DIPLOMATIE GD

DIPLOMATIE

AFFAIRES STRATÉGIQUES ET RELATIONS INTERNATIONALES

AVRIL - MAI 2017

LES GRANDS DOSSIERS N°38

En partenariat avec le Centre français de recherche sur le renseignement (CF2R)

CONTRE-INGÉRENCE
IMAGERIE & ÉCOUTES
LUTTE ANTITERRORISTE
CYBER-RENSEIGNEMENT
RENSEIGNEMENT MILITAIRE

GÉOPOLITIQUE DU RENSEIGNEMENT

BEL : 12 €, CDN : 17.99 $, CH : 20 FS, D: 12 €, DOM : 11.50 €, ESP : 11.30 €, GR : 11.30 €,
IT : 11.30 €, LUX : 12 €, MAR : 86 MAD, TOM : 1300 CFP, PORT. CONT : 11.30 €

Retrouvez-nous sur Areion24.news

M 02271 - 38 - F: 10,95 € - RD

Retrouvez sur le web
les analyses et entretiens
des meilleurs experts sur
l'actualité internationale
et stratégique mondiale.

http://www.areion24.news/

Directeur de la rédaction et rédacteur en chef
Alexis Bautzmann *(bautzmann@areion.fr)*

Rédacteur chargé de la coordination et rédacteur cartographe
Thomas Delage *(delage@areion.fr)*

Secrétaire de rédaction et rédactrice graphiste
Céline Lamartinie *(lamartinie@areion.fr)*

Secrétaire de rédaction (editing)
Nathalie Vergeron *(vergeron@areion.fr)*

Ont collaboré à ce numéro
Gérald Arboit, Thierry Berthier, Alain Charret, Alain Chouet, François-Yves Damon, Claude Delesse, Éric Denécé, David Elkaïm, Brigitte Henri, Wolfgang Krieger, Alain Lamballe, Pascal Legai, Patrick Leroy, Michel Masson, Éric Melchiori, Denis Moura, Gaël Pilorget, Guy Rapaille, Jean Rastine, Claude Revel, Alain Rodier, Julien Tourreille

Partenariats scientifiques
Centre d'Analyse et de Prévision des Risques Internationaux (CAPRI) *(contact@capri-fr.org)*
Centre français de recherche sur le renseignement (CF2R)

Publicité
Jean-Michel Rollant *(rollant@areion.fr)*
Tél. : 06 14 67 38 60 • Fax : 08 11 62 29 31

Abonnements & ventes au numéro
Magazine *Diplomatie* • Service Abonnements
c/o Back-Office Press • 12350 Privezac (France)
Tél. : 05 65 81 54 86 • Fax : 08 11 62 29 31
(contact@bopress.fr)

Site internet et boutique en ligne
www.areion24.news

Diffusion en kiosque
Presstalis • Tél. : 01 49 28 70 00

Diffusion en librairie
Pollen Diffusion • Tél. : 01 43 58 74 11

Placement et réassorts
Destination Média • Tél. : 01 56 82 12 00

Dans quel kiosque trouver *Diplomatie* ?
www.trouverlapresse.com

Impression
AUBIN Imprimeur • 86240 Ligugé (France)

Commission paritaire : 0718 K 90951
ISSN : 2115-256X
Dépôt légal : avril 2017

Directeur de la publication
Alexis Bautzmann

Photo de couverture
(© Gangis khan/Shutterstock)

Pour joindre la rédaction de *Diplomatie*
Areion Group • Magazine *Diplomatie*
128 rue La Boétie • 75008 Paris (France)
Tél. : 01 75 43 52 70 • Fax : 08 11 62 29 31
E-mail : diplomatie@areion.fr

Les Grands Dossiers de Diplomatie n° 38
Bimestriel, avril – mai 2017
Prix unitaire en France métropolitaine : 10,95 €

Les Grands Dossiers de Diplomatie assument la responsabilité du choix des illustrations et de leurs légendes, de même que celui des intitulés et sous-titres des articles ci-dedans publiés. Les opinions exprimées dans les articles ou entretiens n'engagent que leurs auteurs.

Les Grands Dossiers de Diplomatie
sont édités par Areion Group
SAS au capital de 404 352 euros
100 rue Victor Baltard • 13854 Aix-en-Provence (France)

Areion group

éditorial

par Gérald Arboit*

Le récent attentat de Londres, après les soupçons d'ingérence étrangère dans le processus entourant l'élection de Donald Trump à la présidence des États-Unis et les nouvelles publications de Wikileaks sur les cybertechniques de la CIA, jettent une lumière crue sur les pratiques du monde du renseignement. S'ajoutent un climat de guerre froide, engendrée par l'intervention de la Russie en Syrie, et l'apport des nouvelles technologies au service de l'intelligence économique, du renseignement criminel ou du *Geospatial Intelligence* (GEOINT). Terrorisme de nouvelle génération, espionnage, propagande, adaptation des services de renseignement aux innovations de la société de l'information sont autant de raisons pour s'interroger sur leurs réalités géopolitiques.

Le magazine *Diplomatie* et le Centre français de recherche sur le renseignement (CF2R) unissent leurs forces pour réaliser un numéro consacré à ce sujet très peu traité en France. Le CF2R est un *think tank* indépendant, régi par la loi de 1901, spécialisé sur l'étude du renseignement et de la sécurité internationale. Il a pour objectifs le développement de la recherche académique et des publications consacrées à ces questions, mais également d'apporter une expertise afin de démystifier le renseignement auprès du grand public et de le lui expliquer.

À travers ce numéro, les chercheurs du CF2R comme les auteurs de leur réseau entendent offrir un panorama le plus exhaustif possible de la réalité du renseignement au niveau mondial. Ils entendent donner au lecteur, au terme de leur démarche prospective, une meilleure compréhension de l'actualité internationale. Indubitablement, l'appréhension du renseignement y gagnera dans ces temps troublés !

*Gérald Arboit est directeur de recherche au CF2R, Paris.

Photo ci-dessous : Barack Obama à la cérémonie d'investiture de Donald Trump, le 20 janvier 2017. Début mars 2017, le président Donald Trump accusait son prédécesseur, Barack Obama, de l'avoir fait mettre sur écoute avant et après son élection. De son côté, l'ancien président démocrate a accusé Moscou d'ingérence dans l'élection présidentielle américaine, au bénéfice du candidat républicain. (© Xinhua/Yin Gobu)

SOMMAIRE

LES GRANDS DOSSIERS DE DIPLOMATIE N° 38

GÉOPOLITIQUE DU RENSEIGNEMENT

GÉOPOLITIQUE

DU RENSEIGNEMENT

Histoire et enjeux

Photo ci-contre : Image tirée du film *Quantum of Solace*, où l'acteur Daniel Craig incarne James Bond, l'un des agents de renseignement fictifs les plus populaires au monde. Si la fiction est parfois loin de la réalité, l'espionnage demeure une activité stratégique, et probablement plus ancienne que la guerre elle-même. Le général chinois Sun Tzu (VI^e^ siècle avant J.-C.), auteur de *L'Art de la guerre*, estimait qu'« une armée sans agents secrets est exactement comme un homme sans yeux ni oreilles ». (© EON Productions/Columbia Pictures/Metro-Goldwyn-Mayer)

analyse

Par **Gérald Arboit**, directeur de recherche au Centre français de recherche sur le renseignement (CF2R).

Géopolitique historique du renseignement

Interroger l'histoire du renseignement par l'angle géopolitique impose de laisser de côté l'appréhension étatique pour une démarche comparatiste plus internationaliste, qui permet de définir des archétypes du renseignement aussi bien structurels – de la naissance des services secrets modernes avec la Première Guerre mondiale aux avancées technologiques de la guerre froide –, que culturels – diplomatique ou policier – et d'expliquer l'émergence de la transdisciplinarité contemporaine.

Photo ci-dessus :
Selon Sun Tzu, le célèbre général chinois auteur du plus ancien ouvrage de stratégie militaire connu, *L'Art de la guerre*, l'usage des espions relevait de l'obligation : « Un prince avisé et un brillant capitaine sortent toujours victorieux de leurs campagnes et se couvrent d'une gloire qui éclipse leurs rivaux grâce à leur capacité de prévision. Or la prévision ne vient ni des esprits ni des dieux ; elle n'est pas tirée de l'analogie avec le passé pas plus qu'elle n'est le fruit des conjectures. Elle provient uniquement des renseignements obtenus auprès de ceux qui connaissent la situation de l'adversaire. » (© Shutterstock/toiletroom)

Le renseignement consiste en la recherche et l'analyse d'une information particulière et nécessaire à un décideur. Nul besoin, donc, de la préexistence d'un État pour y recourir. Il suffit d'être dans la position de décider une action, au niveau tant politique que militaire ou économique.
Non seulement dissiper le « brouillard de la guerre » (1) n'a jamais été un élément décisif pour une apparition du renseignement, mais qui plus est, ses dynamiques d'intérêt militaire n'ont jamais dépassé le proche environnement. En effet, à toutes les époques, les combats ne se sont jamais déroulés loin des principales bases des combattants. De l'époque romaine à la Première Guerre mondiale, les besoins d'éclairage suffisaient à la cavalerie légère pour reconnaitre les environs de la bataille. Même sous Napoléon, les « parties secrètes », ces Deuxièmes Bureaux (2) avant l'heure, étaient armés à partir d'agents ayant une connaissance de l'espace de bataille : ce furent les Piémontais Ange Pico et Francesco Tolli en Italie du Nord, le Badois Charles Louis Schulmeister en Allemagne et en Autriche, ou encore le Polonais Boguszewski en Russie.

Première Guerre mondiale : la naissance des services modernes

La « Grande Guerre », en raison à la fois de l'européanisation du conflit et de l'immobilisation du front, contribua certes à

l'instauration de services permanents, mais surtout à une adaptation technologique du renseignement. C'est en effet à partir de cette époque que l'on peut parler d'*Imagery Intelligence*, ou renseignement d'origine image (ROIM), et de *Communications Intelligence*, généralisation des écoutes des communications transitant par les ondes. Avec le développement des interceptions des ondes radar (*Electronic Intelligence*) dans les années 1950, se développa plus génériquement la *Signals Intelligence*, ou renseignement d'origine électromagnétique (ROEM). Au début des années 2000, en raison de l'utilisation croissante de moyens satellitaires, le ROIM fut pareillement reclassé comme une partie de la *Geospatial Intelligence* (GEOINT).

Qu'il s'agisse des institutions ou des moyens, une lecture géopolitique est possible à partir de ce XIX[e] finissant que marqua la Première Guerre mondiale. L'apport des histoires nationales du renseignement montre bien que l'Europe mit en place à cette période des services permanents. Après 1870, la concurrence entre la France, la Grande-Bretagne, la Russie et l'Allemagne vit ces quatre pays se doter précocement d'un outil de renseignement, armé par des militaires, pour des raisons géopolitiques. Pareillement, les pays de l'Europe balkanique, en raison de l'écheveau de liens diplomatiques et dynastiques dans lesquels le congrès des Nations de Berlin de 1878 les avait enserrés, utilisèrent le renseignement comme un moyen de faire bouger les lignes. Il n'y eut que les États-Unis pour considérer ce moyen de recueillir une information spécialisée comme indigne « de gentlemen » ; ils restèrent en dehors du club des nations pourvues d'un service de renseignement jusqu'au début de la guerre froide. Ils induisirent alors une rupture géopolitique, dans le sens où la *Central Intelligence Agency* fut conçue comme un outil d'actions idéologiques et politiques, alors que les services européens en étaient encore à une conception seulement militaro-politique, y compris ceux d'Union soviétique. Évidemment, la nature planétaire de la guerre froide induisit que les pays du Proche-Orient, d'Asie, puis d'Afrique qui accédèrent à leur indépendance se dotassent de services de renseignement, formés par leurs anciens pouvoirs métropolitains, ou par l'un des deux grands acteurs de cette période, les États-Unis ou l'Union soviétique.

« Il n'y eut que les États-Unis pour considérer ce moyen de recueillir une information spécialisée comme indigne « de gentlemen » ; ils restèrent en dehors du club des nations pourvues d'un service de renseignement jusqu'au début de la guerre froide. »

La guerre froide : des avancées technologiques stratégiques

La rupture de la guerre froide fut plus marquante que celle de la Première Guerre mondiale, en raison de la course technologique à laquelle se livrèrent les deux protagonistes principaux de cette période, particulièrement dans les domaines du ROEM et du ROIM.

Pour le ROEM, la conclusion du *United Kingdom-United States Communications Intelligence Agreement* (UKUSA), le 5 mars 1946, institua une gradation entre alliés. Ainsi apparurent pour la première fois deux catégories de partenaires, en plus des signataires qu'étaient le London Signal Intelligence Board et le State-Navy-Army Communication Intelligence Board : le Canada, l'Australie et la Nouvelle-Zélande furent considérés comme des « parties secondaires », tandis que ne furent que des « parties tierces » les services d'autres États (3). Et cela, dès la guerre froide, et se poursuivant au-delà jusqu'à nos jours. Cette différence entre partenaires allait à l'encontre d'un usage établi entre la France et la Grande-Bretagne, celui du « tiers parti », qui veut qu'un service recevant un renseignement d'un autre ne peut le retransmettre à un troisième sans l'autorisation de l'émetteur. Là, les États-Unis s'arrogeaient le droit de choisir, au-delà du Royaume-Uni, quel service pourrait accéder temporairement à certains renseignements américains en fonction des facilités électromagnétiques qu'il leur offrirait. Un certain rééquilibrage intervint avec la généralisation des satellites ELINT. Aujourd'hui, 45 sont encore actifs : les États-Unis en disposent de la moitié, la Chine en entretient quinze, la France et la Russie quatre chacun.

La rupture géopolitique induite en matière de ROIM fut encore plus éclatante. Après l'hégémonie spatiale de l'Union soviétique et des États-Unis, au début des années 1960, le club satellitaire s'ouvrit d'abord à la France, puis au Royaume-Uni dans les quinze années suivantes. Dans les années 2000, la baisse des couts technologiques et la multiplication des lanceurs a permis d'élargir le nombre de pays accédant à des moyens satellitaires de ROIM. Aux quatre nations disposant de satellites ELINT, qui s'arrogent 60 % des ressources, il convient d'ajouter la Chine ou l'Inde, au niveau mondial, ainsi que l'Afrique du Sud, l'Allemagne, le Chili, l'Inde, Israël, le Japon, Taïwan et la Turquie, au niveau régional. Évidemment, les données GEOINT disponibles à un aussi grand nombre d'États ne répondent pas toutes à des besoins de renseignement. En effet, ces données sont également utilisées par la géographique physique civile. En France,

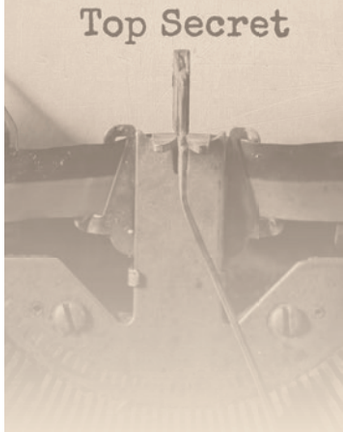


Photo ci-contre :
Ethel et Julius Rosenberg quittent l'US Court House juste après avoir été jugés coupables d'espionnage au service de l'URSS en avril 1951. Ils furent découverts dans le cadre du projet Venona, un travail de cryptanalyse mené par les services de renseignement américains de 1943 à 1980 pour tenter de casser les codes de communication des services soviétiques. Ce dernier permit notamment d'intercepter les renseignements envoyés par les « *atomic spies* », ces agents russes infiltrés aux États-Unis, au Royaume-Uni et au Canada qui aidaient l'URSS à développer sa propre arme nucléaire. (© Roger Higgins)

L'espionnage en France à travers l'Histoire

Ci-contre : Miniature représentant la bataille de Crécy, qui marque le début de la Guerre de Cent Ans. Au cours de cette période, les Capétiens et les Plantagenêt utiliseront de nombreux « observateurs » pour obtenir des informations sur le camp et les positions adverses. (© Jean Froissart)

Ci-dessus : Louis XV, roi de France de 1715 à 1774. C'est sous son règne que sera créé le Secret du Roi, un service secret en charge du renseignement et de la diplomatie secrète qui a fonctionné pendant plus de 20 ans. Il employait 32 agents – dont l'un des plus célèbres est le chevalier d'Eon – ayant pour charge de contrôler les ministres et d'augmenter l'influence de la France à l'Est. Dissout à la mort du Roi, certains de ses agents s'illustreront néanmoins dans la guerre d'indépendance américaine. (© Louis-Michel van Loo)

Ci-contre : Carte postale représentant Mata-Hari en danseuse javanaise en 1906. Elle sera fusillée au cours de la Première Guerre mondiale par la France – pour laquelle elle travaillait –, accusée d'espionnage au profit de l'Allemagne. (© Lucien Walery)

Ci-dessus : Louis XI, roi de France de 1461 à 1483, utilisera les activités d'espionnage pour mener des actions subversives à l'encontre de son ennemi, Charles le Téméraire, telles que la révolte de Liège de 1468.

Ci-contre : Lors de la reddition de la ville d'Ulm, le 20 octobre 1805, Napoléon Ier reçoit la capitulation du général Mack. Cette victoire serait le fait de l'action de Charles Louis Schulmeister, resté célèbre pour sa carrière d'espion au service de Napoléon. (DR)

l'Institut géographique national (IGN) commercialise des images, ainsi que des cartes établies d'après les relevés du satellite militaire Hélios. Potentiels à la fois de renseignement et de connaissance géographique, tant militaire que privée, ces satellites n'ont cependant pas tous les mêmes capacités optiques (résolution, prise de vue...). Seuls les plus puissants (et donc les nations qui les possèdent) seront à même de fournir du renseignement.

Le renseignement diplomatique : l'exemple vénitien

Outre ces ruptures technologiques, une troisième rupture, plus culturelle celle-là, est à prendre en compte. Elle oppose les modèles de renseignement qui furent induits par les régimes politiques qui les créèrent. Historiquement, elle mettrait face à face une tradition diplomatique (motivée par les menaces extérieures) et une autre, plus policière (motivée par les menaces intérieures). Si la France se trouve, pour sa part, dans une position intermédiaire, en raison des conditions de sa construction étatique heurtée, la première « culture » trouverait son origine dans les cités-États italiennes de la Renaissance. Ces entités administratives autonomes se concurrençaient aussi bien sur le plan politique que sur celui, déjà, de l'économie. Si le Saint-Siège inventa la diplomatie, Venise présenta de la fin du XIVe siècle à 1799 des structures de renseignement multiformes : politique (pour surveiller les opposants), diplomatique (ambassadeurs et agents, puisqu'obligation était faite à tout Vénitien à l'étranger de rapporter ses vues à ses autorités souveraines), militaire (à destination de tous les ennemis de la puissance vénitienne, en Europe occidentale comme en Méditerranée), économique (pour protéger l'industrie verrière de Murano). L'usage de chiffres (pour coder les communications écrites), le contre-espionnage (pour protéger les secrets vénitiens et empêcher que des agents étrangers ne s'en emparent) comme l'action (sabotage, attentat, guerre chimique) complétaient les capacités clandestines vénitiennes (4).

Il n'y a pas de prédestination vénitienne, seulement une conjonction de phénomènes historiques qui, en se reproduisant ailleurs, eurent les mêmes conséquences. C'est la recherche de la puissance commerciale et maritime qui porta Venise à ouvrir des comptoirs et à nouer des contacts tout autour de la Méditerranée. De la même façon, elle anima plus tard les Compagnies des Indes (East India Company, 1600 ; Vereenigde Oostindische Compagnie, 1602 ; West-Indische Compagnie, 1621...). La position centrale de Venise dans l'espace informationnel euro-méditerranéen a grandement favorisé la réalisation de ses objectifs. En effet, tout Européen qui revenait de pays lointains, au terme d'un voyage de travail, politique, d'étude ou de pèlerinage, rapportait des « nouvelles » politiques et économiques. Venise les centralisait, comme le firent à sa suite ou parallèlement ces marchands et banquiers de Florence et d'Augsbourg, les Medici (XIIIe-XVe siècles) et les Fugger (XIVe-XVIe siècles), mais aussi la place financière de Londres (depuis 1571). Cette attention accordée à l'information et à son analyse trouve sa source dans les origines de Venise, fondée par les populations qui, fuyant l'envahisseur, s'étaient installées dans les îles des marais situés le long de la mer Adriatique. L'appréhension de la menace fut également la raison pour laquelle le secrétaire principal de la reine Elizabeth, Sir Francis Walsingham, doubla le réseau diplomatique anglais par des correspondants particuliers sur le continent ; il s'agissait autant de surveiller Français et Espagnols, concurrents maritimes, que de limiter les succès de la contre-réforme animée par l'Autriche. Cette utilisation du renseignement dans des buts géopolitiques fut aussi bien à la base du « Secret du Roi », pour offrir la Pologne à Louis XV de France, que de la création des premiers services, en France puis en Grande-Bretagne, au XIXe siècle.

> *« Venise présenta, de la fin du XIVe siècle à 1799, des structures de renseignement multiformes : politique, diplomatique, militaire et économique. »*

La tradition policière, un modèle nord-européen

Toute autre fut la logique perceptible, à la même époque, en Europe du Nord, entre Prusse et Russie tsariste – rejointes plus tard par l'Italie. Leur perception du renseignement fut moins tournée vers l'ensemble des secteurs de la vie publique, que vers la sécurité intérieure. Toutes les puissances continentales craignaient l'action des séditions progressistes venant de la France révolutionnaire. Mais ces trois-là furent les seules à développer des structures permettant de poursuivre à l'étranger leurs ressortissants qui adhéraient à ces idées. Aux lendemains du « printemps des peuples », la Prusse fut ainsi la première à organiser une Union policière des États allemands, de 1851 à 1866, avec comme visée de supprimer toute opposition politique, libérale, socialiste ou anarchiste. Cette culture ancienne de coopération de police criminelle expliquait aussi, après le rôle éphémère d'Albert Ier de Monaco, l'intérêt de l'Autriche et l'Allemagne, notamment nazie, pour la Commission internationale de police criminelle avant 1945.

