératif interarmées

Dès lors que l'on situe l'action dans le cadre d'un contexte interarmées, la délégation de contrôle permet une gestion souple des moyens lorsque, par exemple, **une station terrestre appartenant à l'armée de l'air assure la gestion d'une mission attribuée à un engin habituellement contrôlé par l'armée de terre**, et réciproquement.

Photo Craig Strawser, *Us Navy*

Un *ScanEagle* appartenant à l'*US Navy* a participé à un exercice visant à améliorer la coopération interarmées.

Photo Kurt Lengfield, *US Navy*

Le *Fire Scout*, premier drone à avoir été entièrement contrôlé depuis un avion de patrouille maritime.

En milieu d'année 2004, outre-Atlantique, l'exercice *Forward Look* a ainsi conjointement impliqué des drones aussi différents que le *Predator* (*US Air Force*), *le Shadow* (*US Army*) et le *ScanEagle* (*US Navy*) ; il s'agissait en l'occurrence d'en tester l'interopérabilité. Les trois types de drones ont été utilisés de la manière suivante : au *Predator* revenait la tâche de couvrir une zone étendue et de détecter un éventuel objectif, à la suite de quoi le *Shadow*, plus petit, devait confirmer l'intérêt de celui-ci et le localiser avec précision ; le drone léger *ScanEagle* était alors utilisé à son tour pour assurer la permanence de l'observation sur un objectif ponctuel.

Mais **les difficultés techniques relatives à la compatibilité ne peuvent être surmontées que par la méthode prudente des petits pas.** Aux États-Unis, c'est cette méthode qui a été choisie lorsqu'il a été estimé judicieux d'examiner l'intérêt présenté par le couplage entre un drone *Hunter* et un aéronef d'attaque, en premier lieu un hélicoptère *AH-64D Apache Longbow*[9]. Engagé par l'armée de terre américaine, le programme *Airborne Manned-Unmanned System Technology* (AMUST) a ainsi permis le lancement du programme *Hunter-Stand-Off Killer Team* (HSKT) par l'*US Army Aviation Applied Technology Directorate*[10]. Le programme en question dépasse le strict cadre du combat aéromobile puisqu'il a pour ambition d'étendre le principe expérimenté avec des hélicoptères *AH-64D Apache Longbow* aux avions d'attaque *F/A-18* de l'*US Navy* emportant une munition *Joint Stand-Off Weapon*.

Quoi qu'il en soit, cette initiative a été à l'origine du processus **de formalisation par les services de l'armée de terre américaine de la doctrine d'emploi relative à l'utilisation d'unités mixtes drones/hélicoptères**, formalisation annoncée *urbi et orbi* en janvier 2003, dans le cadre d'un symposium[11]. Ainsi, chaque *Brigade Combat Team* de l'*US Army* future englobera trois formations mixtes, chacune d'entre elles étant dotée de 12 hélicoptères d'attaque et de 8 drones. Ces formations auront pour mission principale la reconnaissance armée, mais seront également capables de procurer aux troupes terrestres un appui-feu aérien rapproché.

Jean-Jacques Cécile
Directeur de recherche au CF2R

9. Version de l'hélicoptère d'attaque *AH-64 Apache* équipée d'un radar pour la détection des cibles.
10. « *UK To Join US Hunter-Killer UAV Tests*? », *Unmanned Vehicles Online*, 18 janvier 2001.
11. Marcia Triggs, « *Aviation adds recon team to ranks* », *Army News Service*, 13 janvier 2003.

Les Américains inventent la surveillance aérienne non traditionnelle

Les réalités de la guerre en Irak ont donné naissance, outre-Atlantique, à une nouvelle méthode qui consiste à tirer profit, à des fins de renseignement, d'informations acquises par des capteurs n'ayant pas été spécifiquement développés à cet effet (aéronefs, missiles), notamment afin de détecter la présence d'engins explosifs improvisés ou de combattants adverses.

Les militaires américains, c'est connu, sont férus d'acronymes. Parmi ceux dont ils parsèment leur jargon, un nouveau vient d'apparaître : NTISR, pour *Non Traditional Intelligence, Surveillance and Reconnaissance*. De quoi s'agit-il ?

Le banc d'essai irakien

Photo Bradley Garfiled, US Marine Corps

En Irak, la NTISR, par moyens aériens, contribue à lutter contre la prolifération des IED.

Une plaisanterie fortement teintée d'humour noir circule outre-Atlantique : **les seules armes de destruction massive que les Américains ont finalement trouvées en Irak sont les engins explosifs improvisés ou *Improvised Explosive Devices* (IED).** Car c'est bien de destruction massive qu'il s'agit : « *Selon le* Central Command, *il y a eu 5 607 attaques en 2004 ; en 2005, il y en a eu 10 953* »[12]. Plus nombreuses, les bombes « artisanales » deviennent également plus puissantes. Les premières auxquelles les troupes américaines furent confrontées, en mars 2003, avaient la taille d'une cannette de bière. Actuellement, **il n'est pas rare que des blindés soient littéralement mis en pièce par des engins composés de plusieurs obus d'artillerie** explosant simultanément. Quelle que soit la puissance des IED, il s'agit là d'une guerre sans fin qui ne laisse aucun répit aux troupes de la coalition : « *Il y a une route que nous appelons l'Allée des IED que les démineurs nettoient régulièrement. Ils n'ont même pas encore atteint la fin de ce tronçon de treize kilomètres que les insurgés ont déjà parfois commencé à poser à nouveau des IED au début* »[13], déclare le sergent Robert Lewis de Carrollton, en Georgie.