En Russie, du lendemain de l'assassinat d'Alexandre II (1881) à la révolution

Photo ci-dessous :
Tableau représentant le Conseil des Dix vénitien assistant à l'exécution du doge Marino Faliero. Le Conseil des Dix, fondé en 1310, avait pour rôle – jusqu'à la chute de la République en 1797 – de veiller à la sûreté de l'État en préservant le gouvernement de la République de Venise des complots et de la corruption grâce notamment à sa mainmise sur la diplomatie et les services de renseignement. (© Francesco Hayez)

Photo ci-dessous :
Siège de la Gestapo à Berlin. Cette « police secrète d'État », fondée en Prusse par Hermann Göring, était chargée de lutter contre les opposants internes ou externes, ainsi que contre les adversaires du régime nazi ou les résistants dans les pays occupés. Selon le décret du 10 février 1936, la Gestapo avait « la tâche de rechercher toutes les intentions qui mettent l'État en danger, et de lutter contre elles, de rassembler et d'exploiter le résultat des enquêtes, d'informer le gouvernement, de tenir les autorités au courant des constatations importantes pour elles et de leur fournir des impulsions. » (© Bundesarchiv)

de février 1917, furent échafaudées les premières *agenture* (« postes extérieurs »), à Paris et à Sofia, d'une Section de préservation de la sécurité et de l'ordre publics, connue sous son nom abrégé, l'Okhrana (« section de sécurité »). Véritable police politique à l'intérieur de l'Empire tsariste, utilisant des agents provocateurs – comme le lui apprirent les agents de la Préfecture de Police de Paris qui furent employés par l'*agentura* française –, il s'agissait d'une agence de renseignement politique à l'extérieur, chargée de surveiller les sociaux-démocrates allemands, suisses et français, les anarchistes polonais et lituaniens à Londres, les socialistes révolutionnaires comme les juifs du Bund, tant à New York qu'à Paris.

À la même époque (1881), l'Italie obtint le soutien de la police britannique pour surveiller la mouvance anarchique au sein de l'immigration péninsulaire résidant en Grande-Bretagne ; cette surveillance dura jusqu'à la Première Guerre mondiale (5).

Quand ces trois pays, la Russie, l'Italie et l'Allemagne, embrassèrent des régimes totalitaires (soviétique, fasciste et national-socialiste), elles adoptèrent le principe d'une police politique. Dès décembre 1917, la Commission extraordinaire panrusse pour la répression de la contre-révolution et du sabotage (Tchéka), comme dix ans plus tard l'Organisation de vigilance et répression de l'antifascisme italienne (OVRA), puis la Police secrète d'État allemande (Gestapo) en avril 1933, eurent pour but de protéger l'idéologie au pouvoir de ses ennemis intérieurs et extérieurs. Fait notable, les services de gardes-frontières de ces pays ressortissaient à ces polices politiques. Si les deux dernières disparurent avec la défaite allemande à la fin de la Seconde Guerre mondiale (1945), la première, devenue en 1957, au terme de quatre mutations inhérentes aux mues du régime soviétique, le Comité pour la Sécurité de l'État (KGB), prolongea ses activités jusqu'à la disparition de l'Union soviétique, en 1990. Elle se réincarna plus tard en Service fédéral de sécurité de la Fédération de Russie. Ironie de l'histoire, certains anciens de la Gestapo et de l'OVRA furent récupérés par les nouveaux régimes démocratiques dans l'immédiat après-guerre ; il s'agissait de ceux qui avaient lutté contre les communistes. L'heure était à la guerre froide et le communisme était l'ennemi du Monde libre.

La transdisciplinarité d'aujourd'hui

Meneurs de ce Monde libre, les États-Unis durent passer outre leurs réticences à se doter d'un service de renseignement – le débat porta notamment sur l'opportunité de se doter d'une « Gestapo » – et à rejoindre le club démocratique des services. Ces réticences expliquaient pourquoi furent séparées au maximum les spécialités (renseignement humain, ROEM, ROIM ; interne et externe), au point de créer une myriade de services – 16 au total. En 1981, conscients que leurs services étaient le meilleur rempart contre une dictature, les États-Unis constituèrent une communauté du renseignement, sous la coordination d'un directeur du renseignement (6).

> *« La perception du renseignement [en Europe du Nord, entre Prusse et Russie tsariste, rejointes plus tard par l'Italie] fut moins tournée vers l'ensemble des secteurs de la vie publique, que vers la sécurité intérieure. »*

Ailleurs, sous la double impulsion de l'affadissement de la guerre froide et de la montée du risque terroriste, il importe aujourd'hui de faire travailler ensemble les différents services. Cette transdisciplinarité appliquée au monde du renseignement est devenue la règle dans tous les pays du monde, comme la séparation du domaine intérieur et extérieur est la garantie du fonctionnement démocratique des moyens de renseignement d'un État.

Gérald Arboit

Notes

(1) Cette expression du célèbre théoricien militaire prussien Carl von Clausewitz (1780-1831) sert à caractériser toute l'incertitude qui entoure une situation de guerre.

(2) Service de renseignement de l'armée (l'expression est apparue pour désigner celui de l'armée française en 1871, en référence au Deuxième Bureau de l'état-major général dont il relevait), NdlR.

(3) Algérie, Allemagne, Arabie saoudite, Autriche, Belgique, Corée du Sud, Croatie, Danemark, Émirats arabes unis, Espagne, Éthiopie, Finlande, France, Grèce, Hongrie, Inde, Israël, Italie, Japon, Jordanie, Macédoine, Pays-Bas, Norvège, Pakistan, Pologne, Roumanie, Singapour, Suède, Taïwan, République tchèque, Thaïlande, Tunisie, Turquie, mais aussi Afrique du Sud, Luxembourg, Mexique, Sud-Vietnam, Philippines ou République populaire de Chine. Voir Jeffrey T. Richelson, The U.S. Intelligence Community, Cambridge, Massachusetts, Ballinger, 1989, p. 280-283.

(4) Paolo Preto, *I servizi segreti di Venezia: spionaggio e controspionaggio ai tempi della Serenissima*, Milan, Il Saggiatore, 2010.

(5) Pietro Di Paola, « The Spies Who Came in from the Heat: The International Surveillance of the Anarchists in London », *European History Quarterly*, vol. nº 37, nº 2, avril 2007, p. 189-215.

(6) Executive Order 12333-United States intelligence activities, 4 décembre 1981.

À quoi sert le renseignement ?

Par **Éric Denécé**, directeur du Centre français de recherche sur le renseignement (CF2R).

En raison de l'absence de culture du renseignement dans la société française et de la déformation de sa présentation par les médias, il n'est nullement inutile de chercher à mieux définir ce qu'est vraiment le renseignement. La profession souffre en effet d'une quadruple méconnaissance : celle de son vocabulaire, de ses missions, de ses métiers et de son contrôle. Sur le plan du vocabulaire, le renseignement a son langage propre qu'il importe de connaître pour comprendre le métier. Généralement, les profanes parlent indifféremment de services secrets, spéciaux, de renseignement, de sécurité, etc. Or chacun de ces termes recouvre une réalité différente :

• Un **service de renseignement (SR)** est la pointe de diamant du dispositif de renseignement d'un État. Sa fonction est de se procurer les informations secrètes grâce auxquelles il sera possible de répondre aux préoccupations des autorités. La *recherche* est le vrai nom de l'espionnage. Elle est par nature clandestine.

• Un **service spécial** est en premier lieu un organisme chargé de pratiquer l'intervention clandestine sous ses différentes formes : politique, psychologique, économique, paramilitaire et violente. Il peut également se livrer à des recherches ponctuelles, le plus souvent aux fins d'action.

• Un **service de sécurité** est un organisme dont la finalité principale et d'assurer la protection d'un corps social contre les menaces externes (espionnage, terrorisme) ou internes (extrémisme et violence politique).

• Un **service secret** est un organisme dont l'existence et les opérations sont inconnues à la fois de ses ennemis, des citoyens et de l'administration de son propre pays, à l'exception de quelques rares personnes, au plus haut niveau de l'État, qui le dirigent. L'existence d'un véritable service secret est devenue impossible dans les démocraties soumises au contrôle parlementaire. Tous les autres services (de renseignement, spéciaux ou de sécurité) ont une existence légale, des budgets votés par le Parlement, sont connus par les citoyens – qui peuvent y faire acte de candidature – par la presse et par les États étrangers. Seules leurs missions et la liste de leurs personnels sont secrètes.

• Contrairement à une confusion extrêmement répandue, un **agent secret** n'est jamais membre d'un service de renseignement. C'est un individu extérieur, qui est ciblé, recruté, instruit et manipulé pour obtenir des renseignements bruts. Il est dirigé par un membre permanent d'un service de renseignement appelé *officier traitant*. Ce titre n'est pas un grade et n'a rien à voir avec le monde militaire. C'est une fonction administrative, au même titre que l'officier ministériel ou l'officier de police judiciaire.

• Enfin, il existe de nombreuses confusions sur ce qu'est un **renseignement**. Celui-ci se distingue d'une information, non par sa nature, mais par sa finalité, c'est-à-dire par l'utilisateur, qui est celui qui lui confère sa valeur. Un renseignement est une information utile à quelqu'un qui l'a demandée dans une perspective précise. « Un renseignement n'est en effet pas une simple information, mais une information qui enseigne quelque chose à quelqu'un. Mais il n'est pas non plus un simple enseignement, car il ne vise pas la formation des gouvernants. Il est au contraire lié à l'action, subordonné à elle, ou impliqué en elle : il est „ciblé". Il vaut par et pour l'action politique » (1).

À quoi sert un service de renseignement (SR) ?

Dans quel but fait-on appel à lui ? Quelles sont ses missions ?
« Le renseignement s'occupe de toutes les choses qui devraient être connues antérieurement à l'élaboration d'une ligne de conduite » (2). En effet, tout État, organisation ou groupe a des projets (conserver ou développer, défendre ou conquérir) et est donc confronté à des risques (ne pas atteindre ses buts, être vaincu, disparaître, etc.). Le renseignement lui permet d'accroître sa connaissance de l'environnement dans lequel il évolue et de faciliter ses prises de décision. Il a pour but d'identifier les opportunités et de détecter les menaces qui pourraient faciliter, perturber ou empêcher la réalisation de sa stratégie. Il permet de réduire l'incertitude, d'employer au mieux ses ressources, d'anticiper les risques et de réduire leur impact éventuel. Ainsi, le recours au renseignement est l'expression d'une volonté de maîtrise de son destin. Au profit d'un État, un service de renseignement remplit six fonctions complémentaires mais distinctes :

• **Obtenir des informations difficiles d'accès**. La première mission d'un service est de satisfaire les besoins en renseignement des autorités en perçant les secrets adverses. Dans cette perspective, un État a besoin d'un organisme capable de lui procurer des informations d'une importance stratégique, protégées par ceux qui les détiennent. Elles ne peuvent être obtenues que par des moyens clandestins, notamment en assurant la pénétration d'agents dans les administrations et les services adverses.

• **Décrypter les stratégies cachées**. Un gouvernement doit connaître les manœuvres secrètes de ses partenaires et adversaires afin de pouvoir les devancer. Les services aident les gouvernants à comprendre quelles sont leurs véritables intentions grâce au suivi de leurs activités clandestines, lesquelles sont l'expression de leur stratégie cachée. En mettant en lumière « l'envers du décor », les services apportent un autre niveau de lecture aux décideurs que ceux de la diplomatie classique ou des médias. C'est une véritable action de décryptage : révéler ce qui est caché et rendre intelligible ce qui ne l'est pas.

• **Détecter les menaces**. Cette fonction consiste à alerter les autorités et les administrations compétentes (Intérieur, Affaires étrangères, Défense, Économie, etc.) des dangers et menaces contre nos intérêts, nos ressortissants et nos alliés, en France et à l'étranger (conflits, terrorisme, enlèvements, activités criminelles, rupture d'approvisionnements, etc.) dès qu'un acteur international développe une action qui pourrait être dommageable.

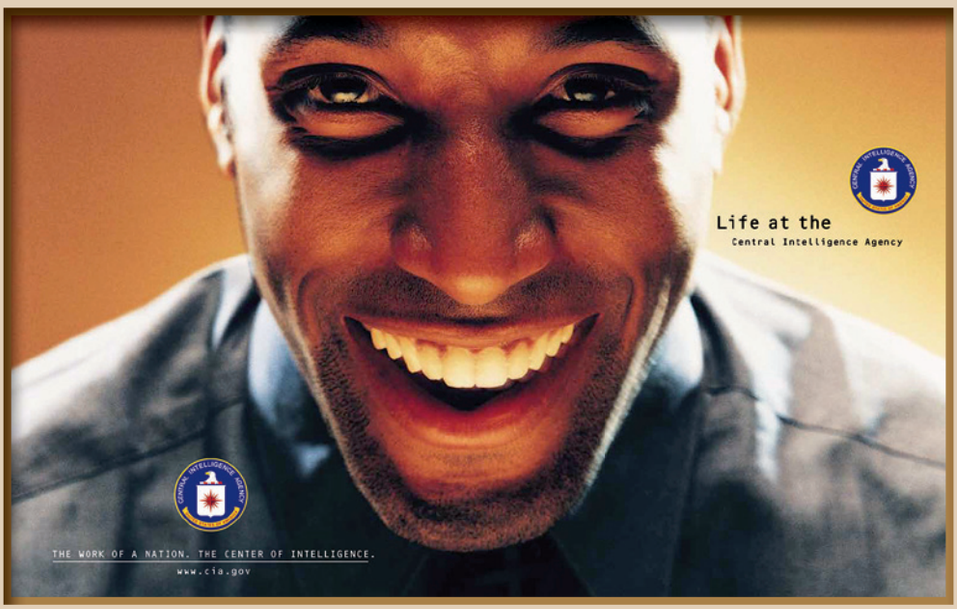
• **Établir et entretenir des contacts secrets avec les adversaires**, en particulier ceux avec lesquels n'existent pas de relations officielles, ce que ne peuvent faire les diplomates. Cette « diplomatie secrète » est particulièrement utile en situation de conflit ou de prise d'otages, car elle permet de maintenir un canal de communication ouvert en permanence entre parties rivales. Cela permet de réduire les risques d'aggravation des différends, voire de préparer la reprise des relations dans l'hypothèse d'une fin d'affrontement.

• **Influer secrètement sur les événements mondiaux**. Un gouvernement fait appel à son service pour intervenir secrètement à l'étranger afin de défendre ses intérêts ou contrer les politiques occultes des autres acteurs internationaux quand ses autres moyens ne le permettent pas. Ce domaine spécifique est celui de *l'Action* : il recouvre l'ensemble des opérations clandestines par lesquelles un État s'ingère secrètement dans les affaires des autres. Les gouvernements y ont recours pour orienter les événements mondiaux en leur faveur, protéger leurs intérêts contre leurs rivaux ou éliminer des adversaires.

• **Neutraliser les moyens d'information et d'action clandestines adverses**. Le rôle du renseignement est enfin d'altérer les moyens d'information et d'action de nos adversaires et de nos concurrents afin de garder un avantage sur eux, car leurs pratiques sont en tout point similaires aux nôtres : eux aussi cherchent par

tous les moyens à s'informer et à influer sur la politique internationale, parfois à nos dépens. C'est pourquoi les actions de contre-espionnage et de tromperie sont essentielles pour affaiblir les capacités des appareils de renseignement et de compréhension adverses.

Le monde du renseignement regroupe donc des activités et des métiers extrêmement variés. Leurs pratiques professionnelles sont très rigoureuses et codifiées, fort différentes d'une spécialité à l'autre. Les qualités d'un bon analyste ne sont pas celles d'un officier traitant chargé de la recherche, et un spécialiste de l'action clandestine n'a que peu en commun avec un expert du contre-espionnage. Dans tous les pays du monde, l'architecture des services de renseignement et de sécurité intérieurs s'organise autour de la concentration ou de la segmentation de ces fonctions, ce qui explique qu'ils ne soient pas toujours comparables les uns aux autres, bien que leur vocation soit similaire.



Au service de l'État

Autre élément qu'il est essentiel de rappeler : les services sont des organismes d'État qui agissent conformément aux directives et aux orientations de leur gouvernement, dont ils ne sont que l'instrument. Tous leurs personnels ont un statut de fonctionnaires, civils ou militaires, ou sont des contractuels de l'administration. Comme le rappelle Constantin Melnik : « Les services spéciaux des démocraties (…) ne sont pas des officines louches confiées à de ténébreux irresponsables, mais des organismes sophistiqués et structurés, hiérarchisés et disciplinés dont la seule vocation est, dans la stricte obéissance au pouvoir civil, quelle que soit sa couleur politique, de servir la nation et l'État. Pendant la guerre d'Algérie, les opérations „Action" du SDECE portant atteinte à la vie humaine ou aux biens matériels – en code : opérations „Homo" et „Arma" – ne pouvaient donc être entreprises que si elles avaient été autorisées par les plus hautes autorités de l'État » (3).
Les services ne s'autosaisissent jamais d'une mission. Douglas Hurd, ancien ministre des Affaires étrangères britanniques (1989-1995) est on ne peut plus catégorique sur ce point : « Pas plus le SIS que le GCHQ ne font ce qu'ils veulent ou n'ont leurs propres agendas, ni ne définissent leurs propres objectifs ou n'agissent de leur propre chef sans la connaissance et l'autorisation des ministères. Ils ne s'inventent pas de missions et ne conduisent leurs tâches qu'en appui de politiques spécifiques » (4). Si les approches des services de renseignement sont différentes de celles des diplomates, elles n'en sont pas moins dictées par le même gouvernement qui cherche, par plusieurs voies, à assurer le succès d'une politique unique.
De même, femmes et hommes du renseignement ne sont pas des individus incontrôlables sans foi ni loi, faisant ce que bon leur semble au nom de la raison d'État. S'ils transgressent régulièrement la légalité, c'est à la demande des autorités de l'État et au bénéfice de l'intérêt national, c'est-à-dire dans un but légitime ou considéré comme tel. La finalité de ces organisations et la vocation des agents publics qui en relève est donc tout à fait unique.

Le renseignement est-il éthique ?

Cela signifie-t-il pour autant qu'il s'agisse d'une profession dénuée de tout sens moral et de toute préoccupation éthique ? Une éthique peut-elle exister dans un métier dont les pratiques – et les qualités recherchées chez les professionnels – sont celles de la dissimulation, du mensonge et de la manipulation de tiers ?
Dans les pays démocratiques, l'exigence éthique s'applique depuis longtemps aux activités de renseignement. La profession a ses règles, ses valeurs, ses codes de conduite – lesquels peuvent, certes, encore être améliorés – et les dérives de quelques-uns ne doivent pas couvrir d'opprobre les autres (5).
Par ailleurs, rappelons que depuis plusieurs décennies, tous les États démocratiques ont mis en place des organismes de contrôle – parlementaires ou administratifs – chargés de vérifier le bon emploi des services par le gouvernement. Le renseignement est donc constamment sous l'œil des élus de la représentation nationale [voir également p. 36 de ces *Grands Dossiers*, NdlR].

En conclusion, il est indispensable de mieux connaître le renseignement afin de comprendre son utilité, de l'employer à bon escient et de ne pas nourrir de faux espoirs quant à son efficacité. Bien qu'indispensable, il n'est pas une arme miracle. Le renseignement ne gagne jamais les guerres à lui tout seul. Si la connaissance est une condition nécessaire, elle n'est en aucun cas suffisante. Ce n'est pas parce que l'on sait, souvent très approximativement, ce que l'adversaire va faire que l'on peut effectivement l'en empêcher. Comme l'a dit un jour un spécialiste anglais du renseignement, « si vous êtes ligoté sur une voie de chemin de fer, la tête sur une file de rails et les pieds sur l'autre, la connaissance de l'horaire et de la composition des trains ne vous sera que d'une bien faible utilité ! ».

Éric Denécé

Photo ci-contre : Affiche de recrutement de la CIA. Alors que le recrutement du personnel s'avère stratégique pour les agences de renseignement, la DGSE française – qui recherche 600 nouveaux agents d'ici 2019 pour parer aux nouvelles menaces – axe son recrutement sur des jeunes ayant des compétences particulières en physique, en balistique, en mathématiques, en langues ou en informatique. De son côté, le MI6 britannique a lancé en mars 2017 une campagne télévisée, signe d'un nouveau type de recrutement, « moderne et multiculturel », adapté aux menaces contemporaines parmi lesquelles le terrorisme, la cybercriminalité ou l'espionnage industriel, qui se développe particulièrement en Asie. (© CIA)

Notes

(1) Hélène L'Heuillet, *Basse politique, haute police : une approche historique et philosophique de la police*, Paris, Fayard, 2001, p. 26.

(2) Rapport du groupe de travail de la deuxième Commission Hoover sur les activités du renseignement (1955).

(3) Constantin Melnik, *1000 jours à Matignon*, Paris, Grasset, 1988, p. 255.

(4) Philip H. J. Davies, *MI6 and the Machinery of Spying*, Londres, Franck Cass, 2004, p. 346.

(5) Il convient de parler de « barbouzeries » quand :
- des privés s'arrogent des pouvoirs et des pratiques réservés aux services d'État ;
- des services d'État utilisent leur position et leurs moyens pour résoudre des affaires personnelles ou catégorielles sans lien avec les intérêts de la nation.

analyse

La source humaine, l'art du renseignement

Si le recueil du renseignement s'est indéniablement modifié au fil des siècles, notamment du fait des révolutions technologiques, le recours à des sources humaines demeure une constante, aujourd'hui trop souvent négligée, mais toujours indispensable.

Par **Brigitte Henri**, ancien commissaire de police des Renseignement généraux (DCRG) et auteur de *Histoire secrète des RG* (Flammarion, février 2017).

Rappelons quelques faits historiques qui montrent bien le rôle et l'importance de la source humaine pour obtenir des renseignements de qualité. Après la Deuxième Guerre mondiale, c'est grâce à des informateurs insérés dans l'appareil communiste français que les Renseignements généraux obtiendront des informations qu'ils n'auraient jamais eues autrement sur ce mouvement politique. En 1962, pendant la guerre d'Algérie, « Jules », bien implanté au sein de l'OAS, donnera le jour et le lieu de la réunion des chefs de cette organisation qui doit se tenir en Italie. Ces renseignements permettront les arrestations de deux membres de l'OAS et surtout celle d'un homme de poids, le dirigeant de cette organisation, Georges Bidault. Grâce à l'infiltration de plusieurs taupes au sein de la Sorbonne, en mai 1968, les RG pourront dresser un état précis de la situation au sein de cette université que divers groupes, parfois dangereux, occupent depuis plusieurs mois. En 1969, un ouvrier prénommé « Paul », responsable d'un petit syndicat à gauche de la CGT, commet un détournement de fonds. Informé, un agent des RG le rencontre et lui promet, en échange de son aide, de ne pas révéler l'affaire à la justice. L'ouvrier accepte et, pendant plusieurs années, infiltre la « gauche prolétarienne ». Il y prend d'ailleurs une place conséquente au point d'être associé aux décisions importantes de ce mouvement. Dans les années 1970, les RG comme la DST infiltreront le bastion des maoïstes, l'usine Peugeot à Sochaux, grâce à deux informateurs qui vont leur livrer des informations précieuses sur les actions menées par ce groupe. Pour tenter de stopper les actions violentes d'Action directe au cours des années 1980, les RG recruteront des indicateurs, notamment Gabriel Chahine qui connait Jean-Marc Rouillan et Nathalie Ménigon, leaders de ce mouvement extrémiste. C'est grâce à cette source que les membres d'Action directe seront arrêtés le 13 septembre 1980 à Paris. Pendant la vague d'attentats à la fin des années 1990 en France, les RG recruteront des informateurs dans les mosquées

Photo ci-dessus :
Selon la théorisation du mode de recrutement et de traitement d'une source humaine, il existe quatre principaux leviers pour l'inciter à fournir le renseignement auquel elle a accès, que l'on peut désigner sous l'acronyme anglais MICE pour *Money, Ideology, Constraint, Ego* (argent, idéologie, coercition et ego). D'autres leviers dits SANSOUCIS existeraient néanmoins : solitude, argent, nouveauté, sexe, orgueil, utilité, contrainte, idéologie et suffisance. (© Lionel Martinez)

Que sont devenus les RG ?

Avant la fusion avec la DST, il y avait environ 4000 fonctionnaires aux RG. Un peu moins de la moitié est restée à la DCRI (aujourd'hui la DGSI), créée en 2008 et fruit de la fusion entre la DST et les RG, où les missions ont été axées sur la lutte antiterroriste, le contre-espionnage, la protection des intérêts économiques, la surveillance des milieux subversifs et les mouvements pouvant menacer l'État.

L'autre moitié de cet effectif a été reversée à la Sous-direction de l'Information générale – SDIG (devenue en 2014 le Service central du Renseignement territorial ou SCRT) –, sous-direction qui a été rattachée à la Direction de la Sécurité publique. La SDIG a eu pour missions de centraliser les renseignements dans les domaines institutionnel, économique et social, en axant leurs investigations sur les phénomènes urbains violents, l'économie souterraine, les violences sportives, les sectes et les conflits sociaux.

La prééminence de la DCRI dans les missions les plus prestigieuses a fait de la SDIG un service de seconde zone, sans réels moyens humains et matériels. Or, c'était les fonctionnaires de la SDIG qui allaient sur le terrain, notamment dans les banlieues difficiles. Les renseignements qu'ils remontaient à la DCRI n'étaient pas ou peu exploités. En outre, les cultures très différentes de la Sécurité publique et du renseignement ont été un frein considérable pour évaluer la dangerosité de certains jeunes de banlieues.

De son côté, la DCRI n'a pas anticipé le caractère hybride des nouveaux terroristes, également condamnés pour des infractions de droit commun (Merah condamné pour 20 faits, les frères Kouachi et Coulibaly dealers et braqueurs, l'un des kamikazes du Bataclan condamné à 8 reprises, etc…). Confrontée à des échecs retentissants dans la lutte antiterroriste, la DCRI est devenue la DGSI en 2014. **B.H.**

Photo ci-dessus :
Nicolas de La Reynie, nommé premier lieutenant général de police de Paris en 1667, sous le règne de Louis XIV. À cette fonction qu'il va occuper durant trente ans, celui qui est considéré comme le père de la police judiciaire française s'est appuyé sur un réseau de dix mille informateurs rémunérés – les « mouches » en liberté et les « moutons » en prison – au sein de tous les milieux sociaux. (DR)

pour évaluer le degré de radicalisation de certains jeunes. C'est le croisement de plusieurs sources, notamment humaines, qui permettra de démanteler le réseau dit « Djamel Beghal », en septembre 2001, alors qu'il prépare un attentat à la voiture piégée contre l'ambassade des États-Unis à Paris. Il faut rappeler que Djamel Beghal fera la connaissance en prison de Chérif Kouachi et d'Amedy Coulibaly, impliqués dans les attentats qui seront commis en janvier 2015 à Paris…

Ces quelques exemples traduisent bien le rôle déterminant des informateurs dans la collecte du renseignement sensible, c'est-à-dire le plus inaccessible, celui que l'on ne trouve jamais sur Internet.

La technologie face à la source humaine

Car un phénomène majeur est venu modifier la collecte du renseignement : la révolution technique et informatique. En effet, l'explosion des réseaux informatiques a entrainé une véritable mutation dans le recueil du renseignement, les serveurs privés ainsi qu'Internet étant devenus des vecteurs incontournables dans ce domaine. Toutefois, cette explosion ne s'est pas toujours accompagnée d'un contrôle rigoureux et fiable du contenu même des informations. Celles-ci ont été souvent constituées de dossiers faits par quelques sources et sont, par contre, véhiculées par plusieurs réseaux, donnant ainsi l'impression à l'utilisateur d'être recoupées alors qu'elles ne sont que copiées. Cela est particulièrement vrai pour Internet. Aujourd'hui, les agents des services de renseignement axent – trop, pour beaucoup – leurs principales sources d'information sur ces outils, négligeant ce qui était auparavant essentiel : la source humaine.

Faut-il rappeler qu'en 2001, les attentats que subissent les États-Unis d'Amérique mettent en exergue la nécessité, dans le cadre de la lutte antiterroriste, de renforcer au plus vite le recours à des indicateurs, négligé au profit d'une recherche du renseignement par des moyens technologiques. Ces dernières années, les difficultés rencontrées par la DCRI puis par la DGSI dans la lutte contre le terrorisme ont mis plus que jamais en exergue le rôle déterminant du travail de terrain qu'assuraient les RG et la DST au quotidien dans ce domaine.

Les attentats du 13 novembre 2015 à Paris le montrent clairement. « On a voulu miser sur le renseignement technologique, à l'américaine, le "Big Data" et toutes ces choses-là. Or, ce n'est pas très efficace. Il suffit de voir aux États-Unis, les déclarations du général Alexander, patron de la NSA, en 2013, sur l'efficacité très relative des milliards dépensés dans la technologie après le 11 septembre 2001. Aujourd'hui, on en est pourtant là : on a concentré nos moyens sur le renseignement technologique, et on a baissé la garde sur le renseignement humain. » (1)

Renforcer le recrutement d'informateurs est donc une nécessité. Mais cela exige du temps ; temps qui ne cadre pas toujours avec les stratégies à court terme des hommes politiques.

Recruter une source humaine : un travail d'artiste…

L'approche d'un service de renseignement par une personne implique une détermination particulière de sa part car elle se dévoile en partie, ne serait-ce qu'en donnant son identité et en évoquant ses activités professionnelles. Elle sait que les renseignements qu'elle apporte peuvent mettre en œuvre des opérations de police judiciaire, telles que des arrestations, gardes à vue, perquisitions…

Sa ou ses motivations doivent donc être suffisamment fortes pour susciter une telle démarche. Ne nous y trompons pas, la motivation n'est pas exclusivement financière. En matière de terrorisme, de trafics de drogue, d'armes ou de prostitution, l'appât du gain peut être à l'origine de quelques renseignements. Les services des Renseignements généraux ou de la DST, lorsqu'ils existaient, mais aujourd'hui ceux de la PJ, de la gendarmerie, des douanes et de la DGSI, rémunéraient ou rémunèrent régulièrement ou accessoirement les « indics » appartenant à ces milieux.

Par contre, dans les domaines financiers, sociaux ou politiques, la démarche du correspondant est autre. L'espoir d'obtenir une faveur ou une information en échange du renseignement donné, le désir de se venger, voire d'échapper à des pressions, ou – et cela se rencontre souvent – le besoin de se rendre utile, d'être écouté, considéré, de faire cesser une injustice et d'avoir le sentiment d'aider la police ou la justice à remplir leurs missions, font partie des principales motivations de ces personnes. Cependant, certains ont une démarche plus pernicieuse. Ils espèrent, moyennant quelques renseignements,

Les limites de la technologie

Stansfield Turner (photo), directeur de la CIA de 1977 à 1981, déclarait en 1985, alors que la difficulté à pénétrer le camp soviétique par des méthodes classiques de renseignement humain avait incité les Américains à développer de nouvelles formes de renseignement, que « l'espionnage humain [était] devenu un complément aux systèmes techniques ». Ce haut fonctionnaire, qui avait la réputation de faire davantage confiance aux ordinateurs qu'à son personnel, fut responsable du licenciement de plus de 600 personnes à la CIA. Les commissions parlementaires américaines qui ont enquêté sur l'affaire des prétendues armes de destruction massive en Irak et sur les attentats du 11-Septembre ont depuis mis au jour les insuffisances patentes de la CIA dans le domaine du renseignement humain. (© US Department of The Navy)

souvent du reste de bonne qualité, pouvoir, lorsque cela les arrange, faire état de leur « collaboration ». Ces informateurs peuvent être dangereux car ils cherchent alors à minimiser leur responsabilité dans des affaires douteuses dans lesquelles ils sont partie prenante. Ils n'hésitent pas à affirmer qu'ils agissent sous contrôle d'un service de renseignement et qu'ils rendent compte régulièrement de leurs activités, même si cela est faux.

Il ne faut certes pas oublier qu'une « bonne police » de renseignements consiste aussi à fréquenter des voyous pour mieux les démasquer. L'agent de renseignement doit donc informer régulièrement sa hiérarchie par des rapports ou des notes destinés à le protéger.

Dans la majorité des cas, le futur informateur est souvent contacté, directement ou indirectement, par le fonctionnaire de renseignement. La rencontre peut avoir lieu d'ailleurs fortuitement, à l'occasion d'un repas, d'une réunion, d'une affaire précise... Le rôle du policier de renseignement est alors déterminant. C'est lui qui doit habilement enclencher le processus des rencontres régulières en décelant les motivations susceptibles d'amener la personne à se confier à lui. C'est également lui qui doit établir un rapport de confiance.

> *« La confiance qui s'instaure entre le correspondant et l'agent de renseignement repose sur le temps. L'agent doit apprendre à connaître celui qu'il traite, à évaluer sa sincérité à son égard, à comprendre ses motivations profondes. Inversement, le correspondant doit se sentir soutenu et savoir ce que l'on attend de lui. »*

Les plus grands atouts en matière de recrutement de sources humaines sont la patience, la capacité d'écoute et une connaissance aussi précise que possible de la source et du domaine dans lequel elle évolue. En tant que demandeur, l'agent de renseignement se trouve en position de faiblesse et doit donc rétablir l'équilibre par un comportement qui permet un échange contrôlé de renseignements. Il doit garder en mémoire que celui qui lui apporte des renseignements refusera – plus ou moins ouvertement – tout lien de dépendance vis-à-vis de lui, même si « on ne peut faire du renseignement efficace sans agents doubles, indicateurs et correspondants soigneusement tenus en main » (2).

La confiance qui s'instaure entre le correspondant et l'agent de renseignement repose sur le temps. L'agent doit apprendre à connaître celui qu'il traite, à évaluer sa sincérité à son égard, à comprendre ses motivations profondes. Inversement, le correspondant doit se sentir soutenu et savoir ce que l'on attend de lui.

Un exercice difficile, jalonné de risques

Quelle que soit la méthode d'approche, la recherche du renseignement auprès des correspondants est un exercice difficile, jalonné de risques. Exercice difficile car correspondants ou informateurs n'apportent pas forcément des renseignements précis et quand bien même ils le font, ces renseignements se trouvent souvent noyés dans des considérations diverses n'ayant pas un intérêt immédiat. La personne peut d'ailleurs donner un renseignement essentiel sans même s'en rendre compte, tout simplement parce qu'elle ne possède pas les éléments qui lui permettent d'apprécier la valeur exacte de ce qu'elle révèle. L'informateur peut avoir également tendance à exagérer, voire à affabuler pour se montrer « à la hauteur ».

Étant avant tout un analyste, l'agent de renseignement doit être capable de trier et de retenir les informations les plus importantes, de les « recouper » aussi. Cette exigence d'intégrité nécessite une vérification systématique de la qualité du renseignement. L'agent doit aussi s'assurer de ne pas trahir ou, en tout cas, de ne pas mal interpréter les dires de son informateur, de ne pas lui attribuer des propos qu'il n'a pas exprimés ou de ne pas influencer celui-ci.

N'oublions pas que lorsqu'un renseignement est transmis par un correspondant, il est déjà déformé, même si ce n'est que de façon infime, par la lecture que ce correspondant en a faite mais aussi par sa culture, son intelligence et son caractère. L'agent de renseignement doit apprécier – et cela n'est pas toujours facile – la touche personnelle qui provient de son contact.

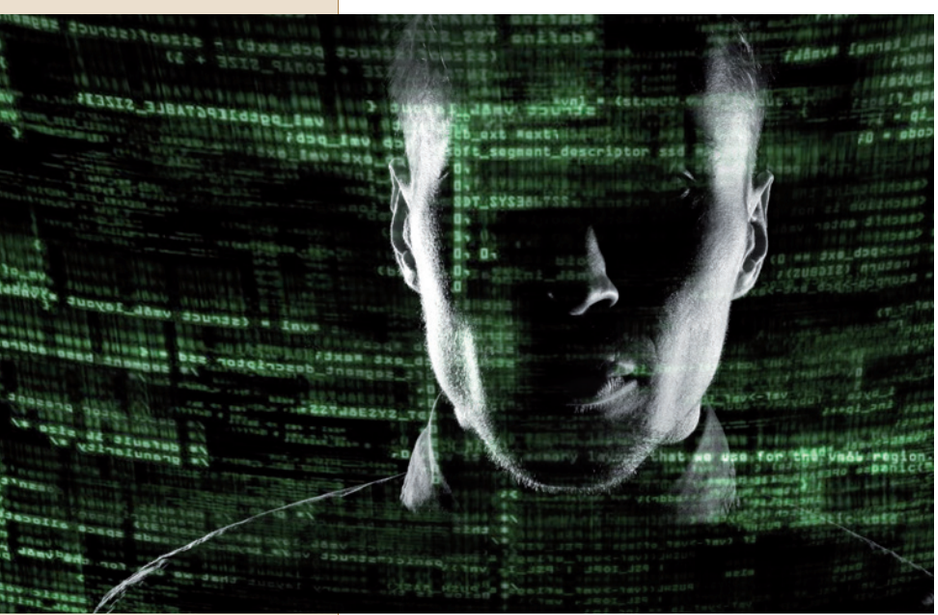
Manipuler les hommes est un moyen utilisé en tout temps, à toute époque. Mais cette omniprésence historique ne rend pas la manipulation sympathique. Le terme « manipuler » est lourd de préjugés ; il renvoie à ce qui est occulte, fourbe. Pourtant, manipuler un informateur, ce n'est pas autre chose que le contrôler, le diriger sans contrainte, bien souvent d'ailleurs avec son consentement tacite. La manipulation consiste à amener l'informateur à dire ce qu'il sait, à adopter une attitude donnée, à exécuter une action déterminée, ceci dans un but précis : obtenir des renseignements susceptibles, par exemple, d'éviter des troubles sociaux graves ou de prévoir des actions déstabilisatrices de la part de groupes extrémistes. Manipuler un informateur n'est pas un jeu. C'est pourquoi le but doit être suffisamment sérieux pour justifier l'utilisation de ce moyen.

Ci-dessus :
Photogramme du film de Christian Carion, *L'Affaire Farewell*, consacré à l'affaire du même nom qui, selon le président américain Ronald Reagan, fut « la plus grande affaire d'espionnage du XXe siècle ». C'est en 1980 que Vladimir Ippolitovitch Vetrov, ayant pour nom de code « Farewell », alors lieutenant-colonel du KGB, responsable de la section Europe occidentale de ce service, deviendra un agent de la DST française. Il permettra à celle-ci et aux autres services occidentaux de renseignement de mieux connaître les méthodes et la structure du KGB dans les années 1980, en pleine guerre froide. Démasqué en avril 1983, il sera condamné à mort pour haute trahison. (© Neoclassics Films Ltd.)

Pour aller plus loin

Brigitte Henri, *Histoire secrète des RG*, Paris, Flammarion, février 2017, 560 p.

Photo ci-dessous :
Alors que de nombreux services de renseignement, intérieur comme extérieur, se sont orientés vers ce que certains appellent un « fétichisme technologique », les évènements récents ont montré que le renseignement doit d'abord être une affaire d'hommes et que la technique doit venir en appoint, l'analyse et l'interprétation de l'information devant primer la collecte de données. (© Shutterstock/GlebStock)



Mais cette manipulation doit être bien ciblée. Celui qui en est l'objet doit être choisi, non seulement en fonction des renseignements qu'il est susceptible de ramener, mais aussi en fonction de sa sincérité vis-à-vis de son traitant.
Mohammed Merah va commettre plusieurs attentats en mars 2012 faisant sept victimes. Pour le juge antiterroriste Marc Trévidic, les fonctionnaires de la DCRI « ont tenté un coup particulier, risqué, mais qui à leurs yeux valait la peine, et qui aurait pu se montrer gagnant. Ils ont tenté de recruter [Merah] tout simplement. De faire une infiltration. D'en faire un agent double. Il y avait le risque bien sûr mais il y a toujours un risque dans ce genre d'opération. On marche sur le fil. C'est l'évaluation qui a foiré ! Merah a vu le coup venir, compris qu'il pouvait en profiter, et en fait s'est joué des hommes de la DCRI de Toulouse, continuant à préparer son Jihad, tout en donnant l'impression qu'il collaborait !... » (3)

La nécessité d'un cadre éthique

Traiter une source humaine doit aussi s'effectuer dans un cadre éthique. Il ne peut y avoir d'autorité et de renseignement légitimes basés sur la coercition, la contrainte, voire la violence non justifiées. La source finit tôt ou tard par se retourner contre son traitant. Deux exemples parmi d'autres illustrent cela. En 1990, un certain Pierre Didier affirmera avoir fait l'objet de manœuvres d'intimidations de la part d'un inspecteur des RG qui aurait voulu le contraindre à infiltrer la librairie « Autres Cultures » dans laquelle le pasteur Joseph Doucé, qui avait fondé le Centre du Christ libérateur, promouvait une sexualité alternative. Plus près de nous, des fonctionnaires de la Sous-direction de l'Information générale créée en 2008 après la fusion RG-DST et rattachée à la Direction de la Sécurité publique, seront soupçonnés de chantage vis-à-vis d'une jeune étudiante russe, sommée de donner des informations sur la manifestation d'opposants au projet d'aéroport de Notre-Dame-des-Landes, en échange de sa naturalisation française.
« Il importe de ne pas généraliser. Les services de renseignement ne manipulent pas leurs informateurs comme des marionnettes ; la plupart ne se laisserait pas faire ou exécuterait les ordres en dépit du bon sens. Quand bien même elle en aurait le pouvoir, la police n'a d'ailleurs souvent ni l'inclination ni la compétence requise pour manipuler ses informateurs. Supposer que telle est la règle générale reviendrait à tomber dans un manichéisme primaire et à estimer en corollaire que la police pousse systématiquement ses informateurs aux attitudes extrêmes. » (4)
Protéger les sources humaines est aussi une obligation. Dans ce but, leurs identités doivent être tenues secrètes et désignées sous un pseudonyme. Il est certain que la pérennité d'un service de renseignement passe nécessairement par la protection de ses informateurs. Révéler qui dit quoi, à qui et pourquoi à une autre autorité que celle à qui est destinée le renseignement, mettrait en danger ces sources et provoquerait un tarissement quasiment immédiat de celles-ci.

> *« Le renseignement ne s'improvise pas. Il faut du temps pour infiltrer les quartiers, connaitre les personnes à risque, savoir ce qui se prépare en coulisse. Il faut aussi du temps pour trouver le bon informateur et le traiter. »*

Ne pas les oublier est également un devoir. Les services de renseignement ont tous, à un moment donné, rencontré des correspondants qui ne veulent pas « décrocher » alors qu'ils ont vieilli et ne sont plus « dans la course ».

Pas de sources humaines sans un travail de terrain

Il n'y a pas de bons renseignements si l'on ne va pas sur le terrain et si l'on n'a pas de sources humaines... Le renseignement ne s'improvise pas. Il faut du temps pour infiltrer les quartiers, connaitre les personnes à risque, savoir ce qui se prépare en coulisse. Il faut aussi du temps pour trouver le bon informateur et le traiter.
C'est ce qu'oublient parfois les hommes politiques car les écueils évités, les mesures judicieuses prises ou les économies réalisées grâce aux services de renseignement sont difficiles, voire impossibles à quantifier.
Pourtant, il est vital pour les États d'être renseignés. C'est là une condition de survie, la garantie de leur liberté et la pérennité de leur culture. La collecte du renseignement, d'autant plus lorsqu'elle provient d'une source humaine, doit être reconnue comme une matière noble et non plus considérée comme sournoise et méprisable.

Brigitte Henri

Notes

(1) Alain Chouet, ex-directeur de la DGSE, « On a baissé la garde sur le renseignement humain », Médiapart, 20 novembre 2015.

(2) Pierre Péan, *Secret d'État*, Fayard, 1986, p. 86.

(3) Confidences du juge Trévidic sur l'affaire Merah. « Un «recrutement» a été tenté, un loupé terrible hélas », publié le 25 janvier 2013 sur le blog de Frédéric Helbert.

(4) Jean-Paul Brunet, *La police de l'ombre*, Paris, Seuil, 1990.

analyse

Par le général **Michel Masson**, directeur du renseignement militaire de 2005 à 2008.

Quels défis pour le renseignement militaire aujourd'hui ? Analyse du cas français

Malgré les apports des deux derniers livres blancs sur la défense et la sécurité nationale, le desserrage de l'étau budgétaire depuis 2015 et son avance technologique en matière d'imagerie, le bras militaire du renseignement français souffre toujours d'un grave déficit qualitatif et quantitatif en ressources humaines. C'est son principal défi et il impacte tous les autres.