Dans ce contexte, il n'est nullement étonnant que le Pentagone cherche des solutions afin d'enrayer ce phénomène. Parmi les nouveaux outils permettant de combattre le fléau, il en est un qui innove : **la *Non Traditional Intelligence, Surveillance and Reconnaissance*. Cette nouvelle discipline consiste à tirer profit, à des fins de renseignement, d'informations acquises par des capteurs n'ayant pas été spécifiquement développés dans ce but.** C'est par exemple le cas des nacelles de naviga-

12. John Barry, Michael Hastings & Evan Thomas, « *Iraq's Real WMD* », *Newsweek*, 27 mars 2006.
13. *Ibid.*

tion et d'attaque *Sniper XR* équipant les chasseurs-bombardiers *F-15E Strike Eagle*. Elles ont été conçues afin d'assurer le verrouillage d'un missile air-surface sur un objectif précis, après un vol à basse altitude dont elles fournissent les données de navigation. Mais elles disposent également de capacités d'acquisition non négligeables en matière d'imagerie diurne et nocturne infrarouge. Convenablement disséminée, cette imagerie permet en particulier d'avertir les troupes au sol de la présence de fuyards lors d'opérations de recherche d'insurgés. Dans une certaine mesure, les nacelles *Sniper XR* permettent également de détecter la présence d'engins explosifs improvisés placés en bordure de route. Les *F-15E* ou *F-16* sont ainsi mis à contribution dès lors que les moyens de surveillance traditionnels font défaut. Ces chasseurs-bombardiers accompagnent parfois aussi un avion de renseignement d'origine électromagnétique (ROEM) *RC-135 Rivet Joint*, prenant en compte non seulement les communications radio, mais également celles qui émanent des téléphones cellulaires ou satellitaires souvent utilisés pour provoquer à distance l'explosion des IED.

En matière de ROEM, les nouveaux aéronefs qui rejoignent les rangs de l'*US Air Force* devraient contribuer à pérenniser le concept de NTISR.

F-22 *et* F-35 *: un avenir plein de promesses*

Outre-Atlantique, les généraux de l'armée de l'air se réjouissent en effet déjà de l'aptitude des *F/A-22 Raptor* et *F-35 Joint Strike Fighter* (JSF) à jouer un rôle prépondérant en matière de *Non Traditional Intelligence, Surveillance and Reconnaissance*. Ce qui intéresse tout particulièrement le Pentagone, ce sont les capacités des deux avions en matière d'interception passive des signaux radar adverses, à tel point que **le *F/A-22* apparaît comme capable de reprendre à son compte certaines des missions autrefois confiées à l'appareil de reconnaissance stratégique *SR-71 Blackbird* ;** les deux appareils présentent en outre un autre point commun : la furtivité. En conséquence, la pénétration discrète de groupes de *F/A-22 Raptor*, dans un espace aérien inaccessible aux aéronefs chargés de la collecte du renseignement d'origine électromagnétique, est un mode d'action faisant actuellement l'objet d'études poussées.

Photo Ben Bloker, *US Air Force*

Le *F/A-22 Raptor* pérennisera le concept NTISR dans le domaine du renseignement d'origine électromagnétique.

DR

SR-71 Blackbird.

Au sein de l'*Air Force*, le sujet est cependant tabou. Dans les couloirs du *Lexington Institute*, des officiers généraux de l'USAF déclarent que 60 % des capacités du *F/A-22* échappent à toute discussion parce que classifiées. Certaines des expressions

employées pour décrire les capacités du *Raptor* comme du JSF sont toutefois révélatrices : **les systèmes ISR installés sur les deux avions – et en particulier leurs radars AESA (*Active Electronically Scanned Array*) – les transformeraient en véritables « *éponges à informations*[14] ».**

Parallèlement, la puissance informatique embarquée leur permettrait d'absorber et de gérer sans broncher ce déluge de données, situation qu'exprime en ces termes Loren Thompson, le vice-président du *Lexington Institute* : « *Le* Raptor *combine des capacités à intercepter les émissions électromagnétiques sur une large bande de fréquences – depuis les ondes radio jusque dans l'infrarouge – avec la puissance de deux ordinateurs de bord capables de stocker une vaste bibliothèque de signaux enregistrés. Cela permet à l'avion de collecter, traiter et identifier les émissions d'une manière impossible à tout autre appareil*[15] ». Sauf peut-être au *RC-135 Rivet Joint*. Quant à la comparaison avec le *SR-71 Blackbird*, elle est pertinente dans la mesure où c'est justement le schéma général des missions ELINT (*Electronic Intelligence*) effectuées par celui-ci au-dessus du Nord-Vietnam qui a servi de référence pour lancer les travaux relatifs à l'emploi NTISR du *F-22*.

Photo Kevin Camara, *US Air Force*

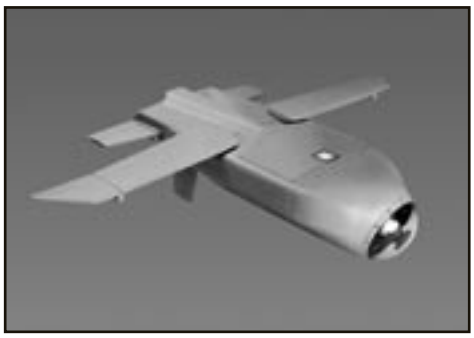
RC-135 Rivet Joint du *398th Air Expeditionary Group*.