En présentant de façon aussi exhaustive et fidèle que possible l'état des risques, des menaces et des opportunités dans les domaines les plus variés (politique, militaire, sécuritaire, économique, énergétique, etc.), le renseignement pris dans son acception la plus globale éclaire la décision autant qu'il précède, appuie et suit l'action. Il doit donc assurer d'une part une *veille permanente* pour évaluer l'environnement général, déceler les risques nouveaux, les premiers signes d'évolutions intéressant notre sécurité et nos intérêts. Mais, d'autre part, s'agissant de la chose militaire, il fournit à nos armées une prestation qui doit s'inscrire au cœur même et autour de la mission des forces armées, à savoir se préparer au combat et le mener. Quel que soit le type d'engagement. C'est ce que l'on appelle l'*appui renseignement aux opérations*. Ce sont les deux piliers du renseignement militaire, à la fois complémentaires et interactifs.

Le renseignement des armées

Aujourd'hui, nous célébrons le centenaire de la Grande Guerre. Comme le soulignait Charles de Gaulle : « La Grande Guerre est une révolution » (1). Elle le fut en particulier pour le renseignement militaire. Les armées françaises ont alors structuré le renseignement militaire moderne, au travers d'une organisation permanente, d'une manœuvre centralisée du renseignement, de capteurs et moyens techniques novateurs et performants entrant dans un triptyque qui sera appelé ultérieu-

Photo ci-dessus :
Image représentant le satellite militaire d'observation *Helios 2A*, en service depuis avril 2005 avec pour mission d'améliorer le renseignement militaire au profit de la France, la Belgique, l'Espagne, la Grèce et l'Italie. Si la DRM possède actuellement plusieurs systèmes satellitaires (Helios et Pléiades), ces derniers seront bientôt remplacés par ceux du programme MUSIS, qui apporteront une meilleure résolution et une augmentation importante du nombre d'images accessibles quotidiennement. (© airbusgroup)

rement : ROEM (renseignement d'origine électromagnétique), ROIM (image), ROHUM (humain). Nous reviendrons sur ces trois volets tout au long de notre développement.
Mais la structure naissante issue de la Grande Guerre ne fut pas pérennisée. Aussi, pour une véritable prise en compte du besoin de rationalisation du dispositif de renseignement des armées après le deuxième conflit mondial, il faudra attendre

Photo ci-contre :
Insigne de la brigade du renseignement d'un soldat du 2e régiment de hussards, stationné à Haguenau en Alsace et appartenant au Commandement du renseignement. Spécialisée dans le renseignement, l'infiltration et le camouflage notamment, la mission de ces soldats – susceptibles d'être déployés sur court préavis – consiste à renseigner sur des objectifs à haute valeur ajoutée.
(© Claude Truong-Ngoc)

la prise en compte des enseignements tirés de la première guerre du Golfe. Ceux-ci avaient mis en évidence l'inadaptation de notre outil de renseignement militaire et notre dépendance à l'égard des Américains. Pierre Joxe, le locataire de l'Hôtel de Brienne, fit mettre en œuvre par les militaires les préconisations d'une étude faite à l'initiative de son prédécesseur, Jean-Pierre Chevènement. Il fit fédérer certains moyens au sein d'un organisme interarmées, malgré les réticences (et c'est un euphémisme) des chefs militaires. La Direction du renseignement militaire (DRM) fut ainsi créée par le décret du 16 juin 1992, fusionnant des organismes et des cellules qui relevaient jusque-là de chacune des armées et du Secrétariat général à la Défense (SGDN).
Sous l'autorité du Président de la République, chef des armées – et sans préjudice des responsabilités du ministre de la Défense (2) – le chef d'état-major des armées (CEMA), conseiller du gouvernement, est responsable de l'emploi des forces et assure le commandement des opérations. Il assure la direction générale de la recherche et de l'exploitation du renseignement militaire et a autorité sur la DRM dont le rôle est double, comme indiqué en remarque liminaire. La DRM doit tout d'abord « connaître », éclairer la prise de décision : elle fournit aux autorités politiques et militaires le renseignement de situation nécessaire à l'exercice de leurs responsabilités permanentes. Elle participe ainsi, comme les autres services de la communauté nationale du renseignement, à la veille stratégique. C'est la veille permanente. Mais son rôle primordial est d'appuyer les forces en opérations. Par le renseignement qu'elle produit, la DRM apporte un appui à la planification et à la conduite des opérations au niveau stratégique et contribue à l'orientation de la manœuvre à tous les niveaux : du stratégique (le Président et le CEMA) au tactique (les unités sur le terrain), en passant par l'opératif (les commandements de théâtre).
La priorité absolue est donnée à l'appui aux opérations par la DRM, ce qui justifie qu'elle assure le rôle de « tête de chaîne » de la fonction interarmées du renseignement d'intérêt militaire.

> *« La DRM participe, comme les autres services de la communauté nationale du renseignement, à la veille stratégique. C'est la veille permanente. Mais son rôle primordial est d'appuyer les forces en opérations. »*

Car toutes les forces, toutes les composantes du dispositif interarmées, toutes les unités – spécialisées ou non, nous y reviendrons – doivent participer à la collecte du renseignement.

Qu'est-ce que le RIM ?

On vient de voir apparaître une expression nuancée par rapport au terme plus brut de « renseignement militaire » : le « *renseignement d'intérêt militaire* ». Le « RIM » concerne à la fois :
• le renseignement militaire proprement dit, c'est-à-dire concernant les forces vives (ou, si l'on préfère, tout ce qui concerne les forces ennemies, menaçantes ou potentiellement dangereuses) : leurs organisations, leurs capacités, leurs doctrines, leurs ordres de bataille, leurs crédibilités militaires...
• le renseignement concernant l'environnement (tous les domaines de l'espace physique dans lequel sont engagées les forces et toutes les particularités du milieu humain dans lesquelles elles sont appelées à évoluer). La difficulté concernant ce sujet est qu'il est en constante évolution, dans ses composantes sociologiques, économiques, religieuses, ses infrastructures, etc.
Le RIM s'intéresse donc aux forces vives et à l'environnement qui ressortissent strictement au seul domaine d'intérêt militaire, c'est-à-dire ayant ou pouvant avoir des conséquences sur nos forces ou nos intérêts nationaux. Mais cela devient plus subtil dans le cadre de certaines missions.

Les menaces, des conflits symétriques aux conflits asymétriques

Les menaces s'inscrivent à la fois dans la perspective de conflits dits « *symétriques* » et « *asymétriques* ».
• Les conflits symétriques se caractérisent par la recherche de la supériorité par des adversaires qui s'opposent avec des struc-

tures et des doctrines semblables suivant les mêmes lois. À titre d'exemple, la remontée en puissance de l'outil militaire de la Russie est un sujet d'intérêt fort, à la lumière des événements récents et actuels en Ukraine et en Syrie. *Ipso facto* la DRM s'en préoccupe, mais n'a pas attendu ces événements. Car le renseignement, y compris militaire, s'inscrit dans le temps long.

• Les conflits sont dits « asymétriques » lorsque deux adversaires s'affrontent dans des espaces différents pour rendre illégitime ou inefficace l'action de l'autre. La guerre psychologique, la maîtrise de l'information et leur corollaire, les actions agressives dans le cyberespace, entrent dans ces formes d'actions. Elles ne sont pas les seules. Mais ce sont là de nouveaux champs à explorer et à surveiller pour ne pas se laisser déborder par l'ennemi. Les modalités et péripéties de la prise de contrôle de la Crimée par les Russes en sont un bon exemple.

De même, les liens entre l'action guerrière et les différentes formes de criminalité sont devenus plus complexes, mais de plus en plus convergents et difficiles à démêler. Ce fut le cas dans les Balkans à la naissance de la DRM ; on sait bien aussi

> *« La France est l'une des rares nations à disposer de l'ensemble des capacités qui fondent un système de renseignement global et cohérent, assorties cependant de limitations qu'il ne faut pas se cacher. »*

que les groupes armés qui opèrent dans le Sahel sont liés à tous les trafics qui utilisent cette portion de continent pour leurs transits. Pour ne citer que ces deux théâtres.

Par ailleurs, les actions militaires s'inscrivent désormais le plus souvent dans une perspective multinationale. L'appui renseignement apporté à la multinationalité peut prendre la forme d'échanges bilatéraux ou de mise en commun. C'est une exigence de terrain, mais qui contribue aussi à notre crédibilité et qui peut constituer un élément d'une stratégie d'influence. La France est d'autant mieux armée aujourd'hui pour y répondre qu'elle est l'une des rares nations à disposer de l'ensemble des capacités qui fondent un système de renseignement global et cohérent, assorties cependant de limitations qu'il ne faut pas se cacher.

Pour faire la guerre, le renseignement militaire ne suffit donc plus. Il n'en continue pas moins à être le cœur d'expertise de la DRM, ce qui fait que le renseignement d'environnement devra le plus souvent être recueilli auprès d'autres services, d'autres organismes, et suppose une indispensable coopération avec ceux-ci. C'est déjà le cas sur les théâtres d'opérations de nos forces : des cellules de coordination interservices furent mises en place sur quatre théâtres différents dès 2006. Ce dispositif a été pérennisé sur les théâtres actuels, mais c'est bien entendu également l'un des défis qui se posent au Coordonnateur du renseignement [voir également p. 13 de ces *Grands Dossiers*, NdlR] – poste national créé en cohérence avec les conclusions du Livre blanc de 2008 – eu égard au fait que les menaces n'ont pas de frontières, se prolongent et se projettent parfois avec violence jusque sur notre propre territoire.

Les difficultés à surmonter

Parmi les défis qui attendent le renseignement militaire, il y a d'abord ceux qui sont communs à l'ensemble des services : la profusion des données et de l'information disponibles, la maîtrise des flux associés et l'impératif de rapidité de distribution du renseignement ne sont pas les moindres. On se situe ici au sein de la problématique générale de « la maîtrise de l'information ». Il y a bien entendu à la clef des implications technologiques de haut niveau qui impactent l'ensemble de la communauté du renseignement. En France, c'est la Direction générale de la sécurité extérieure (DGSE) qui a pris de l'avance sur les autres services dans ce domaine. Elle récolte ainsi le fruit d'une politique volontariste et décomplexée menée depuis plusieurs années, conjointement à l'avantage budgétaire que lui ont attribué les dernières lois de programmation. Il est dommage, que sur ces sujets techniques sur lesquels se jouent l'avenir, le Coordonnateur ne soit pas investi de plus de pouvoir et de moyens.

Photo ci-dessus :
Le *Dupuy-de-Lôme*, en service depuis 2006, collecte du renseignement au profit de la Direction du renseignement militaire. Truffé d'électronique de pointe – c'est l'un des plus modernes de sa catégorie –, il permet notamment de recueillir des données concernant le terrorisme au plus près des foyers principaux de cette menace, car il a le droit de rester dans les eaux internationales et jouit d'une autonomie en mer d'au moins 30 jours. (© Jean-Michel Roche)

Le Cyber constitue également un défi majeur. La France du secteur public se numérise pas à pas, mais a pris en compte avec retard les enjeux sécuritaires dans l'espace cybernétique, malgré un tissu industriel national (de souveraineté ou non) performant dans ce secteur : le « Pacte Défense Cyber » (3) (plan développant les mesures à mettre en œuvre dans tous les domaines de la cyberdéfense) ne date que de... 2014 ! Il n'en demeure pas moins que la menace est d'importance : dans la logique des opérations modernes, le fait militaire se positionne de plus en plus au cœur du combat numérisé, dans le cyberespace et dans l'infosphère. Le RIM doit permettre à la fois de s'en protéger (cybersécurité) et de l'exploiter (cyber-renseignement), mais il doit aussi participer aux mesures actives (cyberguerre).

Enfin, il y a les défis propres au RIM. Le premier de ceux-ci, mais non le moindre, est la multiplication des engagements de

Pour aller plus loin

Voir les articles consacrés au renseignement dans *Défense et Sécurité internationale* hors-série nos 37 et 43, respectivement août-septembre 2014 et 2015, avec notamment deux interviews du général Christophe Gomart (voir ci-dessous), ainsi que des articles consacrés au GEOINT, au renseignement en sources ouvertes, à la réforme du renseignement en général et de la DRM en particulier.

Photo ci-contre :
Le général Christophe Gomart, directeur du renseignement militaire depuis juin 2013. En février 2017, ce dernier déclarait que l'enjeu de la transformation de la DRM était de « conserver un temps d'avance sur nos adversaires pour garantir au chef d'état-major des armées une autonomie d'appréciation de situation renforcée et fournir aux forces déployées un renseignement directement exploitable pour les opérations ». (© Claude Truong-Ngoc)

la France : les opérations extérieures se succèdent, se superposent les unes aux autres, faisant croître le nombre de cellules de renseignement qui fonctionnent 24 heures sur 24. Ceci sans compter la dégradation du format et des capacités des armées qui s'est accélérée en 2008 (l'année de l'avant-dernier Livre blanc !), avec des réorganisations faites avec le seul souci d'économies comptables au travers de la Loi organique relative aux lois de finances (LOLF) et de la Révision générale des politiques publiques (RGPP), sans aucun respect de la rationalité opérationnelle et des exigences sur le terrain. Si la DRM fut moins impactée, le renseignement en opérations, qui repose en grande partie sur les forces déployées, en a tout de même souffert. Or, l'autonomie d'appréciation de situation que requièrent les deux derniers Livres blancs (celui de 2013 ayant entériné les conclusions/décisions de celui de 2008 pour le renseignement et la fonction stratégique « Anticipation & Connaissance ») suppose des moyens qui n'existent malheureusement pas en proportion des forces engagées et des théâtres. Nos forces armées sont sollicitées très au-delà de leurs capacités, ce qui fait que celles dédiées à la recherche comme à l'exploitation du RIM sont aujourd'hui globalement insuffisantes.

À titre anecdotique, dans une interview télévisée récente (4), le directeur du renseignement militaire, le général de corps d'armée Christophe Gomart, répondit malicieusement à son interlocuteur qui lui demandait ce que regardaient précisément à ce moment-là « les yeux de la France » : « ... beaucoup de choses... le monde entier ! ». Ce que ne dira pas le général Gomart (tout au moins à l'antenne), c'est que si les capteurs

nationaux permettent en théorie de regarder le monde entier, c'est une autre affaire que de disposer des spécialistes en nombre suffisant pour exploiter rationnellement cette manne.

Un deuxième défi propre au RIM est lié à l'élargissement du périmètre des missions des armées et à l'extension du champ du RIM qui en découle, à l'échelon national comme international (diversification des missions : maintien et rétablissement de la paix ; opérations humanitaires ; interventions de vive force en autonome ou en multinational ; sécurisation du territoire national...), totalement lié au défi précédent. Dernier en date, le dispositif « Sentinelle », outre la charge supplémentaire créée par la mobilisation permanente des forces déployées, pose directement la double question du rôle de la fonction RIM dans ce type d'engagement et de la coordination renseignement avec le ministère de l'Intérieur au profit des moyens militaires engagés.

Troisième défi spécifique : les capteurs. Il s'agit de donner toute son importance à la manœuvre de la recherche multi-capteurs**,** en s'appuyant sur ses trois principes structurants **:** la synergie

> *« Nos forces armées sont sollicitées très au-delà de leurs capacités, ce qui fait que celles dédiées à la recherche comme à l'exploitation du RIM sont aujourd'hui globalement insuffisantes. »*

(obtenue par la complémentarité des moyens) ; la modularité (réponse à l'adaptation aux besoins, selon la nature de l'engagement) ; la flexibilité (rattachement à tout type de commandement opérationnel, en national comme en multinational). Ce sujet de la modernisation et de la complémentarité des capteurs est abordé plus bas.

Le dernier défi particulier lié à la fonction RIM est aussi le principal : la ressource humaine. La DRM à elle seule compte aujourd'hui un peu plus de 1750 personnes (dont environ 20 % de civils, tous statuts confondus). Il n'y a pas d'augmentation chiffrée prévue par les textes au profit de la seule DRM. Les efforts chiffrés rendus publics concernent le « cyber », ce qui n'est pas dans la responsabilité de la DRM (hormis le « cyber-Rens' »). Par ailleurs, on peut chiffrer (ce n'est qu'une estimation, sans valeur contractuelle ni organisationnelle) à environ 8000 militaires au total (dont plus de 1000 à la DGSE) les effectifs qui œuvrent au profit du renseignement dans l'ensemble des forces. Mais certaines spécialités sensibles et critiques souffrent en effet de déficits criants en effectifs. Cela a toujours été souligné par les directeurs successifs de la DRM et mis en exergue par la Délégation parlementaire au Renseignement (5). Les performances d'un service, sa crédibilité ne valent que par les hommes et les femmes qui le composent. La seule technique ne suffit pas : elle n'est qu'une valeur ajoutée aux qualités et capacités humaines qui sont essentielles.

Les capteurs

Les capteurs sont directement associés aux ambitions et aux défis du RIM. Nous ne les passerons pas en revue faute de place. Ils sont la « face visible » de cette fonction et occupent – sans doute trop – le discours politique et médiatique qui entretient un certain « despotisme du capteur », nourri par le complexe politico-industriel. Nous nous bornerons à les caractériser par champs d'action :

• *Capteurs stratégiques :* ils sont actionnés directement par la DRM via des centres dédiés (ROIM, ROEM, ROHUM). Dans l'espace, il s'agit de satellites (satellites d'observation : aujourd'hui les systèmes optiques français Hélios et Pléiades – complétés par un échange capacitaire émanant des satellites radar allemands et italiens –, qui devraient être remplacés par le système européen MUSIS (6) dès 2018 ; est à venir aussi, le système satellitaire ROEM/SIGINT (7) CERES (8), pour capter, identifier, localiser depuis l'espace puis caractériser les signatures des systèmes d'armes et, en particulier, ceux de tous les radars, là où les autres capteurs ne peuvent aller). Sur mer, nous disposons d'un bâtiment d'écoutes très perfectionné, le MINREM (9) *Dupuy de Lôme*. Sur terre, nous utilisons un réseau mondial de stations d'écoute (10), de plus en plus mutualisé avec la DGSE.

• *Capteurs de théâtre (opératifs et tactiques) :* ce sont les moyens mis en œuvre par chacune des armées. Ils sont nombreux, et concourent tous ensemble à la collecte, la « manœuvre du RIM », sous l'autorité des commandants de théâtre. La DRM en récolte également les fruits.

On a beaucoup parlé des drones. La France a depuis longtemps fait le choix de ne pas se doter de drones stratégiques (haute altitude, longue endurance : HALE (11)). En matière de drones de théâtre (moyenne altitude, longue endurance : MALE), après moult tergiversations et un long feuilleton à rebondissements, la France a choisi l'achat sur étagères du MQ-9 « Reaper » américain (General Atomics), avec une « francisation » *a minima*. La rançon de ce choix fait dans l'urgence, faute de réflexion en amont, est que nous nous trouvons en partie dans la main des Américains pour cette composante, ce qui est un pied de nez à notre autonomie stratégique, en attendant le programme en coopération internationale inscrit dans le plan de l'Organisme conjoint de coopération en matière d'armement.

N'oublions par le renseignement humain (ROHUM) : les armées disposent chacune d'unités spécialisées dans la recherche du renseignement humain, de façon confidentielle (mais non clandestine, la clandestinité restant propre à la DGSE). C'est en particulier le cas des unités des forces spéciales, ou d'autres unités dédiées. De façon ouverte, c'est aussi la mission permanente des attachés de défense, depuis leur généralisation au sein des ambassades, à la fin du XIX^{e} siècle (12). La recherche humaine est un complément indispensable à tous les modes de recherche technique visés *supra*.

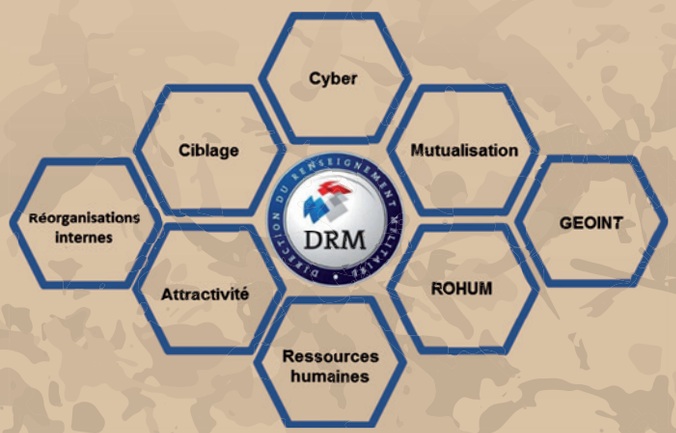
En tout état de cause, la DRM reste la « tête de chaîne » du dispositif d'orientation de la recherche, d'exploitation et de diffusion du RIM, tant au profit du niveau stratégique (Présidence, ministre, CEMA), qu'opératif (commandants de théâtre et de composantes) et tactique (les unités sur le terrain).

Quels enjeux pour la France ?

Le positionnement de la France à l'international, la préservation des intérêts nationaux et la protection de nos concitoyens doivent pouvoir s'appuyer sur un renseignement fiable et performant. Ce fut laborieux, mais les obstacles culturels et idéologiques en France vis-à-vis du renseignement semblent sur ce point derrière nous. Au premier rang des préoccupations actuelles, il y a deux écueils majeurs : le premier, c'est la réalisation d'une coordination-coopération plus poussée entre toutes les composantes de la communauté nationale du renseignement, sur les plans tant technique et opérationnel qu'humain. Si un grand pas a été fait en 2008 en ce sens, la réforme n'a pas été au bout de ses ambitions. Le second est propre au RIM. Au sein des armées, la ressource humaine (en termes de quantité, qualité et diversité) dédiée à cette fonction pâtit de l'héritage à la fois des incohérences et de l'aveuglement des politiques publiques récentes – en dépit des priorités affichées et déclamées – tout comme du désintérêt de nos chefs militaires par le passé. Ce n'est qu'au prix de mesures adaptées sur ces deux points majeurs que nous pourrons réduire encore l'incertitude face à la surprise stratégique et contribuer à dissiper un peu plus « le brouillard de la guerre » (13).

Michel Masson

Transformation dans le renseignement militaire



Dans le cadre de la réforme des armées « Cap 2020 », la DRM a entamé un processus de transformation selon 9 axes : devenir l'organisme référent dans le domaine du renseignement géospatial (GEOINT), mutualiser les capteurs avec les autres services de renseignement, renforcer le rôle de la DRM dans le processus de ciblage, développer une véritable capacité d'engagement et de pilotage opérationnel de la recherche humaine, instituer un pôle d'excellence en matière de renseignement d'origine cyber, réorganiser et accélérer le cycle du renseignement en interne, améliorer le recrutement et le déroulé des carrières, renforcer son attractivité grâce à la création de l'"Intelligence Campus", optimiser la coordination entre les différents organismes de renseignement des armées au profit des opérations. (© EMA/Ministère de la Défense)

Notes

(1) Charles de Gaulle, *La France et son armée*, (1re éd., Plon, 1938), Paris, Perrin, coll. « Tempus », 2016.

(2) Décret n° 2013-816 du 12 septembre 2013 relatif aux attributions du ministre de la Défense et du chef d'état-major des armées.

(3) « Pacte Défense Cyber : 50 mesures pour changer d'échelle », Ministère de la Défense/DICOD, 2014.

(4) Émission « Complément d'enquête » diffusée sur la chaîne nationale France 2 le 19 janvier 2017.

(5) Rapport relatif à l'activité de la Délégation parlementaire au Renseignement pour l'année 2014 (chap. V, p. 93) (http://www.assemblee-nationale.fr/14/rap-off/i2482.asp).

(6) *MUltinational Space-based Imaging System*, dont la France développe la composante spatiale optique.

(7) SIGINT pour SIGnal INTelligence, c'est-à-dire la captation des signaux électromagnétiques émis par les systèmes d'armes.

(8) Capacité de renseignement électronique spatiale.

(9) Moyen interarmées naval de recherche électromagnétique.

(10) Pour le ROEM conversationnel seulement : c'est-à-dire les communications, ou COMINT (COMmunications INTelligence).

(11) Exemple : le drone américain RQ-4 Global Hawk. D'une envergure de 40 mètres, il peut voler jusqu'à 20 000 mètres d'altitude pendant une trentaine d'heures à une vitesse de 650 km/h. Il est propulsé par un turboréacteur .

(12) En France, dès la guerre de Trente ans, le duc de Richelieu missionnait des officiers à l'étranger pour établir une liaison avec les forces alliées, surveiller leurs développements militaires et récolter des informations.

(13) Cette expression du célèbre théoricien militaire prussien Carl von Clausewitz (1780-1831) sert à caractériser toute l'incertitude qui entoure une situation de guerre. Dans son célèbre ouvrage *De la guerre, Clausewitz dit cependant que le renseignement ne sert à rien, et que la plupart du temps... il est faux !*

analyse

Par **Éric Melchiori**, ancien officier supérieur DPSD (Direction de la protection et de la sécurité de la Défense).

Quels enjeux pour la Contre-Ingérence Défense ?

Analyse du cas français

Les forces armées, tous les organismes de la Défense, ainsi que l'industrie de Défense peuvent faire l'objet d'actes hostiles de la part d'organisations ou d'individus qui cherchent à porter atteinte aux intérêts de la Défense par d'autres voies que la confrontation militaire : ces actes sont alors qualifiés d'ingérences. Afin de les prévenir ou de les neutraliser, il convient de mettre en œuvre des stratégies et moyens de contre-ingérence.

Photo ci-dessus : Le 23 mai 2016, des militaires français et britanniques participent à un exercice à Fort Béar, dans les Pyrénées-Orientales. Un an plus tôt, un projet d'attentat contre cette base d'entrainement de l'armée de terre avait été déjoué après l'arrestation de trois jeunes se revendiquant du groupe État islamique – dont un militaire réformé connaissant le site. (© AFP/ Raymond Roig)

Dans le domaine de la Défense nationale, une ingérence est une action qui vise à porter atteinte aux intérêts fondamentaux de la nation, à la sécurité des forces armées, aux zones protégées intéressant la Défense nationale et au secret de Défense au sein des forces armées ou de l'industrie de Défense.

Renseignement et Contre-Ingérence

La sécurité en matière de renseignement est l'état caractérisé par la protection satisfaisante des personnes, des informations, des matériels et des installations sensibles contre le terrorisme, l'espionnage, le sabotage, la subversion et le crime organisé.

La contre-ingérence (CI) a pour objectif de déceler et de neutraliser toute menace contre la sécurité résultant des activités des services de renseignement (SR), d'organisations ou d'agents. La CI repose sur deux types d'actions permanentes complémentaires :

- l'acquisition du renseignement de sécurité,
- l'application de mesures de protection qui ont pour objet d'assurer et de maintenir au meilleur niveau la sécurité des forces armées.

La CI, par ses modes d'action, de recherche et de protection essentiellement préventifs, se distingue du contre-espionnage (CE) dont l'objectif est plus offensif, puisqu'il s'agit alors de neutraliser et de détruire les moyens de renseignement adverses et de conduire des actions de déception.

L'action de la Direction du Renseignement et de la Sécurité de la Défense (DRSD, voir encadré) s'exerce donc de manière essentiellement préventive et participe à la neutralisation de la menace. Les autres SR et la Gendarmerie nationale, dans le cadre de leurs missions spécifiques, contribuent à l'acquisition du renseignement de sécurité intéressant la Défense nationale. La DRSD établit donc les liaisons nécessaires avec les autres services du ministère de la Défense (notamment la Gendarmerie nationale) et des autres ministères concourant à la sécurité de Défense, et les services homologues alliés en opérations extérieures et à l'occasion des exercices interalliés.

> *« La menace doit être constamment réévaluée et faire l'objet d'une analyse prospective qui permette d'en anticiper au mieux les modalités d'action, le point d'application et le moment d'exécution. »*

La menace TESSCo : terrorisme, espionnage, subversion, sabotage, et criminalité organisée

Une menace est un projet conçu et organisé par toute organisation ou individu pour mener à bien une ingérence. Elle est caractérisée par ses auteurs qu'il convient d'identifier, son vecteur qu'il faut déceler et ses cibles qu'il faut protéger.

Les auteurs de la menace sont principalement :

- des SR étrangers,
- des organisations terroristes,
- des organisations subversives,
- des organisations criminelles,
- des individus animés par une volonté terroriste, subversive ou criminelle, mais dont les intentions ne sont pas clairement identifiées.

Les vecteurs de la menace sont les moyens par lesquels les auteurs de la menace accomplissent leur dessein. Ils relèvent des types d'activités identifiées sous l'acronyme TESSCo. Cette menace peut, pour chacune de ces activités, également revêtir la forme d'attaques des systèmes d'information et de communication.

- **Le terrorisme** est l'emploi illégal, ou la menace d'emploi illégal, de la force ou de la violence contre les personnes ou les biens, afin de contraindre ou d'intimider les gouvernements ou les sociétés dans le but d'atteindre des objectifs politiques, religieux ou idéologiques.
- **L'espionnage** consiste en la recherche d'informations par des moyens secrets ou illicites dans un but de renseignement. Il s'exerce indifféremment au sein de la Défense et dans l'industrie de Défense.
- **Le sabotage** est une destruction, une perturbation ou une mise hors service intentionnelle d'un équipement, d'un matériel ou d'une installation.
- **La subversion** est une action ayant pour objectif d'affaiblir le moral des militaires et du personnel civil de la Défense ou de l'industrie de Défense, de compromettre leur loyauté ou leur probité en vue de porter atteinte à la Défense.
- **Le crime organisé** recouvre les actions d'organisations criminelles, structurées en réseaux, sous la direction d'un ou plusieurs chefs, qui comprennent plusieurs unités subordonnées réparties sur un large territoire. Leur but est de se procurer illégalement des moyens et des fonds afin d'acquérir du pouvoir, en violation des lois démocratiques du pays où elles opèrent.

Cette classification TESSCo ne doit cependant pas laisser penser que les menaces sont uniquement sectorielles : une organisation peut mener des actions d'ingérence sous de multiples formes à l'encontre d'organismes relevant de domaines variés (formations militaires, industrie de Défense, individus, moyens de protection ou moyens de communication). L'organisation du renseignement de sécurité et l'analyse des mesures de protection doivent prendre en compte ce caractère protéiforme et global de la menace.

La menace peut être potentielle, c'est-à-dire découlant des possibilités théoriques de l'adversaire, ou effective, c'est-à-dire liée à la mise en œuvre de ces possibilités. Chaque menace peut être analysée et évaluée à partir de renseignements de documentation ou de renseignements de situation.

Cependant, la menace étant permanente, elle nécessite une capacité de riposte également permanente. Aussi, la menace doit être constamment réévaluée et faire l'objet d'une analyse prospective qui permette d'en anticiper au mieux les modalités d'action, le point d'application et le moment d'exécution.

Face à ces menaces, la Défense présente un certain nombre de vulnérabilités qui sont soit des faiblesses humaines, soit des faiblesses dans la sécurité des forces, des installations ou des réseaux. L'analyse des vulnérabilités permet d'identifier les cibles potentielles des auteurs de la

La DRSD

La Direction du Renseignement et de la Sécurité de la Défense (DRSD) est le service de renseignement dont dispose le ministre de la Défense pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles*. Héritière de la Direction de la Sécurité Militaire créée en 1961, la DRSD succède depuis octobre 2016 à la Direction de la Protection et de la Sécurité de la Défense créée en 1981.

Service de contre-ingérence de 1200 personnels majoritairement militaires (20 % civils), les missions principales de la DRSD sont la protection des forces françaises en opérations, la protection du secret de la défense nationale, la sécurité économique et la surveillance du commerce des armes. **E. M.**

*Code de la défense, article D3126-5.

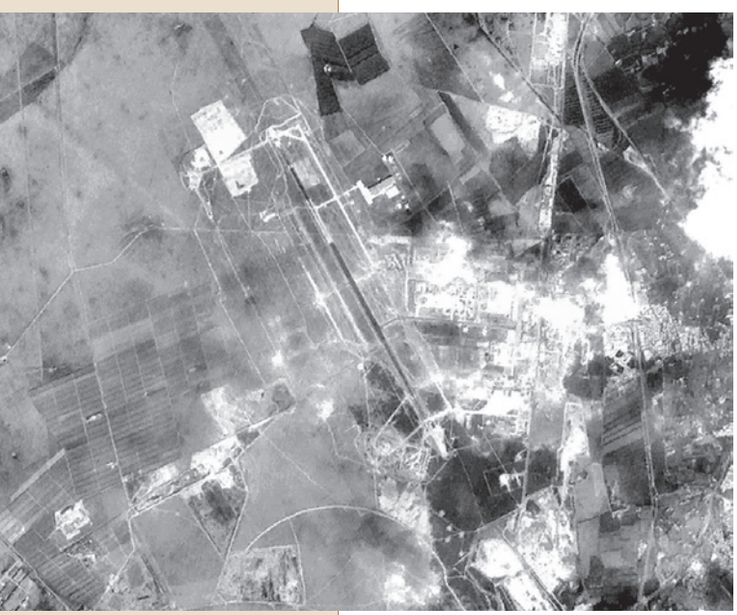


Photo ci-dessus :
Photo satellite de la base aérienne 125 Istres-Le Tubé appartenant à l'armée de l'air française et accueillant notamment des unités des Forces aériennes stratégiques (en charge de l'emploi des armes nucléaires).
Les mesures physiques de protection mises en place par la DRSD ont pour objectif de garantir l'intégrité des sites relevant de la Défense. En raison des contraintes qu'impose une telle garantie, l'intégrité totale, quelle que soit la menace envisagée, n'est recherchée que pour un nombre limité de points ou réseaux très sensibles. (DR)

menace. Ces cibles peuvent être des personnes, des informations, des installations ou des matériels.
La confrontation des menaces et des vulnérabilités permet de déterminer les risques encourus par la Défense. La sécurité ne pouvant jamais être atteinte de manière totale face à toutes les menaces, il appartient au commandement militaire de définir le niveau de risque consenti.

Le renseignement de sécurité

Un renseignement de sécurité est un renseignement sur la nature, les possibilités et les intentions d'organisations ou d'individus hostiles qui sont ou pourraient être engagés dans des activités terroristes, d'espionnage, de sabotage, de subversion ou de crime organisé. Le renseignement de sécurité est nécessaire au commandement militaire pour assurer la sécurité des personnes, des informations, des matériels, des installations sensibles et des systèmes d'information dans le domaine de la Défense ou dans celui de l'industrie de Défense. Transmis sous une forme exploitable et adaptée, il a pour objet d'expliquer un fait, de déterminer une menace ou de mettre en évidence une intention.
À la base du renseignement de sécurité, il y a des informations. Une information est la relation d'un fait ou d'une observation, elle est une donnée recueillie par un capteur.
L'information est ensuite exploitée pour devenir un renseignement. Ce dernier est une donnée élaborée à partir d'une ou plusieurs informations recherchées, recueillies, validées, corrélées et replacées dans un contexte, puis diffusée sous une forme exploitable et adaptée aux besoins d'une autorité.
Le renseignement de sécurité porte sur :
• des personnes physiques ou morales, auteurs, victimes ou témoins de menées ou d'atteintes à la sécurité de la Défense,
• des faits en rapport avec la sécurité de la Défense, qui peuvent concerner des personnes, des lieux ou des installations.
Les besoins en renseignements de sécurité sont satisfaits à l'issue du processus appelé « cycle du renseignement » qui comprend quatre étapes : l'orientation, la recherche, l'exploitation et la diffusion.
Neuf principes régissent la production du renseignement et l'organisation de la chaine du renseignement :
• **La centralisation** : le renseignement doit être contrôlé de manière centralisée pour éviter toute répétition injustifiée et contreproductive, pour un concours mutuel et un emploi efficient des ressources.
• **La rapidité** : l'information ou le renseignement le plus exact est sans intérêt s'il arrive trop tard à destination. L'organisation des sources et des services doit donc être capable de mesurer et de rendre compte, sans délai, de tout changement de situation.
• **L'exploitation systématique** : les informations collectées par des sources ou des organismes de recherche doivent être exploitées de manière méthodique et minutieuse.
• **La séparation entre recherche et exploitation** : les personnels en charge de l'exploitation du renseignement doivent être différents de ceux qui le recherchent afin de proscrire tout biais dans le cycle du renseignement.
• **L'objectivité** : toute tentation de faire correspondre le renseignement à des idées préconçues doit être rejetée.
• **L'accessibilité** : toute information ou renseignement pertinent doit être facilement accessible par ceux qui en assurent l'exploitation et par les utilisateurs.
• **La réactivité** : l'exploitation du renseignement doit, en tous temps et toutes circonstances, satisfaire rapidement les demandes des autorités.
• **La protection des sources** : les sources d'information doivent être parfaitement protégées.
• **La mise à jour continuelle** : le renseignement doit être actualisé de manière systématique et éventuellement révisé de toute nouvelle information.

La contre-ingérence en opérations extérieures

Menaces et risques relevant de la CI

Toute force militaire engagée dans la durée dans une opération de maitrise de la violence à l'étranger, dans un cadre national ou multinational, est directement exposée à tout ou partie des menaces non militaires couvertes par le domaine de la CI.
Ces menaces s'exercent à des degrés d'intensité divers selon le contexte local. Elles constituent un risque permanent pour la sécurité de la force et sont susceptibles d'entamer son potentiel opérationnel. Elles peuvent prendre les formes TESSCo suivantes :
• menace *terroriste* qui, en dehors d'une situation de conflit ouvert, reste un moyen d'action et de pression efficace dans un rapport de force du faible au fort ;
• *espionnage*, systématiquement pratiqué par les SR locaux et facilité par le recours aux ressortissants du pays pour la sous-traitance de nombreuses tâches au sein de la force ;
• actions de *sabotage*, qui peuvent être facilitées par l'instauration d'un certain relâchement dans l'application des mesures de sécurité et par une bonne connaissance du dispositif et des infrastructures par l'adversaire local ;
• *subversion*, avec pour corollaire les atteintes au moral de la force qui en accroissent la vulnérabilité ;
• *crime organisé*, dont les divers trafics (drogue, prostitution, matériels ou produits de contrebande, armes) sollicitent directement les membres de la force et peuvent en affaiblir le potentiel, voire porter atteinte à sa crédibilité.

> *« La recherche des informations dans les domaines du terrorisme et de la criminalité organisée nécessite une étroite coopération entre tous les services concernés. »*

La protection des bâtiments de la Marine nationale en escale à l'étranger est un cas particulier de la protection des forces en opérations extérieures (OPEX).

Rôle de la CI dans la protection de la force

Dans ce contexte, la protection de la force revêt une importance capitale et nécessite la réalisation d'un état de sécurité minimum au regard des différentes menaces. En appui d'une force en opérations, l'action de CI se concentre donc essentiellement sur :

- la recherche des renseignements permettant d'identifier les différentes menaces TESSCo et d'en évaluer en permanence le niveau d'intensité ;
- le conseil au commandement concernant les mesures de sécurité à prendre pour réaliser un état de protection minimum de la force face à ces menaces ;
- le contrôle, à la demande du commandement, de la mise en œuvre des mesures de sécurité qu'il a édictées.

La recherche des informations dans les domaines du terrorisme et de la criminalité organisée nécessite une étroite coopération entre tous les services concernés.

Mise en œuvre de la CI

Lorsque des forces françaises sont engagées en OPEX, la fonction CI est organisée selon deux schémas :

- dans le cadre d'une opération nationale, elle est chargée de fournir des experts à la chaine de commandement ;
- dans le cadre d'une opération multinationale, elle doit en premier lieu armer la chaine de commandement des éléments français (COMELEF), en particulier auprès de l'autorité militaire « REPFRANCE » du théâtre et des commandants des forces françaises et, en second lieu, participer à la chaine multinationale de CI. Dans ce dernier cas, en tant que nation contributrice, elle peut fournir du personnel inséré dans la chaine de commandement interallié (UE, OTAN) ou, en tant que nation-cadre, fournir le noyau clef de cette structure.

Chaine nationale de CI

La fonction CI est alors assurée par des équipes DRSD adaptées aux différents niveaux de commandement des éléments français, auxquels elles apportent leur concours dans l'exercice de leurs responsabilités en matière de sécurité et de protection de la force. La prévôté, les unités de Gendarmerie et les forces de police internationale complètent ce dispositif CI.

Sur un théâtre d'opérations, le dispositif DRSD est déployé en cohérence avec celui des forces françaises engagées. Le chef de détachement DRSD est placé auprès du REPFRANCE ou du COMELEF dont il est l'interlocuteur privilégié dans le domaine de la CI dans sa zone d'intérêt. Les antennes DRSD sont adaptées, autant que de besoin, aux différents niveaux de commandement des forces françaises (division, brigade, groupement tactique).

Le volume des éléments DRSD à engager dans une opération est étudié et décidé par l'État-major des armées (EMA) en liaison avec la DRSD dès la phase de planification dite « à chaud ». Il reste susceptible d'adaptations ultérieures en fonction de l'évolution de la situation.

L'emploi de la DRSD en opérations fait l'objet d'une directive particulière de l'EMA. Tout engagement extérieur de la DRSD fait l'objet d'un ordre d'opérations remis au commandement d'emploi sur le théâtre d'opérations.

Chaine multinationale de CI

La fonction CI au sein d'une force multinationale est déclinée depuis le niveau opératif jusqu'aux états-majors de niveau division ou brigade.

La recherche de renseignements dans les domaines du terrorisme et de la criminalité organisée se fait en liaison avec les services de police et les SR locaux lorsque ceux-ci sont encore en mesure de remplir leurs missions régaliennes et présentent des garanties suffisantes, ainsi qu'avec les services de police internationaux (Europol, Interpol).

La fonction CI est assurée par des cellules spécialisées identifiées CJ2X (*Combined Joint 2 Counter-intelligence* – CI interarmées interalliés) au sein des bureaux renseignement états-majors dont elles sont parties intégrantes.

Dans le cadre d'un engagement au sein de l'OTAN, la chaine CI dépend directement de SHAPE (1), qui reçoit toutes les synthèses de renseignement de CI et oriente son action.

Les personnels DRSD (2) insérés au sein des cellules CJ2X sont placés pour emploi au sein d'états-majors de l'OTAN et n'ont alors plus de lien hiérarchique et fonctionnel avec la DRSD.

L'efficacité de la CI en OPEX repose sur l'établissement et le maintien de liaisons efficaces avec :

- les différents SR nationaux présents sur le théâtre,
- les services CI des autres nations contributrices de la force,
- les forces armées et services locaux (Police, Gendarmerie, Douanes, etc.) lorsque la situation le permet,

- les autorités civiles et la population.

Cette nécessaire complémentarité des deux chaines de renseignement, nationale et multinationale, doit assurer au commandement une appréciation exhaustive de la situation dans le domaine de la CI et de la sécurité sur le théâtre d'opérations.

La Direction du Renseignement et de la Sécurité de la Défense a acquis ses lettres de noblesse « 1er cercle » dans son domaine d'expertise de la Contre-Ingérence Défense au sein de la communauté nationale et internationale du renseignement.

Éric Melchiori

Notes

(1) SHAPE : *Supreme Headquarter Allied Power in Europe.*

(2) La DRSD est le service français de contre-ingérence officiellement reconnu par l'OTAN.

Photo ci-dessous :
En mars 2016, des soldats français participent à un exercice interarmées de cyberdéfense. Alors que les cyberattaques se multiplient et que la cyberdéfense a été élevée au rang de priorité nationale, le rôle de la DRSD consiste également à assurer la protection des systèmes d'information, via notamment le contrôle et la surveillance des accès aux installations. Les principales mesures reposent sur l'emploi de moyens de chiffrement, de matériels protégés contre l'émission de signaux parasites compromettants et de moyens informatiques qui remplissent des fonctions de sécurité afin d'empêcher l'usage illicite des systèmes d'information. (© C. Risse/ Armée de l'air)

Le renseignement économique

Par **Claude Revel**, ancienne déléguée interministérielle à l'intelligence économique.

Le renseignement économique consiste à la fois en une information à caractère économique et en une activité menée par un acteur économique. Le renseignement économique a toujours existé, en témoignent par exemple les efforts mis en œuvre par Colbert pour mieux connaitre les industries anglaises (ces dernières agissant de la même manière en sens inverse).

L'élargissement du champ économique

Aujourd'hui, les choses sont à la fois plus simples et plus complexes pour trois raisons : les champs économique, politique, technologique, social… sont décloisonnés et un bon renseignement dans le champ économique doit en réalité prendre en compte tous les autres pour être vraiment pertinent ; en deuxième lieu, l'information, devenue matière première de notre société, n'est plus rare mais au contraire surabondante, particulièrement en matière économique, et ses modes de traitement doivent évoluer ; en troisième lieu, les acteurs économiques ne sont plus seulement les entreprises, car les règles du jeu de la mondialisation et de la puissance fondées sur le libre-échange placent les États en concurrence non seulement entre eux, mais aussi avec de grandes entreprises multinationales plus riches que les deux tiers d'entre eux. Le champ du renseignement économique s'est étendu aussi bien au privé qu'à toutes les activités concernées par la compétition, qui concernent la quasi-totalité des secteurs (les ONG, par exemple, en sont de grandes utilisatrices pour attirer des fonds, pour gagner en image).