Finalement, la seule limite à ce concept semble être le coût de l'engin : 180 devraient être acquis alors que le nombre d'appareils alignés par l'USAF avait été initialement fixé à 750. Dans ces conditions, l'armée de l'air américaine aura-t-elle la volonté de risquer ses précieux *Raptor* pour des missions de pénétration profonde à des fins de renseignement d'origine électromagnétique ? Sans doute d'autant moins que d'autres moyens émergent. **L'irruption de la *Non Traditional Intelligence, Surveillance and Reconnaissance* dans le paysage militaire contribue à rendre plus floue la ligne de démarcation entre les missiles, d'une part, et les drones, d'autre part :** sous la dénomination générique de « missiles persistants », une nouvelle catégorie d'engins hybrides est en passe d'envahir le champ de bataille.

Missiles ou drones ?

Schématiquement, **un « missile persistant » est capable de patienter en volant au-dessus du champ de bataille, afin d'attendre que se dévoile une cible qu'il va repérer par ses propres moyens, puis traiter au moyen d'une attaque suicide.** En la matière, le coup d'envoi a été donné par le programme *Low Cost Autonomous Attack System* (LOCAAS) maintenant arrivé à son terme, non sans avoir fourni son lot d'enseignements : « *Lors d'essais concernant le système de détection de cible du LOCAAS, des vols captifs de son radar laser (LADAR) ont permis de tester la transmission*

14. Michael Fabey, « *Supersonic SIGINT Is Back* », *C4ISRJournal.com*, 17 juin 2005.
15. *Ibid*.



DR

Le LOCAAS (*Low Cost Autonomous Attack System*).

d'imagerie à un centre d'opérations aériennes en mettant à contribution le satellite de communications commercial Globalstar. *Cette potentialité fournit non seulement une capacité de surveillance immédiate, mais également, dans l'autre sens, la possibilité de transmettre à un missile persistant de nouvelles instructions d'attaque, ouvrant ainsi la voie à une gestion dynamique des paramètres de ciblage.* (...) *Les missiles peuvent également transmettre l'imagerie par l'intermédiaire des satellites* Iridium[16] .»

Le LOCAAS aura une descendance. Auparavant dénommé *NetFires* (littéralement « réseau de feux »), le *Non-Line-of-Sight Launch System* (NLOS-LS) sera partie intégrante du *Future Combat System*, ensemble cohérent de blindés de l'*US Army* du futur ; parallèlement, il devrait équiper les *Littoral Combat Ships* (LCS). Le NLOS-LS comprendra deux types de missiles, en particulier le *Loitering Attack Missile* (LAM), engin persistant équipé d'un radar laser capable de survoler le champ de bataille pendant 45 minutes – ou 30 minutes à 70 kilomètres de distance – en attendant de fondre sur un objectif qu'il aura acquis par ses propres moyens.

Pressentant qu'il y a là un marché lucratif, la société *Lockheed Martin* s'est lancée dans le développement de deux missiles persistants, le *Surveilling Miniature Attack Cruise Missile* (SMACM) et le *Top Cover*. Ce dernier n'est pour l'instant qu'un projet. En revanche, le premier est à un stade plus avancé et a d'ores et déjà retenu l'intérêt de l'*Air Force Research Laboratory*, qui envisage de le tester contre des cibles mobiles. Compatible avec l'utilisation à partir des *F-22 Raptor* et *F-35 Joint Strike Fighter*, le SMACM est un missile persistant de 68 kg – des versions ultérieures pourraient atteindre 110 kg – avec une tête militaire d'un peu plus de 8 kg et capable de voler pendant deux heures. Sa principale particularité est d'être équipé d'un « *système de senseurs tri-mode combinant un radar millimétrique à ondes radio, un capteur infrarouge ainsi qu'un détecteur laser semi-actif.* (...) *Cette combinaison offre une capacité tout temps et permet de catégoriser rapidement les cibles grâce à l'emploi de techniques de fusion de données*[17] ».

Il est à souligner que le SMACM n'a pas été conçu *ex nihilo* : sa motorisation miniaturisée est celle du *Loitering Attack Missile*, son radar millimétrique est celui de l'hélicoptère d'attaque *AH-64D Apache Longbow* et son détecteur laser semi-actif est celui du missile antichar *Hellfire* ; à l'instar du LOCAAS, le SMACM est en outre capable de transmettre de l'imagerie *via* les satellites de communication commerciaux.

16. Clarence Robinson, « *Smack'em Flattens Targets* », *SIGNAL Magazine*, mars 2006.
17. *Ibid.*

L'intérêt américain quant à l'utilisation de missiles dans le cadre de la *Non Traditional Intelligence, Surveillance and Reconnaissance* est tel, qu'**il est maintenant envisagé de transformer des engins de croisière contemporains en « drones de circonstance consommables ».** *Raytheon* a ainsi procédé au test d'un « Tomahawk *simulé équipé d'une caméra auquel il a été ordonné d'effectuer des cercles au-dessus d'une zone où une cible était située. Le missile a pris des clichés et a renvoyé l'imagerie à destination d'un réseau centralisé*[18] ». Un tel engin permettrait d'effectuer des missions d'évaluation des dégâts après bombardement (*Bomb Damage Assessment*), voire d'acquérir, dans la profondeur, un renseignement de circonstance sur un objectif fugitif ; il pourrait en outre jouer, *in fine*, le rôle de missile d'attaque en détruisant une cible non durcie par sa seule énergie cinétique, même en l'absence de charge explosive.