Sur le fond, du fait de l'abondance de l'information, le renseignement économique fait face à deux obligations nouvelles : d'abord rechercher l'information sur l'environnement, le contexte et – toujours et encore – expliquer, comparer et anticiper ; ensuite, savoir traiter la désinformation passée à l'échelle industrielle. Quand le romancier Antoine Bello écrivait en 2007 *Les Falsificateurs* et évoquait le « Consortium de falsification de la réalité », nul n'imaginait que cette activité serait un jour si répandue. Savoir prendre conscience de ces falsifications volontaires et les contrecarrer demande une professionnalisation de la fonction du renseignement. Cette matière première qu'est l'information est le carburant de toute l'économie et, de plus en plus, des entreprises. C'est aussi leur première vulnérabilité.

Un autre défi, pour elles comme pour les États, est de savoir extraire la valeur ajoutée des données qu'elles possèdent parfois sans le savoir. On ne peut pas ne pas parler à ce stade du *kwowledge management* et de la méthode très utile permettant de faire émerger, à partir de savoirs disséminés et non conscients, des renseignements et des informations.

La naissance de l'intelligence économique

Cette professionnalisation et cet élargissement ont conduit à la création d'une nouvelle approche intitulée « intelligence économique » (IE), dont le premier des trois piliers est le renseignement – mère de toutes les batailles –, assorti donc de deux autres activités : la sécurisation des actifs immatériels et la prévention des risques ; la transformation de toute cette connaissance en influence internationale.

La méthode reste bien la même : traitement méthodique de la donnée (collecte, tri, validation), simplement les statuts des informations recueillies ne sont pas les mêmes et elles peuvent être acquises par des moyens différents. Dans tous les cas, il s'agit bien d'exploiter l'information pour en faire du renseignement, notion plus pointue, voire aujourd'hui de la connaissance, notion plus diffuse qui relève du partage et de la collaboration sur cette matière première.

Faire la différence entre renseignement économique et intelligence économique

La grande différence entre intelligence économique et renseignement économique est que celui-ci, pour

Photo ci-contre : Livraison, en octobre 2011, d'un Airbus A380 à la compagnie China Southern Airlines, à Pékin. Selon une note de la DGSI (Direction générale du renseignement intérieur), les Chinois seraient particulièrement actifs en France en matière d'espionnage économique, et excelleraient dans le vol de matériel expérimental et le piratage informatique avec un intérêt marqué pour le spatial, l'aéronautique et la biologie médicale. (© Xinhua/Jing Lei)

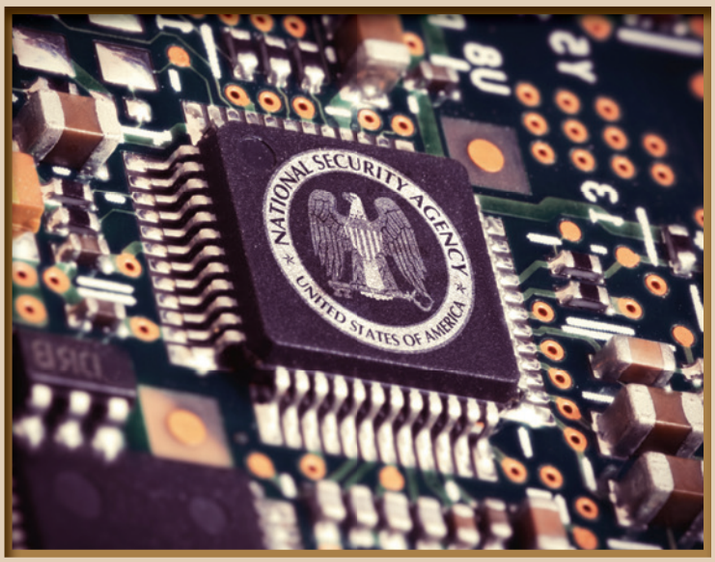


Photo ci-contre : En juin 2015, des documents rendus publics par Wikileaks ont révélé un système mis en place par les États-Unis qui permettait de collecter des renseignements au plus haut niveau de l'État sur les affaires économiques. Des ministres français de l'Économie, ainsi que des centaines d'entreprises françaises ont ainsi été mis sur écoute par la NSA, qui s'intéressait surtout au renseignement sur les appels d'offres impliquant des entreprises américaines. (© Shutterstock/Carsten Reisinger)

le compte de l'État, utilise à la fois des sources ouvertes et fermées et des moyens légaux et illégaux, autorisés voire ordonnés par l'autorité publique, tandis que l'IE n'a recours qu'à des sources ouvertes et à des techniques légales, ce qui ne l'empêche pas de se mettre au service de l'État en tant que mode de gouvernance par la connaissance et l'anticipation. Du coup, le mot renseignement économique voit sa signification se concentrer sur l'information précise à caractère économique dont l'obtention utilise des techniques des services, voire en provient, alors que l'IE est devenue une activité professionnelle de gestion d'une matière première. Certes, nombre de gens confondent encore les deux et mettent l'ensemble dans le sac de l'espionnage, mais l'avènement de la société numérique et de sa matière première contribue à éclaircir les frontières. Elle contribue aussi à trouver de nouveaux outils de dissection de l'information et à créer de nouveaux métiers (*data scientists*...) et, paradoxalement, à renforcer l'importance des sciences humaines et des réseaux de connaissance pour, en particulier, déceler les biais de toutes sortes et obtenir des recoupements d'informations de première main.

La nécessaire mise en place d'un service de renseignement économique pour les États

Une des questions clés qui se posent aujourd'hui est celle du partage de cette information. Par exemple, les États n'ont en principe plus le droit d'aider leurs entreprises à exporter, pour respecter un principe partagé de *fair competition*. Aujourd'hui, l'aide financière n'est plus primordiale et l'apport ou non d'information au bon moment peut faire basculer des opérations dans la réussite ou à l'inverse dans l'échec. Partager des renseignements économiques obtenus à partir de moyens non éthiques (incitation financière, usage de motifs idéologiques, compromission ou flatterie de l'ego) ou en violation du secret voulu par les producteurs de l'information est-il légitime ? La question peut aller plus loin : est-ce à l'État de produire des informations mêmes obtenues de sources ouvertes et éthiques mais au profit de ses entreprises ? Certains États confondent les fonctions dans des lieux comme le Joint Intelligence Committee britannique [voir p. 72 de ces *Grands Dossiers*, NdlR] ou dans un autre ordre d'idées, l'Advocacy Center américain (1).

La vraie solution, pour un État, est de se doter d'un véritable service de renseignement économique à la fois ouvert (IE) et fermé, pour servir les intérêts du pays, y compris ceux liés à son image, pour préserver les données sensibles liées au patrimoine informationnel de l'État et à celui des acteurs privés sensibles, pour étendre son influence au sein des organisations internationales prescriptrices de règles et pour, dans un partenariat bien compris, coopérer avec les acteurs privés et associatifs. Par ailleurs, en France en tous cas, le lien entre renseignement économique et renseignement tout court, notamment terroriste, est encore trop mal appréhendé, uniquement sous sa forme financière et à travers les circuits éventuels de blanchiment. Or le renseignement économique pourrait s'interroger sur les intentions derrière les prises de contrôle étrangères de certaines entreprises nationales, sur les liens plus ou moins étroits entre certains investisseurs et le terrorisme ou la diffusion de valeurs hostiles à la République, sur les cultures que voudraient promouvoir certains repreneurs d'affaires ou financiers de start-ups, sur les patrons de multinationales du numérique qui veulent pulvériser la notion même d'État et, enfin, sur les influences susceptibles d'être exercées sur les décideurs de l'administration, notamment par des États ou fonds souverains soutenant des interventions d'entreprises étrangères. Certaines des informations recueillies pourraient être mutualisées entre États européens.

Et la France ?

Pour finir sur la France, une vraie doctrine serait nécessaire en matière de renseignement pour y intégrer le renseignement économique et exploiter tout ce qu'il peut apporter à une connaissance commune des risques, menaces et opportunités. Pour cela, il est crucial de *définir les critères de l'intérêt stratégique* pour limiter l'action de l'État à l'essentiel et ainsi la légitimer, ainsi que d'*établir un schéma géoéconomique* pour les dix ans à venir qui orienterait utilement les chercheurs de renseignement économique. Parallèlement, il faut développer une intelligence économique d'État à vocation anticipatrice et d'influence, nécessairement interministérielle et professionnelle. En effet, toute l'évolution de l'information aujourd'hui fait de son traitement un élément majeur de souveraineté, qu'il faut savoir gérer en lien avec les autres aspects de la souveraineté.

Claude Revel

Note

(1) Unité du Département du Commerce américain dont le rôle est de coordonner l'action interministérielle d'aide aux entreprises américaines pour l'obtention de marchés publics à l'étranger.

Photo ci-contre : C'est au début des années 1980 que la Direction générale de la sécurité extérieure française a entrepris d'infiltrer 49 entreprises américaines – parmi lesquelles IBM, Hewlett Packard ou Texas Instruments – dans lesquelles des ingénieurs français se sont fait embaucher pour tenter d'accéder à des secrets industriels. Le FBI a démantelé ce réseau en 1989. (© Shutterstock/Adriano Castelli)

analyse

Par **Alain Chouet**, ancien chef du service de renseignement de sécurité de la DGSE.

Photo ci-dessus :
Des Navy Seals en opération en février 2016. Peu de temps après son élection, le nouveau président américain, Donald Trump, autorisait une opération secrète des Navy Seals au Yémen afin de surprendre des combattants d'Al-Qaïda dans la péninsule Arabique (AQPA). Selon le porte-parole de la Maison-Blanche, Sean Spicer, cette opération ne peut être qualifiée de « succès à 100 % » en raison de la mort d'un soldat américain, mais elle aurait permis de collecter une « énorme quantité » d'informations sur AQPA et d'éliminer 14 combattants ennemis. L'opération aurait également tué « de nombreux civils, dont au moins dix femmes et enfants », selon l'ONG International Crisis Group. (© NavySeals.com)

Lutte antiterroriste : un axe prioritaire du renseignement

La menace terroriste est aujourd'hui de plus en plus diverse et imprévisible. Elle s'est ainsi imposée comme l'une des priorités des principaux services de renseignement mondiaux. Quels en sont les enjeux ?

Dans un monde dominé par la puissance militaire et technologique des États-Unis et de leurs alliés de l'OTAN, l'expression des conflits d'intérêt, de pouvoir ou d'idéologie ne peut plus être obtenue par l'affrontement en rase campagne de grands corps de bataille. Elle ne peut qu'emprunter le temps long des manœuvres politiques complexes éventuellement appuyées sur des stratégies du faible au fort dont la sauvagerie médiatisée et les violences disproportionnées sont des éléments de base. À l'évidence, cette menace ne relève que marginalement de contre-mesures militaires, mais plus immédiatement de la capacité de connaissance et d'action des services de sécurité des communautés et des États ciblés.

La distinction entre renseignement de sécurité intérieure et renseignement de sécurité extérieure n'est pas une distinction géographique mais une distinction fonctionnelle. Le renseignement intérieur s'efforce de prévenir l'éclosion de la violence politique et du terrorisme, en continuité avec l'institution judiciaire, en essayant d'identifier le plus en amont possible et de neutraliser ou réprimer dans un cadre juridique formel les atteintes à la loi et le trouble à l'ordre public. Le renseignement de sécurité extérieure s'exerce par définition hors du cadre juridique de la zone où il s'applique et sans le support des prérogatives ou des instruments de contrainte légale de la puissance publique.

Considérant que le degré zéro du terrorisme s'analyse en pertes humaines et matérielles, il est clair que l'action des services de renseignement et de sécurité doit se situer le plus en amont possible, bien avant l'exécution de l'acte criminel, au stade de l'élaboration de l'idéologie violente, du recrutement et de la formation des exécutants, de la recherche ou de la réunion des instruments matériels de l'action terroriste. En résumé, il s'agit de mener des « procès d'intention » et d'en inférer des contre-mesures qui, quelle que soit leur justification pratique ou morale, sont très étrangères à l'État de droit et à l'éthique des sociétés démocratiques.

Photo ci-dessus :
Alors que le recrutement d'arabisants est aujourd'hui une nécessité pour les services de renseignement, le directeur de la DGSI, Patrick Calvar, a déclaré que cette question « commence à devenir un souci, car nous rencontrons des difficultés d'habilitation » en raison du risque d'être infiltrés. (© Shutterstock/librakv)

Photo ci-dessous :
En juillet 2016, le patron des services extérieurs français (DGSE), Bernard Bajolet, annonçait que son service avait « contribué à la conception, à la planification et à la conduite de 69 opérations d'entrave de la menace terroriste, dont 12 ayant permis d'éviter des attentats contre des intérêts français à l'étranger, 6 des projets d'attentats susceptibles de frapper des intérêts occidentaux » et 51 opérations de réduction de la menace qui ont consisté à « arrêter des gens, déjouer des projets ou mettre des terroristes hors d'état de nuire ». (© Shutterstock/Hadescom)

Un certain nombre de dispositions légales françaises – en particulier l'incrimination pour « association de malfaiteurs en relation avec une entreprise terroriste » – permettent des opérations préventives efficaces sur le territoire national. Elles sont cependant très controversées, n'épuisent pas le sujet dont les racines sont le plus souvent à l'étranger, et demeurent une « exception française ».
En tout état de cause, les services extérieurs ne peuvent se prévaloir de ces dispositions. Ils doivent adopter un cheminement complexe et sinueux entre l'obligation de résultat dans la prévention de la violence, le respect des règles éthiques communément admises et la protection de la réputation et des intérêts internationaux de l'État employeur. Leur démarche est donc empirique, clandestine et extra-légale. Elle repose sur l'expérience acquise depuis près de quarante ans en matière de connaissance et de traitement du terrorisme international et met en œuvre des méthodes pragmatiques aussi inventives et adaptées que possible à chaque cas, chaque terrain et chaque acteur. Car il n'existe pas une forme de terrorisme indifférenciée mais des terrorismes divers aux buts, méthodes et stratégies particulières, évolutifs dans l'espace et dans le temps, nécessitant une gestion adaptée à chaque cas de figure.

> *« Il n'existe pas une forme de terrorisme indifférenciée mais des terrorismes divers aux buts, méthodes et stratégies particulières, évolutifs dans l'espace et dans le temps, nécessitant une gestion adaptée à chaque cas de figure. »*

Comprendre le terrorisme

Contrairement à un cliché complaisamment répandu, le terrorisme n'est jamais « aveugle » et c'est à dessein qu'il frappe des « innocents ». C'est l'innocence des victimes qui fonde l'acte terroriste. Car le but du terrorisme est de terroriser, c'est-à-dire, en frappant de façon imprévisible, disproportionnée et apparemment irraisonnée, de tétaniser et diviser un adversaire supérieur en force et en nombre, d'annihiler sa capacité de résistance collective, de l'amener à négocier avant l'épreuve, à se rendre sans combattre ou au contraire à mettre en œuvre des réactions inadaptées ou contre-productives.
Cette stratégie du faible au fort n'est ni gratuite ni irrationnelle. Tout mouvement terroriste est porteur d'un message qu'il ne sait, ne peut ou ne veut transmettre autrement que par la violence. Il convient de lire, de comprendre et d'évaluer ce message pour savoir si son contenu est ou non négociable, si l'interpellation qu'il contient doit conduire au dialogue ou à l'affrontement. C'est aux services de renseignement d'en découvrir et interpréter le sens, et c'est au politique d'en tirer les conclusions.
À l'exception de quelques rares mouvements indépendantistes, aucune organisation terroriste ne se crée ni n'existe sans le soutien au moins moral ou idéologique, et en tous cas financier, d'un ou plusieurs États ou de généreux donateurs ayant pignon sur rue. De même, il n'existe pas de mouvance terroriste sans instigateurs intellectuels et agents d'influence, ne participant que rarement à l'action violente mais initiant la stratégie d'éveil des militants et sympathisants.
Une organisation terroriste n'est pénétrable qu'à hauteur de l'ouverture de son idéologie et de son propre prosélytisme. Une organisation à forte cohésion idéologique, nationaliste, religieuse ou sectaire pratiquant une stratégie de rupture avec le reste du monde n'est pas pénétrable de l'extérieur.
Toute organisation terroriste qui n'arrive pas rapidement à la réalisation de ses objectifs tend à subir une dérive psychopathe, à se replier sur elle-même, à adopter un fonctionnement sectaire, à pratiquer une stratégie de rupture avec le reste du monde. Plus une organisation terroriste est fermée et en état de rupture, plus elle est sensible à la loyauté et à la fiabilité de ses membres. Le moindre indice de déviance ou de trahison y produit un effet interne dévastateur pouvant entraîner l'élimination mutuelle de ses membres.

Terroriser les terroristes ?

Le premier réflexe des sociétés frappées par l'horreur du terrorisme est de réclamer vengeance et, puisque services d'action extérieure il y a, d'exiger leur intervention immédiate afin d'en pourchasser et éliminer les auteurs au mépris de toutes les règles de droit interne et international. C'est une réaction primaire et populiste qui ne manque d'ailleurs pas d'être exploitée par les responsables politiques qui y voient un expédient pour éluder leur propre responsabilité face au désastre. Il ne faut cependant pas trop accorder de crédit à la légende qui voudrait que l'on puisse facilement « terroriser les terroristes ».
Sachant qu'il n'existe pas d'organisation terroriste sans sponsor étatique direct ou indirect, ces instigateurs « institutionnels » sont difficiles à atteindre sans entrer dans une logique de guerre ouverte ou de remise en cause de grands équilibres géopolitiques. De nombreux exemples prouvent que, tant que l'action terroriste n'atteint pas un niveau totalement insupportable ou ne s'inscrit pas dans la durée, les États cibles préfèrent traiter avec les États sponsors *(Iran, Libye, Syrie)* ou faire semblant d'ignorer leur rôle *(Arabie Saoudite, Qatar, Pakistan)*, ou frapper un tiers plus ou moins concerné *(Irak)* plutôt que remettre en cause leurs alliances ou les systèmes régionaux de stabilité.

Quant aux exécutants, ils sont la plupart du temps, comme les criminels de droit commun, peu accessibles à l'effet dissuasif du châtiment quand ils ne sont pas, de plus, dans une logique sectaire et fanatique les conduisant à mettre leur propre vie en jeu dans l'action. Dans tous les cas, ils sont plus sensibles à la menace pesant sur eux de la part de leurs chefs qu'à celle, nécessairement limitée, pouvant provenir d'États de droit.

L'action violente offensive préemptive, même ciblée, pose en effet le problème du respect de ses propres valeurs et du risque de s'inscrire dans une stratégie de radicalisation voulue par l'adversaire *(Irak, Afghanistan, Territoires palestiniens)*. Elle comporte de plus le risque non négligeable de dérives dont l'une des principales est celle d'une auto-perpétuation des structures d'action offensive qui peuvent parfaitement « s'autonomiser » *(Escadrons de la mort)*, ou « imaginer » des terroristes *(Irlandais de Vincennes)*, ou pis, en fabriquer *(Attentat de la gare de Bologne)*.

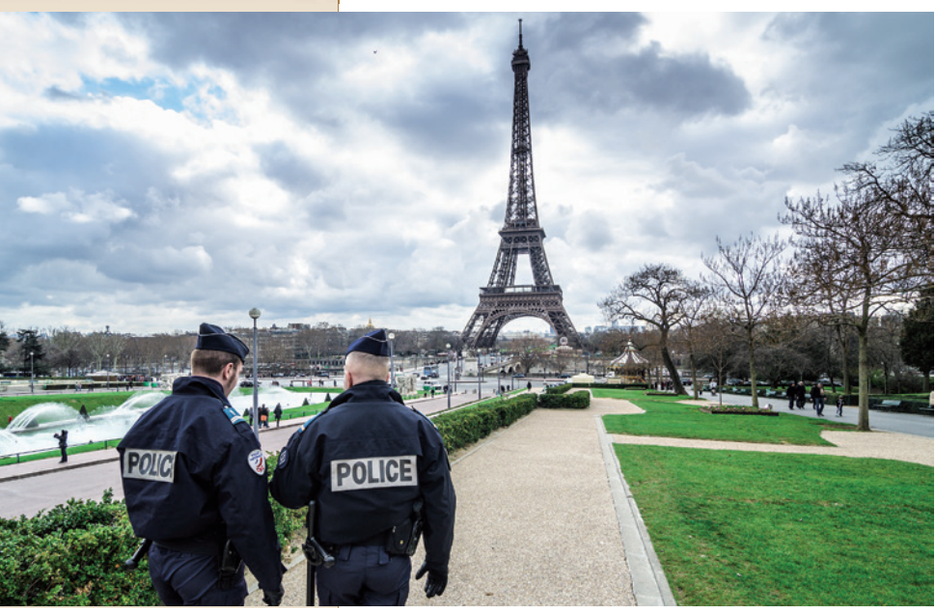


Photo ci-dessus :
Lors d'une audition organisée à huis clos en mai 2016 à l'Assemblée nationale par la commission d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme, le directeur général de la DGSI (renseignement intérieur), Patrick Calvar, s'inquiétait de l'évolution du mode opératoire des terroristes en France et déclarait que plus des deux tiers des capacités de la DGSI étaient mobilisés sur le front de la lutte antiterroriste. Pour faire face à la menace, la DGSI devrait voir croitre ses effectifs de 40 % pour atteindre les 4000 personnes en 2018. (© Shutterstock/BlackMac)

Gérer la menace

L'ensemble de ces constatations peut permettre d'esquisser de façon raisonnée des lignes possibles de gestion de la menace qui ne relèvent par définition ni de la prévention diplomatique ni de la réaction militaire mais de l'action permanente des services extérieurs de sécurité, de renseignement et d'action.

• *Identifier*

La logique terroriste reposant essentiellement sur l'entretien d'un sentiment d'irrationalité et d'insaisissabilité des auteurs, tout préliminaire à la lutte passe par l'identification des acteurs, la localisation et le maillage de leurs structures, la détermination des stratégies utilisées et des buts recherchés. Il importe peu que l'information sur ces données soit au départ précise et fine. Il est cependant essentiel qu'elle apporte les éléments nécessaires à préciser la nature, l'origine et la finalité du danger, à sortir rapidement de la logique de terreur induite par l'incompréhension.