Jean-Jacques Cécile
Directeur de recherche au CF2R

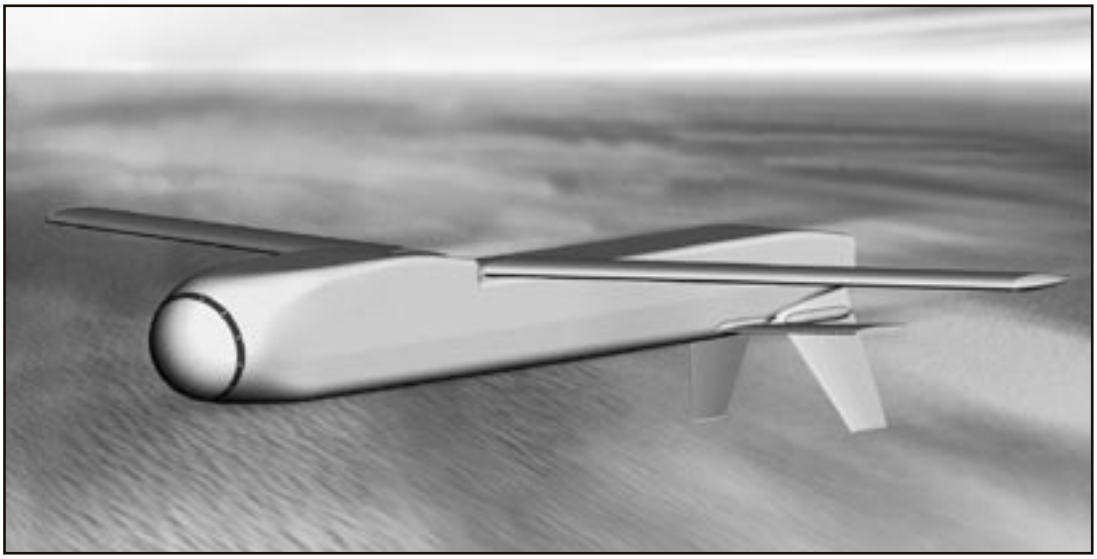


Photo Lockheed Martin

Surveilling Miniature Attack Cruise Missile (SMACM).

18. Grace Jean, « *Missiles May Become Aerial Surveillance Alternative* », *National Defense Magazine*, mai 2006.

Le renseignement *via* les « sources ouvertes » (OSINT) : une nouvelle discipline ?

La multiplication quantitative et qualitative des « sources ouvertes » et des logiciels d'acquisition automatique de l'information accroissent les possibilités de produire des analyses de qualité à partir de données publiques. Cela influe directement sur le métier du renseignement.

Le 5 avril 2006, Amnesty International rendait public un rapport sur les vols de la CIA (*http://web.amnesty.org/library/Index/ENGAMR510512006*). Ce document d'une quarantaine de pages fait la synthèse de tous les éléments à charge sur les avions utilisés par les États-Unis, dans le cadre de la guerre contre le terrorisme, pour transporter certains prisonniers de manière extra-judiciaire. Ce rapport est le fruit d'un travail de collecte, de recoupement et d'analyse de diverses données ouvertes. Ces données corrélées entre elles auront permis d'identifier certains vols affrétés par les autorités américaines. Citons par exemple les permis accordés aux avions civils (*http://www.usaasa.belvoir.army.mil/CALP/CALPDec05.htm*) et les données des vols internationaux (notamment : *http://www.airfleets.net/flightlog/?file=recherche*).

Nous ne préjugeons pas ici de la qualité des travaux d'Amnesty International. Mais force est de constater qu'**un travail réalisé à partir de sources ouvertes aura réussi, d'une part, à produire des informations que l'on pourrait aisément croire non ouvertes, d'autre part, à créer un événement médiatique d'ampleur internationale.**

L'accroissement des possibilités de produire de l'information de qualité à partir des sources ouvertes influe directement sur le métier d'homme de renseignement. Diverses évolutions récentes viennent le confirmer. Par exemple, la CIA annonçait en novembre 2005 la création d'un *Open Source Center* (*http://www.cia.gov/cia/public_affairs/press_release/2005/pr11082005.html*). Ce centre reprend et augmente les capacités du FBIS (*Foreign Broadcast Information Service*) qui collecte et traduit les informations diffusées par les radios et journaux du monde entier[19].

Les inestimables ressources des « sources ouvertes »

Pour tâcher d'en comprendre l'intérêt, il nous faut tout d'abord essayer de définir ce que l'on appelle « sources ouvertes ». Nous choisirons ici d'en prendre une définition restreinte, qui se rapprochera de la définition de l'information documentaire. **Nous appelons « sources ouvertes » les sources d'information accessibles à tous au moyen de médias spécifiques.** Il est important de noter que l'accès à ces sources peut être payant (bases de données commerciales) ou non.

19. Le FBIS est en partie armé par les Britanniques au travers du *BBC Monitoring Service.*

Nous excluons par contre toute information ou donnée récupérée, même ouvertement, dans le cadre d'une action qui ne serait pas accessible à tout le monde. Ainsi un entretien, certes réalisé « le plus ouvertement du monde » – par exemple auprès d'un expert reconnu – ne sera pas ici considéré comme provenant d'une source ouverte.

Cette définition n'est pas unanimement partagée ; l'un des chantres de l'information ouverte, l'Américain Robert Steele, considère qu'un entretien réalisé de façon « transparente » – c'est-à-dire sans cacher son identité et en annonçant ses intentions – relève aussi de l'information ouverte. Fort de cette conception, il a récemment défié les services de renseignement américains en pariant qu'il obtiendrait de meilleurs résultats qu'eux, en n'utilisant que des sources ouvertes et en ne dépensant que 10 000 dollars par question posée (voir *http://tinyurl.com/juaeh*).

Notre définition, plus restrictive, inclut cependant tous les médias internationaux (presse, radio, télévision), la production mondiale de livres et tout ce qui est publié et accessible sur Internet. La montée en puissance et en ubiquité d'Internet a obligé tous les fournisseurs professionnels d'information à migrer vers le *web*. On ne trouve presque plus de bases de données commerciales dont l'accès n'est pas possible *via* la Toile.

DR

Des millions de personnes s'inscrivent sur des sites ouverts, ce qui fait exploser la possibilité de trouver des informations sur Internet.

De même, la facilité de publication de l'information sur le *web* est maintenant triviale, au point d'avoir créé son propre vocabulaire, tel les *blogs*. Toute personne ou organisation peut publier sur la Toile. Et le *web* n'est pas le seul média que recouvre Internet : les forums, les listes de discussions par courrier électronique, les *podcasts* et autres diffusions multimédia font exploser la possibilité de trouver de l'information sur Internet.

Pour la grande majorité, cette information correspond bien à notre définition de l'information ouverte, commerciale ou non. Internet est donc un moyen unique d'accès à une multitude de sources d'information, indépendantes et hétérogènes. Indépendantes, car deux informations ou données issues d'Internet n'ont pas de raison *a priori* de provenir de la même origine. Hétérogène, car l'on y trouve toutes les qualités : de l'information mise à disposition par une personne privée, des informations institutionnelles de grandes entreprises, des informations à valeur légale (comme les registres du commerce français, britannique), etc.

L'intérêt des sources ouvertes provient d'ailleurs de cet aspect multidimensionnel : la possibilité de recouper des informations hétérogènes. Par exemple, si nous nous intéressons à une entreprise aéronautique française, nous avons la possibilité :

DR

L'acquisition de données et d'informations ouvertes ne pose plus aujourd'hui de problèmes techniques.

- ☞ d'obtenir ses documents déposés aux greffes et donc d'identifier les actionnaires et les gérants (*www.infogreffe.fr*),
- ☞ d'identifier de fait les entreprises dans lesquelles ces gérants ont d'autres participations (*www.societe.com*),
- ☞ d'obtenir les CV de certains de ces gérants (base de biographies de *www.lesechos.fr* et recherche sur le *web* avec Google),
- ☞ d'identifier des employés de l'entreprise avec des sites d'anciens collègues, comme *copainsdavant.linternaute.com*,
- ☞ d'étudier la R&D de l'entreprise au travers de ses dépôts de brevets (*fr.espacenet.com*),
- ☞ etc.

Les applications en matière de renseignement

Mais si l'on comprend l'intérêt d'une telle démarche, par exemple pour une entreprise civile qui voudrait mieux connaître un partenaire ou un concurrent, quel peut en être l'intérêt pour un homme de renseignement, en particulier dans un cadre militaire ? La réponse vient d'elle-même lorsque l'on constate **l'imbrication toujours plus étroite des enjeux civils et militaires sur les théâtres d'opération.** En matière de renseignement, il ne suffit plus de compter les divisions et d'identifier les insignes des unités. Il faut identifier et cribler chacun des acteurs que nos forces vont rencontrer. Or ces acteurs sont aussi des entreprises, des ONG ou des personnes privées, tous susceptibles d'avoir laissé des traces de leurs actions, de leur histoire, dans une des innombrables sources de données électroniques.

Obtenir ces données ne permettra peut-être pas de répondre à l'ensemble des questions soulevées au sujet de tel ou tel acteur. Par contre, **les éléments obtenus permettront, au minimum, de mieux cibler les autres actions non ouvertes jugées nécessaires.** Ainsi, les campagnes de privatisation des entreprises du Kosovo font entrer dans cette province des nouveaux acteurs industriels, tous justifiables d'un criblage initial au moyen de ces sources ouvertes.

De façon générale, **épuiser les possibilités des sources ouvertes avant de lancer sur une cible des moyens de collecte « non ouverts » devrait être un réflexe systématique.** Au pire, les données recueillies permettront de mieux cibler les actions futures ; au mieux, les données s'avéreront suffisantes pour permettre de décider.

L'acquisition de données et d'informations ouvertes ne pose plus aujourd'hui de problèmes techniques : les outils développés ces dix dernières années permettent de maîtriser la phase « collecte » du cycle du renseignement. Moteurs de recherche, agrégateurs de bases de données, indexeurs locaux, métamoteurs, etc., tous ces outils servant à la recherche automatisée fonctionnent parfaitement.

Les autres phases du cycle, adapté au contexte des sources ouvertes, nécessitent aussi chacune des outils particuliers. **Les phases d'orientation, de diffusion des travaux et éventuellement de travail collaboratif entre analystes, bénéficient toutes également des développements effectués, au cours de ces dernières années, pour les grandes entreprises** et leurs Intranets.