De telles connaissances reposent sur l'existence préalable d'une expertise du phénomène et de ses acteurs, d'un fonds documentaire, d'un environnement humain des structures hostiles, d'un suivi technique de leurs activités et communications, régulièrement alimentés et entretenus, même en temps d'accalmie, sur les évolutions idéologiques, les formes de pensée déviantes, le rôle des maîtres à penser, gourous et agents d'influence, les sources de contentieux internationaux non réductibles par le dialogue, les déséquilibres de forces non maîtrisés ou non compensés, la cartographie fine des zones de non-droit, l'identification précise des élites intermédiaires qui s'y substituent aux États.

Il est clair que l'entretien permanent d'une telle expertise est coûteux. Son poids est mal supporté, surtout dans les périodes plus ou moins longues d'accalmie relative qui séparent les grandes périodes de fièvre terroriste. Il est cependant le préalable indispensable à toute réelle stratégie antiterroriste, faute de quoi les États de droit sont condamnés à une vulnérabilité, aux initiatives désordonnées, à la répétition de réponses inadaptées aggravant parfois le risque.

> *« L'action violente offensive préemptive, même ciblée, pose le problème du respect de ses propres valeurs et du risque de s'inscrire dans une stratégie de radicalisation voulue par l'adversaire. »*

• *Subvertir*

Toute action terroriste ayant pour préalable – et souvent pour accompagnement – une réflexion théorique et idéologique, il est essentiel d'en déterminer les auteurs. Ceux-ci ont, par définition, une certaine visibilité sans laquelle leur message n'aurait pas d'écho. Facilement identifiables et localisables, il est rare, pour ces raisons, qu'ils soient directement mêlés à l'action violente. Ils ne peuvent donc faire l'objet de mesures préventives ou répressives dans un État de droit garantissant la liberté d'expression.

Rien n'interdit cependant de leur opposer des contre-feux, de susciter ou favoriser des rivaux intellectuels leur portant la contradiction, soit dans le sens d'un maintien de l'ordre établi, soit dans un courant de dépassement, et, en tout cas dispersant leur message, le soumettant à la contradiction, voire à la confusion.

Il peut également être utile de les déconsidérer aux yeux de leurs disciples actifs en recherchant dans leur vie personnelle les éléments de contradiction intellectuels ou comportementaux avec les doctrines qu'ils propagent. Au contraire des exécutants – en général condamnés à la clandestinité et à une certaine austérité –, les inspirateurs intellectuels recherchent en général la notoriété et les accessoires qui y sont liés.

• *Ruiner*

Même si elle met en jeu des moyens limités, l'action terroriste suppose un minimum de moyens financiers. Plus que l'action violente elle-même, sa préparation à long terme, la recherche, la mise en condition, la formation, la mobilisation des militants, la prise en charge de leurs familles dont ils sont séparés par la clandestinité et parfois la mort, requièrent des moyens considérables.

Après les services de l'Est dans les années 1970-1985 au profit des mouvements révolutionnaires violents euro-palestiniens et du Tiers Monde, l'Iran dans le monde chiite et les pétromonarchies du Golfe dans le monde sunnite investissent chaque année des millions de dollars dans le soutien aux organisations et institutions intégristes islamiques qui constituent le vivier de recrutement des organisations terroristes. De même, ils financent largement, directement ou indirectement, un certain

nombre de mouvements violents relayant leurs stratégies et intérêts politiques.

Pour les mouvements terroristes qui ne bénéficient pas de soutiens directs d'États, les ressources proviennent en général d'activités délictueuses supposant la constitution de réseaux délinquants et de structures de blanchiment d'argent. L'identification de ces réseaux de financement, qu'ils soient légaux ou délictueux, de leurs relais, de leurs bénéficiaires ainsi que leur neutralisation constituent un préalable et un accompagnement indispensable de toute forme de lutte antiterroriste.

• Désorienter

Fortement structurés, soudés par la clandestinité et les risques partagés, les mouvements terroristes sont particulièrement vulnérables au soupçon et particulièrement attentifs à la loyauté et à la fiabilité de leurs membres. Le moindre doute à ce sujet entraîne, en général sans que soit recherchée une preuve quelconque, l'élimination physique de l'élément suspect avec les risques de vendetta et d'éclatement du groupe que ce type de mesure peut induire dans des mouvements à l'idéologie fragile ou déstabilisée.

Un axe prioritaire de la prévention antiterroriste doit donc être la recherche systématique des stratégies permettant d'instiller ce type de doute au sein des organisations, soit en corrompant réellement un ou plusieurs de leurs membres, soit en fabriquant tous les éléments de suspicion nécessaires à faire croire à cette corruption.

Revisiter les politiques de défense

Considérant les lignes de défense ainsi esquissées, les actions visant directement les structures terroristes hors du territoire national relèvent à l'évidence de la compétence et du savoir-faire des services extérieurs, mais elles n'ont de sens que si elles s'inscrivent en permanence dans une démarche de défense collective qui ne peut se réduire à l'activité de spécialistes.

La prévention du terrorisme a donc un coût constant qui est celui d'une assurance contre un risque. Ce coût ne peut être constamment remis en cause en fonction de l'état plus ou moins élevé de la menace et de la couleur du plan « Vigipirate ». Le fait que la menace soit par moment moins évidente est parfois dû à une action proactive efficace des services de sécurité... C'est exonérer sa responsabilité à bon compte et entrer dans le jeu des terroristes que de faire de la surenchère à l'horreur, de donner une importance exagérée à leur action, de répondre de façon démesurée à leurs attaques et de « faire monter les enchères ». Cela dit, il demeure que l'État de droit ne peut être un état de licence pour ses pires ennemis. Les attentats dévastateurs commis depuis quinze ans contre les États-Unis, divers pays européens et nombre de pays musulmans ont été inspirés et prescrits par des maîtres à penser réfugiés en Afghanistan, occupé par une force multinationale occidentale, au Pakistan allié des États-Unis, dans les zones grises d'États faillis suite à des interventions extérieures mal avisées (Irak, Syrie, Libye, Somalie, etc.). Ces attentats ont été conçus, préparés et exécutés par des acteurs délinquants identifiés vivant au sein des sociétés visées, dans des zones de non-droit tolérées au nom d'un « droit à la différence » ou désertées par la puissance publique. Ces acteurs du terrorisme ont été éduqués dans des écoles de subversion par des zélateurs de l'exclusion protégés au nom de nos libertés publiques, financés par des ressortissants de pays que nous persistons à croire indispensables à nos intérêts et à vouloir intouchables, ou par des activités délictueuses trop nombreuses et trop marginales pour être résolument poursuivies par nos services de police et de justice.

Avant même de mettre en œuvre l'instrument ultime de la politique régalienne et de la raison d'État que sont les services de renseignement et d'action, c'est d'abord en répondant à ces différentes contradictions essentiellement politiques que pour-

ront être dessinés les axes efficaces d'une stratégie antiterroriste. Et il y a urgence à le faire. Si le terrorisme dit islamiste occupe aujourd'hui le devant de la scène, il cache mal le fait que la violence constitue désormais l'arme ultime de tous ceux qui entendent contester l'ordre établi : activistes écologiques, laissés pour compte de la mondialisation, communautés irrédentistes, mafias, dealers et trafiquants, sociétés militaires privées autonomisées, ONG contestataires, etc. La liste est longue de ces minoritaires qui proclament que « la violence est le seul moyen de se faire entendre ».

Alain Chouet

Pour aller plus loin

Les Grands Dossiers de Diplomatie nº 32, « Géopolitique du terrorisme », avril-mai 2016.

Photo ci-contre :
Les besoins croissants en analystes compétents constituent un axe de recrutement majeur des services de renseignement. « La complexité des problèmes et menaces traités impose de recourir à des personnels non issus de la police nationale mais spécialisés dans l'économie, la finance, voire dans d'autres domaines plus opérationnels tels que des psychologues et des linguistes », estime ainsi le directeur de la sécurité intérieure française. (© Shutterstock/Tomasz Trojanowski)

Photo ci-contre :
En décembre 2017, l'infiltration d'une cellule terroriste par la DGSI ayant abouti à une vague d'arrestations à Marseille et Strasbourg a permis de déjouer une possible série d'attentats, notamment contre le siège de la police judiciaire à Paris, ainsi qu'à la DGSI. L'infiltration demeure l'un des moyens les plus puissants et méthodiques pour comprendre les terroristes et leur façon de fonctionner. (© Shutterstock/oneinchpunch)

Le *renseignement criminel* : une doctrine récente issue d'une longue histoire

Par **Jean Rastine**, doctorant en science politique.

Au sens strict, le renseignement criminel consiste à recueillir, enrichir et analyser des informations relatives à des crimes constatés – en cela, il fait partie intégrante de l'enquête judiciaire classique – ou à des crimes non encore connus. C'est donc une activité tout entière tournée vers un but judiciaire et répressif et les informations peuvent être issues de sources ouvertes, c'est-à-dire accessibles à tous ou bien fermées, par l'utilisation de techniques spéciales d'enquêtes. Au sens large, le renseignement criminel inclut l'analyse et le recueil d'informations relatives au contexte dans lequel le crime s'épanouit dans le but de le réprimer mais également de le prévenir, de telle sorte que l'on parlera de « renseignement d'intérêt criminel » (1).

On distingue classiquement trois niveaux de renseignement criminel :

• De niveau stratégique : il aide à la compréhension globale des phénomènes criminels émergents et s'inscrit volontiers dans une démarche macro et prospective.

• De niveau tactique : il approche le crime de façon plus micro, en appréhendant des objets tels que les bandes criminelles, les modes opératoires ou les victimes.

• De niveau opérationnel : il s'exprime particulièrement lors des phases d'interpellations, de perquisitions ou d'auditions des mis en cause.

Des politiques publiques de sécurité centrées sur le renseignement criminel se sont développées (2) dans plusieurs pays dans les années 1990 et on leur a volontiers attribué des résultats parfois spectaculaires. Avec celles-ci, on passe d'une logique policière réactive, qui consiste à constater un crime et à en rechercher les auteurs et les preuves afin de les présenter à la justice, à une logique proactive : connaître les phénomènes criminels sériels et les milieux criminels hyperactifs de façon à orienter plus efficacement les services d'enquêtes ou à prévenir le crime.

Si les doctrines de renseignement criminel sont d'un développement relativement récent, l'activité de renseignement à des fins de lutte contre la criminalité a une longue histoire, presque aussi longue que la police elle-même (3), mais cette activité dispersée dans plusieurs services de l'État n'a jamais vraiment été assumée par les autorités publiques et n'a jusqu'à présent pas fait l'objet d'une politique publique intégrée.

Garder une vision large des clients du renseignement criminel

On l'a dit, le « client naturel » du renseignement criminel est d'abord l'autorité judiciaire. La création des brigades de recherches et d'interventions dans les années 1960 formalise ce travail en amont. Comme le précise le commissaire Le Mouël, premier chef de la Brigade de recherche et d'intervention (BRI) parisienne : « au lieu de partir du crime pour aller au criminel, on partait du criminel pour aller au crime avec en filigrane l'idée de prévention ».

Les BRI ont développé des techniques de renseignement criminel diverses, allant du traitement des informateurs, aux écoutes téléphoniques en passant par la pose de balises sur les voitures ciblées. On leur a attribué des succès majeurs, notamment dans la lutte contre les équipes de braqueurs fortement actives dans les décennies 1970 et 1980.

Si l'autorité judiciaire est le « client naturel » du renseignement criminel *lato sensu*, d'autres débouchés lui sont ouverts. Les autorités préfectorales, fiscales, voire dans certains cas diplomatiques, peuvent s'y intéresser.

Illustrons notre propos : dans le cadre de la politique de la ville, les autorités politiques et préfectorales auront tout intérêt à avoir une connaissance fine des risques relatifs aux émeutes urbaines, des conditions dans lesquelles celles-ci se déploient et des facteurs de réductions de ces risques le cas échéant (4). De même, les informations financières (5) peuvent intéresser au premier chef les autorités administratives, qui diligenteront des contrôles fiscaux ou interministériels à l'instar des opérations dans le cadre des CODAF (Comités opérationnels départementaux anti-fraude).

Photo ci-contre : La ville de New York a enregistré une baisse spectaculaire de sa criminalité entre le milieu des années 1990 et les années 2000 (-78 %). Le criminologue américain Franklin M. Zimring attribue ce phénomène à une politique centrée sur l'analyse des « *hotspots* » du crime, le recueil systématique des informations criminelles et leur traitement. (© Shutterstock/Pio3)

Photo ci-contre : Des policiers britanniques patrouillent dans les rues de Londres. Alors que le renseignement criminel, qui s'appuie sur trois piliers fondamentaux (analyse géographique de la délinquance, détection des phénomènes et des séries et focalisation sur les auteurs et les groupes d'auteurs prolifiques), constitue une source d'inspiration pour les polices britannique, canadienne et américaine, ce modèle peine encore à s'imposer en France en raison de la distinction trop étanche entre police administrative et police judiciaire et de la prééminence du modèle d'enquête judiciaire sur celui du renseignement. (© Shutterstock/singh_lens)

Enfin, plus marginalement, les autorités diplomatiques peuvent également être un client du renseignement criminel. On sait que le ministère de l'Intérieur entretient un réseau important d'attachés de sécurité intérieure dans les ambassades de France et que certaines informations particulièrement sensibles peuvent rentrer en compte dans le cadre des relations diplomatiques (6). En France, plusieurs structures font du renseignement criminel au sens large, à destination de différents « clients ». Une structure intégrée de renseignement criminel, à l'instar des Unités de renseignement criminel néerlandaises, regroupant à la fois le traitement des informateurs et l'analyse des informations, présenterait probablement l'avantage de mutualiser les informations policières, fiscales, douanières et préfectorales afin de mieux servir ces clients.

Judiciariser l'information sans judiciariser l'activité de renseignement criminel

L'information produite par le renseignement criminel a vocation la plupart du temps à être « judiciarisée ». La « judiciarisation du renseignement » peut ne pas poser de difficultés lorsqu'il s'agit simplement d'enrichir une enquête déjà existante ou même d'en ouvrir une, à partir d'informations obtenues en source ouverte. L'enquêteur rédigera alors « un procès-verbal de renseignement » et l'intégrera en procédure. Lorsqu'il s'agit de « blanchir » un renseignement obtenu par un informateur, la tâche est plus ardue. Il faut absolument protéger l'anonymat de la source et la pratique des enquêteurs (7) consiste alors, sans faire de faux procès-verbaux, à omettre de tout relater en procédure, que ce soit par des formules générales telles « qu'une source anonyme nous révèle », ou par une articulation de procédure telle que l'origine du renseignement semble attribuée à une source sans contact avec l'informateur : tiers ou encore service étranger.

Si le ministère de l'Intérieur a encadré la rémunération des informateurs par la LOPSI de 1995, puis par des textes réglementaires, on voit que le statut du traitement des sources reste fragile. Il peut alors être tentant de judiciariser l'activité même du renseignement criminel, à l'instar du modèle belge et de son enquête proactive. En effet, si l'activité de la police judiciaire française consiste seulement à rechercher les auteurs « d'infractions constatées » (8), le Code d'instruction criminelle belge élargit son champ de compétence aux infractions à venir dans le cadre de l'enquête proactive (9). L'enquêteur traite alors ses informateurs sur autorisation du magistrat et selon ses instructions.
Un tel modèle, s'il a le mérite de donner un cadre plus solide aux traitants, comporte des faiblesses certaines. On sait que le traitement d'une source s'étend sur plusieurs années et que le lien de confiance entre l'enquêteur et la source est primordial et pourrait être entamé par un cadre trop rigide dans lequel le décisionnaire final serait trop éloigné du terrain. Par ailleurs, le renseignement criminel est une activité pragmatique, où le traitement de l'informateur et sa rémunération (assortie éventuellement d'un « écrasement » par l'enquêteur de certaines affaires judiciaires de moindre importance) se justifient par l'élucidation d'affaires plus importantes. Il n'est pas sûr que la culture judiciaire française se prête à ce type de logiques (10).

Jean Rastine

Notes

(1) François Farcy et Jean-François Gayraud, *Le renseignement criminel*, Paris, CNRS éditions, 2011.

(2) L'*Intelligence led policing* ou « police guidée par le renseignement » est définie comme « un modèle organisationnel et une philosophie du management dans lequel l'analyse des données et le renseignement criminel jouent un rôle central dans la prise de décision relative à la réduction de la criminalité et des désordres, et à la prévention de la délinquance » par Jerry Ratcliffe dans *Intelligence-led policing* (Willan Publishing, 2008).

(3) Citons les mouchards des commissaires parisiens du XVIII[e] siècle étudiés par Justine Berlière.

(4) La section « violences urbaines » des Renseignements généraux répondait en partie à cette demande.

(5) Qu'elles proviennent des différents services du ministère des Finances sur le terrain comme les Brigades de contrôles et de recherches qui recueillent des renseignements dans les départements, ou de services à dimension nationale comme TRACFIN ou la DNEF.

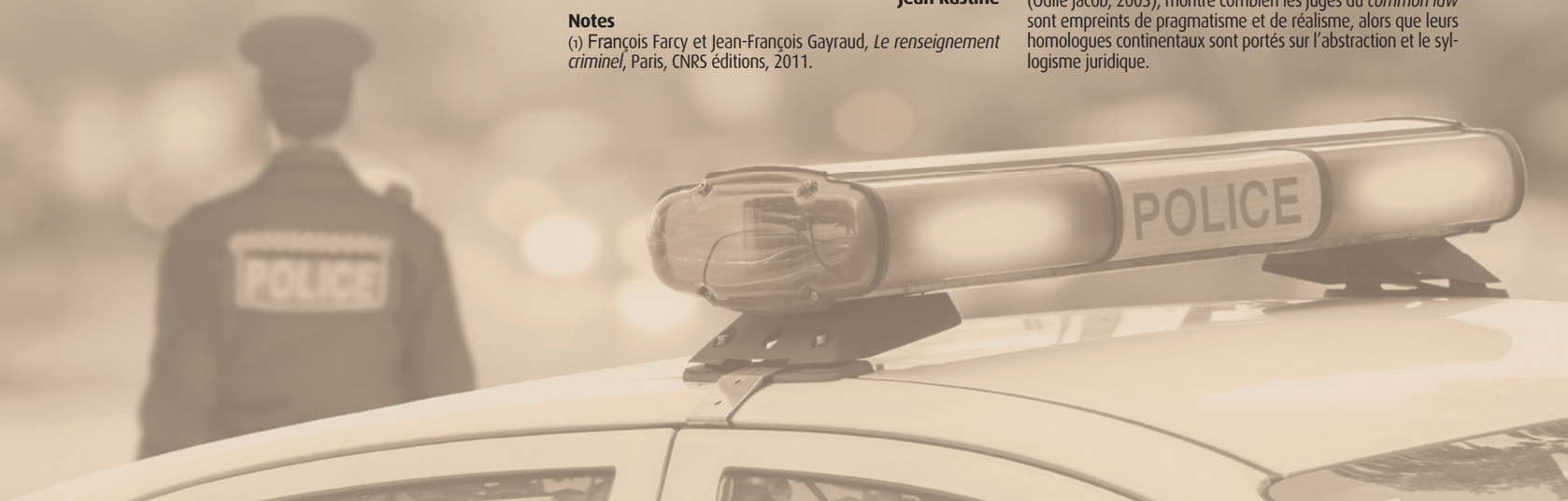
(6) Le site internet du ministère de l'Intérieur recense 40 000 échanges de renseignements opérationnels réalisés par les attachés de sécurité intérieure des ambassades françaises en 2015.

(7) L'ancien commissaire Michel Neyret relate à la fois ces pratiques et les risques inhérents à celles-ci dans son ouvrage *Flic* (Plon, 2016).

(8) Art. 14 du Code de procédure pénale.

(9) L'article 8 du CIC belge dispose que la police judiciaire « recherche les crimes » sans préciser qu'ils sont constatés et l'article 28 bis §2 instaure l'enquête proactive sous l'autorité du procureur du roi sur la base « d'une suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus ».

(10) Antoine Garapon, dans *Juger en Amérique et en France* (Odile Jacob, 2003), montre combien les juges du *common law* sont empreints de pragmatisme et de réalisme, alors que leurs homologues continentaux sont portés sur l'abstraction et le syllogisme juridique.



Les sociétés démocratiques ont mis en place des mécanismes de contrôle de leurs services de renseignement car – bien qu'agissant secrètement et ayant le droit de collecter des informations sur les personnes –, comme toute autre agence financée par l'État, ils utilisent des fonds publics ; ils sont tenus de respecter les droits humains ; ils ne doivent pas mettre en danger les éléments essentiels de la démocratie (partis politiques, médias, etc.) ; ils doivent faire leur travail efficacement et dans le respect des lois. Les modalités de contrôle varient selon les pays et sont exercées par une ou plusieurs de ces institutions : services eux-mêmes en interne, pouvoir exécutif, pouvoir judiciaire, Parlement, organes composés d'experts. Cette question est traitée ici à travers l'exemple belge. [Sur ce même pays, lire également p. 76]

Contrôler les services de renseignement : *le cas de la Belgique*

Par **Guy Rapaille**, président du Comité belge permanent de contrôle des services de renseignement et de sécurité.

La loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace a introduit en Belgique le contrôle parlementaire des services de renseignement. Le Comité permanent R, en charge de ce contrôle, a débuté ses activités en mai 1993 et porte sur les deux services de renseignement que sont la Sûreté de l'État (service civil) et le Service général du renseignement et de la sécurité (SGRS, service militaire). Depuis 2005, le contrôle s'est également étendu – mais avec le Comité permanent P (contrôle des services de police) – sur l'OCAM (Organe pour la coordination de l'analyse de la menace).

Pourquoi contrôler les services de renseignement ?