Certains de ces outils – par exemple les produits de la filiale de Thalès, *Arisem*, ou encore le produit *Tropes* de la société Acetic – prennent le parti d'une intelligence embarquée, qui permet l'analyse sémantique des textes. L'utilisateur se base alors sur ces logiciels pour accélérer sa prise en compte des informations. D'autres font, au contraire, le pari de laisser toute l'intelligence à l'utilisateur. Ainsi des logiciels, issus du monde de l'analyse criminelle, comme *Analyst's Notebook* ou *Visual Analystics*, vont permettre de représenter et de décortiquer les relations existant entre des personnes, des entreprises et des événements préalablement identifiés dans un corpus. Cela signifie que c'est à l'utilisateur de remplir cette base de connaissance : l'outil n'est là que pour l'aider à traiter une masse très volumineuse d'informations, lui permettant en particulier de détecter dans cette « mine » des régularités ou des organisations qui n'auraient pas été visibles à l'œil nu.

Toutefois, il manque encore, pour un traitement efficace de l'ensemble des informations issues des sources ouvertes, des outils capables d'assurer la structuration automatique des informations et leur homogénéisation. Des logiciels intéressants sont actuellement à l'étude : transcription automatique des conversations orales, traduction automatique en de nombreuses langues, identification automatique des noms propres et des liens existants entre personnes – des produits de structuration de textes, comme ceux de la société française Temis ou de l'américaine SRA (*Netowl*) sont particulièrement intéressants –, identification et classification automatiques d'images, etc.

Bien évidemment, ces outils, s'ils voient le jour, ne serviront pas qu'à traiter des sources ouvertes. Ils devraient permettre de rendre toutes les sources d'information inter-opérables et « inter-analysables ». Le Graal de l'analyste, en quelque sorte.

Jean-François Loewenthal
Consultant associé d'*Intelligences* SARL, chercheur associé au CF2R

La montée en puissance de l'intelligence économique

L'accroissement de la concurrence internationale et des rivalités géoéconomiques entre États place les acteurs économiques dans des situations de plus en plus instables. Cette évolution les conduit à faire appel à des pratiques issues du renseignement pour se développer ou simplement survivre dans ce nouveau contexte.

La nouvelle situation internationale consécutive à la désagrégation de l'Union soviétique n'a pas fait disparaître les sources de tensions entre États. **Le nouveau contexte confère à l'économie une place privilégiée comme domaine d'affrontement entre les nations.** Les rivalités pour la conquête des marchés sont ainsi venues s'ajouter aux traditionnelles rivalités géopolitiques. La guerre économique à laquelle nous assistons se caractérise par un trait spécifique : elle oppose simultanément les entreprises entre elles et les États entre eux, et ces deux niveaux d'affrontement influent l'un sur l'autre. En raison de l'accroissement de l'intensité concurrentielle, les entreprises prennent conscience que les lois du marché et de la libre concurrence sont de moins en moins respectées. Il leur faut donc agir différemment, d'où le recours à de nouvelles pratiques d'information et d'influence, issues du monde du renseignement et connues sous le nom d'intelligence économique. **En appui de leurs entreprises, les États adaptent à leur tour leur dispositif d'« intelligence » à la compétition économique et culturelle.**

Les origines de l'intelligence économique

À partir de la fin des années 1950, les grandes entreprises américaines créèrent des départements de marketing, influencées par les méthodes de raisonnement tactique militaires issues de la seconde guerre mondiale. **Un des premiers exemples de transfert des savoirs du domaine militaire vers le domaine commercial fut le « marketing de combat », une pratique du marketing qui s'inspirait des principes d'affrontement, de motivation des troupes, d'infiltration du territoire de l'adversaire,** en montrant l'analogie qui pouvait être faite entre un environnement concurrentiel et un champ de bataille. Le marketing fut ainsi défini, dès l'origine, comme l'ensemble des activités couvrant l'appréhension la plus scientifique possible du marché et la définition des actions nécessaires à sa conquête.

Dès lors, les entreprises prirent progressivement l'habitude de réaliser des études de marché afin de suivre l'évolution des attentes des consommateurs, le positionnement de leurs produits, les innovations techniques applicables à leurs activités et les actions des concurrents.

Mais les entreprises furent prises au dépourvu lorsqu'un événement important se produisait entre deux études de marché. Elles ressentirent alors le besoin de suivre en continu les concurrents et l'évolution de la consommation. Ainsi se développèrent les activités de veille concurrentielle et commerciale. Parallèlement, les scientifiques apprirent à suivre l'avancement des travaux de leurs confrères et néanmoins concur-

rents. Ainsi naquirent les pratiques de veille technologique, au départ, centrées sur les publications scientifiques et techniques et les brevets.

Puis, au début des années 1960, en raison du contexte d'affrontement concurrentiel croissant entre grandes entreprises américaines sur leur marché intérieur, est apparue l'intelligence économique – désignée, outre-Atlantique, sous les vocables de *Business, Competitive* ou *Corporate Intelligence* – directement issue des pratiques de renseignement développées à l'occasion de la Guerre froide. Elle n'a cessé de se développer, notamment dans les années 1970 et 1980, au sein d'entreprises telles que *Motorola* et *IBM*, pour s'imposer au début des années 1990. Depuis, elle est largement pratiquée et enseignée. L'intelligence économique n'est donc pas fondamentalement une nouvelle discipline. Elle a toujours existé. Dès le début des années 1960, le service d'information de *General Motors* disposait d'un budget équivalent à celui des services secrets français. Au Japon, le *Worldwide Information Network* de *Mitsui* est aujourd'hui un réseau centralisé aussi important, par sa taille et ses effectifs, que celui de la CIA. Mais cette discipline est restée longtemps cantonnée au sein de quelques grands groupes. Elle se généralise depuis quinze ans en raison de l'accroissement de l'intensité concurrentielle.

L'intelligence concurrentielle, nouvelle arme de la compétition économique

Si les marchés ont toujours été complexes, ils le sont davantage aujourd'hui en raison de la mondialisation de l'économie et de l'entrelacement des données politiques, économiques et techniques. Le nombre de facteurs extérieurs à l'activité des entreprises qui concernent leur devenir ne cesse de croître. Le développement de l'intelligence économique n'est donc pas un effet de mode. **Les entreprises constatent que leurs moyens traditionnels d'action sur l'environnement sont devenus inopérants. Il leur faut donc recourir à de nouveaux outils de prévision et à de nouveaux modes d'action.**

Dans un environnement devenu hyper-concurrentiel, les entreprises doivent en permanence anticiper sur les évolutions, d'où le rôle central de l'information. Leur première tâche consiste donc à surveiller en permanence l'environnement pour y déceler toutes les modifications susceptibles d'affecter leur activité, pour connaître rapidement toutes les applications nouvelles que peut offrir la science, pour ne pas se laisser déborder par leurs concurrents et pour préserver leurs avantages.

Mais la turbulence des marchés s'avère parfois tellement prononcée, que toute prévision fiable devient impossible. Seule une autre modalité d'action demeure : modifier l'environnement. Dans ce cas, la principale finalité d'une stratégie n'est pas l'adaptation ni l'anticipation, mais la construction d'un environnement favorable, en imposant ses règles du jeu aux autres acteurs.

Ainsi, dans le monde entier, un nombre croissant d'entreprises mettent en œuvre des méthodes inspirées de l'art de la guerre et des réflexions des stratèges militaires. Dans ce contexte de haute compétitivité, l'objectif prioritaire de certaines firmes n'est plus de satisfaire les besoins du marché, mais de détruire psychologiquement les

offres et les propositions des entreprises concurrentes dans l'esprit des clients actuels et futurs. Cette démarche peut aller jusqu'à s'en prendre physiquement aux centres de décision, de recherche, de production ou de distribution, voire aux transports, de la concurrence. **Cela conduit les acteurs économiques à faire appel à des savoirs et à des pratiques issus des métiers traditionnels du renseignement,** même si la filiation avec ceux-ci est rarement reconnue.

L'intelligence économique, adaptation des pratiques du renseignement à l'entreprise

Lorsque l'on analyse ses finalités et ses méthodes, **l'intelligence économique, avec ses spécificités propres, apparaît comme la fille légitime du renseignement, car ses fonctions sont la transposition des métiers traditionnels du renseignement dans la sphère économique, publique et privée.**

- La veille dite passive (ou surveillance des environnements) correspond aux tâches de documentation et de suivi de la situation internationale effectuées quotidiennement par les services.

- La veille dite active (ou investigation), indispensable lorsque l'entreprise veut en savoir plus sur un sujet précis, s'identifie directement à la recherche de renseignement sur le terrain, en complément ou en vérification d'hypothèses identifiées ailleurs. Le renseignement sur les marchés (consommateurs, caractéristiques), et sur son environnement, correspond au travail effectué par un service de recherche. Le renseignement sur les partenaires (fournisseurs, sous-traitants, alliés) et sur les concurrents s'apparente au contre-espionnage (les surveiller, connaître leurs intentions, leurs moyens, leurs actions).

- L'action, lorsque l'investigation confirme une piste (menace ou atout), qui amène l'entreprise à attaquer ou à contre-attaquer (OPA, *lobbying*, utilisation offensive de l'information, campagne de presse, déstabilisation d'un concurrent) , correspond en tous points aux attributions d'une direction des opérations et répond aux mêmes conditions de risque et aux mêmes critères de confidentialité.

- Enfin, la sûreté est présente à tous les stades de ces démarches.

Les seuls éléments nouveaux qui pourraient laisser penser que l'intelligence économique est distincte du renseignement sont l'utilisation de plus en plus systématique de sources ouvertes et la réduction au strict minimum des cloisonnements. Or l'utilisation de sources ouvertes se généralise elle-même dans les services de renseignement. Elle rend inévitable la disparition d'un certain nombre de procédures de sécurité héritées de la Guerre froide : l'interaction en temps réel entre les acteurs est un impératif auquel les services sont soumis au même titre que les entreprises. **La règle d'efficacité maximale en matière de protection du secret est désormais l'exploitation rapide de l'information et non sa classification :** tout renseignement n'étant pas exploité rapidement est une occasion d'action perdue.

À l'avenir, les métiers de l'intelligence économique vont se rapprocher encore de ceux du renseignement. Différentes fonctions très spécialisées – dont certaines existent déjà – vont rapidement émerger :

- les spécialistes de la documentation au sens large (bibliométrie, infométrie, archivage pour constituer la mémoire de l'entreprise),
- les spécialistes de la recherche technique et de l'interrogation des bases de données (*datamining*), qui opéreront en premier lieu sur Internet,
- les spécialistes de la sécurité informatique et de la sûreté de l'entreprise,
- les spécialistes des sources humaines (conscientes ou inconscientes), véritables officiers traitants, qui seront chargés de recueillir des informations – y compris sous « couverture » – sur les salons, au cours d'entretiens, dans les colloques et conférences, dans les lieux publics et les transports,
- les analystes et exploitants dans tous les domaines concernant l'activité de l'entreprise,
- les animateurs de la fonction intelligence (réseau interne à l'entreprise, échanges d'informations avec d'autres sociétés et l'administration),
- les *lobbyistes*, chargés des actions d'influence,
- les spécialistes de la guerre de l'information et de la communication offensive,
- les personnes chargées des opérations inavouables, activités dont on doit craindre le développement.

On retrouve dans cette énumération les grands métiers qui sont ceux des services de renseignement : recherche technique et humaine, exploitation et analyse, influence et actions secrètes, sécurité et contre-espionnage.

DR

Le recours à l'intelligence économique résulte donc du besoin des entreprises de se doter d'un outil adapté au nouveau contexte concurrentiel. L'entrée du renseignement dans le monde économique ne date pas d'hier, mais son usage ne s'est généralisé que depuis le début des années 1990. Comme cette évolution s'est exercée de pair avec la révolution des techniques de l'information, beaucoup d'acteurs économiques ont pensé découvrir une nouvelle discipline. Pourtant, même si elle s'enrichit d'un croisement avec les approches scientifiques et rigoureuses du *marketing* et du conseil, **l'intelligence économique n'est pas une création liée à Internet. Elle est bien une adaptation du renseignement à la problématique des activités économiques concurrentielles,** à l'ère de l'information, avec des impératifs éthiques et légaux.

Éric Denécé
Directeur du CF2R

Glossaire

CICR	Comité international de la Croix-Rouge
COMINT	*COMmunications INTelligence*
DIA	*Defense Intelligence Agency* (États-Unis)
ECHELON	Réseau mondial d'interception des communications réunissant, sous la direction des États-Unis, les services d'écoutes américain, britannique, canadien, australien et néo-zélandais.
ELINT	*ELectronic INTelligence*
GSPC	Groupe salafiste pour la prédication et le combat (Algérie)
HALE	*High Altitude, Long Endurance*
HF	Haute fréquence
IED	*Improvised Explosive Devices*
IMINT	*IMagery INTelligence*
IP	*Internet Protocol*
LOCAAS	*Low Cost Autonomous Attack System*
NTISR	*Non Traditional Intelligence, Surveillance and Reconnaissance*
ONG	Organisation non gouvernementale
OODA	Observation, orientation, décision, action
OPA	Offre publique d'achat
OSINT	*Open Sources INTelligence*
ROEM	Renseignement d'origine électromagnétique
SIGINT	*SIGnal INTelligence*
SMACM	*Surveilling Miniature Attack Cruise Missile*
UAS	*Unmanned Aerial Systems*
UHF	Ultrahaute fréquence.

Présentation du CF2R

Fondé en 2000, le Centre français de recherche sur le renseignement (CF2R) est un *think tank* indépendant, régi par loi de 1901, spécialisé dans l'étude de l'ensemble des domaines historiques, techniques et politiques du renseignement.

Le CF2R est structuré en plusieurs commissions spécialisées :

- histoire du renseignement,
- fonctionnement du renseignement,
- renseignement technique et nouvelles techniques,
- opérations spéciales,
- actions psychologiques et désinformation,
- privatisation des activités de défense et mercenariat,
- intelligence économique et influence,
- drogue, criminalité et mafias,
- terrorisme et islamisme.

Autour de ces thèmes, le CF2R développe :

- des activités de réflexion et de recherche, réservées à ses seuls membres actifs (dîners-débats, groupes de travail),
- des actions de sensibilisation à l'intention de la presse, des parlementaires, des universités et des décideurs économiques,
- des publications, pour l'information du grand public,
- des enseignements (à l'université et dans les écoles militaires), notamment un diplôme de 3e cycle « Étude du renseignement » à l'université de Bordeaux IV,
- des études et des formations, à la demande de clients divers.

En parallèle, le CF2R réalise des études à caractère régional afin de suivre un certain nombre d'évolutions géopolitiques.

Le CF2R dispose d'une trentaine de chercheurs associés. Tous sont experts en leur domaine et disposent à la fois de compétences académiques reconnues et d'une véritable expérience de terrain. Ils interviennent à la demande, en fonction de leurs spécialités, de leur disponibilité et des projets considérés.

Les publications du CF2R comprennent :

- des *Notes d'actualité* rédigées régulièrement par ses experts et diffusées sur son site Internet (*www.cf2r.org*),
- la revue quadrimestrielle *Renseignement et opérations spéciales* (180 pages) (éditions L'Harmattan),

- le bulletin électronique hebdomadaire *Renseignor* (Renseignement ouvert par l'écoute des programmes radiophoniques étrangers en langue française),
- la collection *Culture du renseignement* (éditions L'Harmattan),
- ainsi que divers ouvrages collectifs (éditions Ellipses).

Enfin le CF2R développe des partenariats avec des centres de recherches français et étrangers, ainsi qu'avec le projet *Spyland* (parc d'attractions consacré au monde du renseignement).

Pour plus d'information, contacter :

CF2R
17 square Édouard VII
75009 Paris
Tél. : 33 1 53 43 92 44
www.cf2r.org

Les Cahiers du CESA
Centre d'études stratégiques aérospatiales
1, place Joffre
B.P. 43
00445 ARMÉES

www.cesa.air.defense.gouv.fr