Les années 1980 avaient, en effet, été assez troublées par plusieurs « affaires » qui avaient amené le Parlement, notamment au travers de plusieurs Commissions d'enquête parlementaires, à envisager un contrôle des services de renseignement – directement ou indirectement – par une instance parlementaire.
Sans être exhaustif, il s'agissait de l'affaire dite « des tueurs du Brabant wallon » (non élucidée à ce jour), des attentats des « cellules communistes combattantes (C.C.C.) », de la découverte d'un groupuscule d'extrême droite (WNP - Westland New Post), et de l'affaire « Gladio ».
La première particularité du « système belge », est que le contrôle est double : contrôle de légalité (ce qui est assez classique pour une instance parlementaire) et contrôle d'efficacité/coordination.
Il peut paraître étonnant que le Parlement porte son intérêt sur l'efficacité des services qui relèvent du pouvoir exécutif. Mais, en se rapportant aux années 1980 au cours desquelles les services de renseignement et de police avaient été mentionnés dans plusieurs « affaires », soit parce que les services ou des agents avaient été cités, soit parce que ces services n'avaient pu prévenir ou résoudre rapidement ces « affaires », le contrôle de l'efficacité des services constituait la préoccupation première du Parlement qui ne pouvait, cependant, négliger le contrôle de légalité.
Le contrôle porte ainsi sur les activités et la méthode des services et non sur la politique publique de renseignement qui relève du contrôle parlementaire classique (que ce contrôle soit effectif ou non…). Il se concrétise par des enquêtes. Même si la loi ne l'interdit pas formellement, le contrôle ne porte pas sur les activités en cours menées par les services. Le but du contrôle est de constater des imperfections et dysfonctionnements éventuels dans les activités des services et de formuler des recommandations destinées à y remédier. Le contrôle organisé par la loi de 1991 est donc à distinguer du contrôle hiérarchique interne, du contrôle disciplinaire ou du contrôle exercé par les autorités judiciaires en cas d'infractions commises par les agents des services.
Une deuxième particularité du « système belge » doit être mentionnée : le contrôle est exercé par le Comité permanent R (Comité permanent de contrôle des services de renseignement et de sécurité) et par la Commission parlementaire du suivi. Les termes ont leur importance : le Comité R dispose d'une compétence de contrôle, tandis que la Commission du suivi n'a pas légalement de prérogatives particulières à l'égard des services de renseignement.

Le Comité permanent R

Il est composé de trois membres non parlementaires, mais désignés par la Chambre des représentants pour un mandat de six ans renouvelable. Le Président doit être magistrat. Le Comité R est une autorité collégiale. La collégialité est destinée à garantir son indépendance tant à l'égard du gouvernement qu'à l'égard des services eux-mêmes.
Les enquêtes de contrôle sont ouvertes à l'initiative du Parlement (la Commission du suivi), des ministres compétents (Justice pour la Sûreté de l'État et Défense pour le SGRS) ou du Comité R lui-même. Des enquêtes peuvent aussi être ouvertes suite à des plaintes ou dénonciations de particuliers ou de membres ou d'anciens membres des services.
Le Président de la Chambre, qui préside la Commission du suivi, est toujours informé de l'ouverture d'une enquête, de même que les deux ministres concernés si l'enquête porte sur les deux services ou du seul ministre concerné si l'enquête ne porte que sur un service. Cette information est essentielle. D'une part, elle garantit la transparence des enquêtes menées par le Comité R à l'égard du Parlement et du pouvoir exécutif et, d'autre part, lui procure le « *need to know* », et donc l'accès à toutes les informations jugées nécessaires. Dans le cadre d'une enquête, le Comité R dispose de prérogatives importantes :

- accès à tous les locaux, en présence du chef de service ou de son représentant ;
- accès à tous les documents utiles à l'enquête. Le Comité R respecte cependant la règle du tiers service. Pour les documents internes, en cas de réticence d'un service, le président du Comité R tranche en dernier ressort après avis du chef de service ;
- audition de tout membre du personnel et pas seulement les chefs de service. Les membres des services ne peuvent invoquer le secret professionnel à l'égard du Comité R. Ici aussi, en cas de problème, le président du Comité R prend la décision finale après avis du chef de service.

Dans la pratique, le Comité R travaille principalement sur des documents écrits puisqu'il a accès à tous les documents qu'il juge utiles et procède aux auditions

nécessaires, le plus souvent en fin d'enquête.
Le rapport classifié est rédigé et soumis aux trois membres du Comité R en vue d'une approbation. Les recommandations formulées découlent fort logiquement des constatations faites. Ce rapport est transmis aux services concernés pour remarques ou corrections éventuelles. Le Comité R s'inspire de la méthode des audits de telle manière qu'il n'existe plus de désaccord entre le Comité R et les services concernant les constatations matérielles. Ce rapport classifié sera transmis au ministre compétent qui peut encore y réagir.
Un rapport déclassifié est transmis à la Commission du suivi, qui n'a pas souhaité recevoir d'habilitation de sécurité. Il y est discuté lors d'une audience à huis clos. Formellement, la Commission du suivi n'approuve pas le rapport, mais peut suggérer la poursuite ou la reprise de l'enquête sur tel ou tel point déterminé. Lors des discussions à huis clos, la Commission du suivi invite parfois le ministre compétent qui se fait, à cette occasion, accompagner du chef de service ou d'agent désigné par lui.

La Commission du suivi de la Chambre des représentants

Il s'agit d'une commission spéciale composée de 13 députés choisis par la Chambre et présidée par le président de la Chambre. Les membres sont, en principe nommés pour la durée de la législature et n'ont pas de suppléant.
Le fonctionnement de la Commission du suivi est fixé par le règlement de la Chambre et par un règlement d'ordre intérieur. Le respect du huis clos est essentiel pour garantir la confiance entre le Comité R (et les services de renseignement) et la Commission. Malheureusement, des « fuites » sont quelquefois à déplorer… !
Un point important qui fait toujours débat en Belgique et qui étonne souvent l'étranger : l'absence d'habilitation de sécurité des membres de la Commission du suivi qui, en conséquence, ne reçoit pas de rapport classifié. C'est le choix du Parlement… ! Le Comité R estime que ce choix ne l'empêche pas – dans la très grande majorité des cas – d'informer complètement la Commission du suivi. N'oublions pas que la fonction de contrôle appartient au Comité R et que le rapport présenté à la Commission du suivi est destiné à lui permettre d'exercer le contrôle politique sur les ministres et le gouvernement. Pour réaliser ce contrôle politique, il n'est pas nécessaire d'avoir connaissance de données opérationnelles dans la plupart des cas.

Un contrôle transparent

Le Comité R publie chaque année un rapport annuel comprenant une synthèse des enquêtes réalisées et des recommandations formulées. Ce rapport contient également une présentation des autres activités du comité.
Les rapports sont également consultables sur Internet (1). Cette publication très large assure la transparence des activités du Comité R à l'égard du public et assure également une forme d'ouverture des services qui ne publient pas de rapport public de leurs activités.

La conséquence des attentats de Bruxelles

La Commission du suivi actuelle s'est, en quelque sorte, mise en congé suite aux attentats de Bruxelles le 22 mars 2016 puisqu'une Commission d'enquête parlementaire a été instituée. Les enquêtes du Comité R, dont plusieurs avaient été entamées avant les attentats de Bruxelles et Zaventem, ont été examinées par la Commission d'enquête parlementaire. Celle-ci a demandé au Comité R de réaliser des missions complémentaires précises relatives à l'activité des services dans la matière du contre-terrorisme et particulièrement en relation avec les attentats de Paris en 2015 et de Bruxelles en 2016. Il s'agissait d'une décision prise par le Parlement qui permettait l'ouverture d'une enquête beaucoup plus large à l'égard des services de renseignement et de police avec des pouvoirs d'investigation plus étendus pour la Commission d'enquête parlementaire. À situation exceptionnelle, décision exceptionnelle…

Guy Rapaille

Note
(1) www.comiteri.be

Références

Les articles et études concernant le « système belge » de contrôle des services de renseignement sont peu nombreux. Il est permis cependant de citer :

• J.-Cl. Delepière, « Le Comité permanent de contrôle des services de renseignement », *La Sûreté : essais sur les 175 ans de la Sûreté de l'État*, M. Cools, K. Dassen, R. Libert et P. Ponsaers (dir.), Bruxelles, Politeia, 2005, p. 225-240.

• G. Rapaille et J. Vanderborght, « L'herbe est toujours plus verte ailleurs. Sur le contrôle belge des services de renseignement et de sécurité », *Cahiers de la sécurité 2010*, INEHSJ, juillet-septembre, p. 122-123.

• W. Van Laethem et J. Vanderborght (dir.), « Regard sur le contrôle : vingt ans de contrôle démocratique pour les services de renseignement », Anvers, Intersentia, 2013.

• D. Stans, « Le Comité permanent R dans sa relation avec le Parlement et certains acteurs du pouvoir exécutif. Cohérence ou incohérence ? », thèse de doctorat présentée à l'Université de Liège et de Gand, Anvers, Maklu, 2016.

Photo ci-contre : Le 21 novembre 2015, peu après les attentats de Paris, des militaires belges patrouillent dans les rues de Bruxelles alors que le pays est en alerte attentat maximum suite à une évaluation de l'Organe de coordination pour l'analyse de la menace (OCAM). Lorsque le pays sera frappé à son tour en mars 2016, le Comité R, qui contrôle les services de renseignement du pays, soulignera des problèmes structurels dans la diffusion d'informations entre les services de renseignement et l'extérieur, ainsi qu'un problème de moyens qui fait « courir un risque à l'ensemble du processus ». Le Comité R soulignera également que les services de renseignement militaires du pays ne sont pas adaptés pour travailler sur le contre-terrorisme. (© Xinhua/ Zhou Lei)


NTELLIGE
UNITED STATES OF

Services de renseignement

Photo ci-contre : En mars 2017, Wikileaks publiait près de 9000 documents présentés comme internes à la CIA et dévoilant les techniques et « l'arsenal » de piratage et de surveillance de l'agence américaine – transformation de télévisions en appareils d'écoute, stratégie de contournement des applications de cryptage, élaboration de programmes malveillants, contrôle de véhicules ou d'appareils électroniques… Ces documents démontrent, selon le site créé par Julian Assange, que la CIA opère de la même façon que la NSA – principale agence américaine en charge de la surveillance électronique et dont l'ampleur du système de surveillance avait également été largement exposé –, mais avec moins de supervision. (© Sal Loeb/AFP)

analyse

Par **Éric Denécé**, directeur du Centre français de recherche sur le renseignement (CF2R).

Quels défis pour le renseignement français ?

Si la France constitue l'un des rares pays à surveiller l'évolution de toutes les zones de la planète, ses services – quoique dotés de capacités de renseignement et d'action très honorables – doivent faire face à des limites imposées par un dispositif sous-dimensionné, qui n'est pas à la hauteur d'un pays engagé sur de multiples théâtres et devenu une cible prioritaire du terrorisme djihadiste.

La France est aujourd'hui la seule nation de l'Union européenne à disposer d'une panoplie presque complète des moyens de renseignement techniques (stations d'écoutes, drones, satellites), et bénéficie donc d'une véritable indépendance en matière de renseignement. Cela lui a permis de conserver son autonomie d'appréciation des crises internationales. Ainsi, en 2003, à l'occasion de l'invasion de l'Irak par les États-Unis, Paris a pu s'opposer aux arguments américains parce que la Direction du renseignement militaire (DRM) a pu fournir aux autorités gouvernementales des renseignements contredisant la version construite par Washington pour justifier son action. Depuis l'opération « Serval » (2013), DGSE (Direction générale de la sécurité extérieure) et DRM sont largement impliquées dans la surveillance du Sahel, dans le cadre de la lutte contre les groupes terroristes qui y opèrent.

Le renseignement français dans son ensemble n'est toutefois pas à la hauteur de la menace terroriste, des enjeux internationaux, ni de nos ambitions diplomatiques et miliaires. En effet, pour un pays membre du Conseil de sécurité des Nations Unies, engagé depuis des décennies dans de nombreuses interventions extérieures, et cible prioritaire des terroristes djihadistes, notre dispositif est, humainement et financièrement, largement sous-dimensionné. Parallèlement, de nombreux aspects organisationnels et fonctionnels doivent être revus et améliorés.

Photo ci-dessus :
Un garde de sécurité se tient devant le quartier général de la DGSE à Paris. Selon le patron de la Direction générale de la sécurité extérieure, Bernard Bajolet, le service Action de la DGSE serait utilisé « au plein de ses capacités » depuis l'intervention française au Mali en janvier 2013, en raison d'un accroissement du rythme et de l'intensité des opérations sur différents théâtres, parmi lesquels « l'Afrique subsaharienne, la zone afghano-pakistanaise, la Corne de l'Afrique, la Syrie, l'Europe, la Libye et l'Égypte ». (© AFP/ Martin Bureau)

Un manque de culture du renseignement

La première des faiblesses de notre dispositif de renseignement est *l'incompréhension, le dédain et le désintérêt de la classe politique* à l'égard de cette profession. En effet, si la discipline, tour à tour, fascine ou révulse, elle n'a jamais donné lieu à une approche très rationnelle, ni à un intérêt marqué des autorités politiques. Ce manque de considération les rend incapables de bien manager cet important domaine de l'action étatique, à la différence de la plupart de leurs partenaires étrangers. En dépit des discours ronflants consécutifs aux récents attentats terroristes, les dirigeants gouvernementaux n'ont jamais accordé la priorité au renseignement, qui demeure le parent pauvre de notre appareil sécuritaire.

> *« La première des faiblesses de notre dispositif de renseignement est l'incompréhension, le dédain et le désintérêt de la classe politique à l'égard de cette profession. »*

La conséquence directe de ce désintérêt est *l'insuffisance des effectifs et des moyens attribués globalement au renseignement*. Comptant environ 18 000 personnes toutes structures confondues et 14 000 personnes pour ce que l'on nomme la « communauté du renseignement » au sens strict (voir le détail service par service dans le Focus p. 43), le renseignement français dans son ensemble est en sous-effectif et en sous-dotation budgétaire par rapport à celui de nos principaux alliés (États-Unis, Royaume-Uni, Allemagne, Israël).

Au Royaume-Uni – pays dont les ressources, la population et les responsabilités internationales sont similaires à celles de la France –, la communauté du renseignement regroupe un peu plus de 20 000 personnes (30 000 au sens large) et est en constant accroissement. En matière de renseignement technique (interceptions, cryptographie, informatique, etc.), les effectifs et les moyens britanniques sont 3,5 fois supérieurs aux nôtres. Et Londres a encore annoncé, en décembre 2015, le recrutement de 2000 « *geeks* » pour développer ses capacités de cybersécurité et de cyber-renseignement. Sur le plan financier, au cours des dix dernières années, les Britanniques ont augmenté leur budget et de près de 50 % et cet effort se poursuit [voir également p. 72 de ces *Grands Dossiers*, NdlR].

En Allemagne, les trois services de renseignement fédéraux regroupent plus de 18 000 personnes. Cela signifie que les Allemands, qui n'ont pas nos implications internationales, disposent d'effectifs supérieurs aux nôtres [voir également p. 80 de ces *Grands Dossiers*, NdlR].

Israël, qui compte moins de 9 millions d'habitants, dispose d'une communauté du renseignement de plus de 18 000 personnes, soit 30 % supérieure à la nôtre. En particulier, le service de sécurité intérieure (*Shin Beth*), chargé de lutter contre le terrorisme, compte 7000 personnes, contre moins de 4000 pour notre Direction générale de la sécurité intérieure (DGSI) ; et en matière de renseignement technique, les effectifs et les moyens israéliens sont plus de trois fois supérieurs aux nôtres. L'intensité et la permanence des menaces expliquent évidemment l'importance accordée au renseignement par ce pays [voir également p. 53 de ces *Grands Dossiers*, NdlR].

Enfin, aux *États-Unis* – pays auquel il est difficile de se comparer –, la communauté du renseignement *stricto sensu* compte plus de 150 000 membres. En complément, près de 1300 structures gouvernementales et 1900 compagnies privées réparties sur 10 000 sites à travers le pays sont impliquées sur le renseignement ou la lutte antiterroriste, illustrant le recours massif aux sous-traitants privés. Le budget américain du renseignement s'élève approximativement à 75 milliards de dollars. Il représente 10 % du budget annuel de la Défense américaine et dépasse celui du Trésor et de plusieurs autres ministères. Les États-Unis consacrent ainsi au renseignement un budget supérieur à celui que la France attribue à la Défense ! Pour mémoire, la NSA, chargée des interceptions et de la cryptographie, dispose d'un budget annuel estimé à 15 milliards de dollars (25 fois le budget total de la DGSE et 40 fois celui de sa direction technique, qui fait le même métier). Toutefois, ce gigantisme n'est pas un gage d'efficacité [voir également p. 48 de ces *Grands Dossiers*, NdlR].

Photo ci-dessus :
Le 15 février 2017, le président François Hollande faisait part de ses inquiétudes face au risque de cyberattaques à l'occasion de la prochaine présidentielle française. Alors que la menace terroriste occupe l'ensemble des services de renseignement, il convient de ne pas oublier les autres menaces telles que celles en provenance du cyberespace, comme en attestent les révélations de la CIA sur le rôle qu'aurait joué la Russie dans les élections américaines. La DGSE, qui s'inquiète de l'ingérence d'influenceurs favorables à Donald Trump et Vladimir Poutine, semble estimer que des phénomènes analogues seraient à l'œuvre en France. (© European Council)

Des moyens insuffisants

La comparaison de notre « effort » avec celui de nos principaux alliés met en lumière *l'insuffisance des moyens français* consacrés au renseignement. En proportion des populations respectives, il faudrait que nos services comptent plus de 40 000 personnes pour égaler l'effort des États-Unis, 21 000 pour égaler celui des Britanniques et près de 17 000 pour égaler celui des Allemands. Nous en sommes loin ! Et si nous faisions un effort similaire à celui d'Israël, nous devrions compter plus de 140 000 membres dans les services. L'information et la sécurité ont indéniablement un prix.

Sur le plan budgétaire, pour mémoire, tous services confondus, en France, les financements attribués au renseignement n'ont progressé que de 9 % entre 2001 et 2005, alors que les augmentations budgétaires atteignaient en moyenne 40 % outre-Manche et outre-Atlantique. À titre de comparaison, en 2007, le budget des services britanniques chargés du renseignement

Photo ci-dessus :
Le 5 mai 2015, l'Assemblée nationale votait la loi relative au renseignement par 438 voix contre 86 (42 abstentions). Si certains ont dénoncé une loi « liberticide » en raison de méthodes de surveillance intrusives et massives, cette loi fut considérée comme une avancée par les services de renseignement français, dans un pays qui était l'une des dernières démocraties occidentales à ne pas disposer d'un cadre légal cohérent et complet régissant l'action des services de renseignement. Cette loi doit permettre de renforcer les pouvoirs des services de renseignement dans plusieurs domaines tels que la défense des intérêts majeurs de la politique étrangère, celle des intérêts économiques, industriels et scientifiques majeurs de la France, ainsi que la prévention des atteintes à la forme républicaine des institutions et des violences collectives de nature à porter atteinte à la sécurité nationale. (© Dutourdumonde Photography)

s'élevait à 3,31 milliards d'euros, soit près de 4,5 fois celui alloué aux services français (743,5 millions d'euros), sans prendre en compte le soutien technique et financier que leur apportaient les États-Unis.
En France, en 2015, les trois services dépendant du ministère de la Défense (DGSE, DRM, DPSD) ne représentaient (hors rémunérations) que 0,7 % de son budget… lequel ne s'élevait lui-même qu'à 1,7 % du budget national. Peut-on parler dès lors d'une priorité accordée au renseignement ?
Ces insuffisances humaines et budgétaires placent nos services – à l'exception de la DGSE – dans *une situation de dénuement critique*. Vétusté et surpopulation des locaux, usure et insuffisance du parc automobile, vétusté et insuffisance du parc informatique, des équipements et des moyens techniques pour la surveillance ; et surtout, effectifs sous-dimensionnés pour pouvoir surveiller efficacement terroristes et activistes qui menacent notre pays.

Des réformes sources de déséquilibre

Ces lacunes ont été accrues par les réformes récentes qui ont nui à l'efficacité de la lutte antiterroriste. Si nul ne conteste qu'une réorganisation du renseignement intérieur était nécessaire, la réforme de 2008 a remis en cause un système qui reposait sur une logique éprouvée et a entraîné de nouveaux déséquilibres en privilégiant la centralisation des opérations entre les mains d'une DGSI à vocation nationale, au détriment du renseignement de terrain et du quadrillage territorial. De plus, cette réforme n'a pas réduit le nombre des services : en Île-de-France, quatre services dépendant de quatre directions distinctes opèrent parallèlement pour un résultat inférieur ou égal à ce qui existait avant 2008. Une telle situation n'est pas faite pour réduire les rivalités interservices.
Il en résulte *une organisation du renseignement intérieur inappropriée*. La DGSI fonctionne avec une culture du contre-espionnage héritée de la guerre froide (forte centralisation, cloisonnement interne, culte du secret excessif). Cette approche, adaptée pour lutter contre l'espionnage et le terrorisme étrangers de nature étatique (comme dans les années 1980), n'est pas appropriée pour faire face à un terrorisme des banlieues. Avec la suppression des Renseignements généraux [voir également p. 15 de ces *Grands Dossiers*, NdlR], nous nous sommes privés d'un maillage territorial essentiel dans le cadre de la lutte contre un terrorisme domestique. Car c'est bien en surveillant comme ils le faisaient les cités sensibles, les communautés immigrées ou étrangères, les petits trafics, les gangs et les violences urbaines, les mosquées et les associations que l'on détecte les phénomènes de radicalisation. Tous les experts observent qu'il y a un passage de plus en plus fréquent de la contestation à la violence puis au terrorisme, pour des causes et des groupes divers. Séparer le renseignement « fermé » de « l'ouvert » n'a donc pas de sens. De plus, il n'est possible de lutter contre des terroristes *homegrown* (« ayant grandi sur le territoire national ») que si l'on est présent dans les banlieues à risque et si l'on connaît leur dynamique.

> *« Avec la suppression des Renseignements généraux, nous nous sommes privés d'un maillage territorial essentiel dans le cadre de la lutte contre un terrorisme domestique. »*

On observe également un important déficit en matière de formation**.** Dans tous les services, la formation initiale et continue reste notoirement insuffisante. Elle laisse notamment toujours à désirer dans les services chargés de suivre l'islam radical, en particulier pour le renseignement territorial. Il n'y a toujours pas d'école du renseignement au ministère de l'Intérieur et les formations sur l'islam sont sommaires, quand elles existent.

D'autres menaces négligées au profit du terrorisme

L'acuité de la menace actuelle provoque par ailleurs une polarisation excessive sur le terrorisme. Tous les services y consacrent l'essentiel de leurs moyens. Si cela est légitime, cela signifie que d'autres enjeux majeurs pour notre sécurité sont négligés : la criminalité internationale, l'espionnage politique et économique (États-Unis, Russie, Chine, etc.), et la montée en puissance de nouveaux phénomènes violents pouvant déboucher sur le terrorisme (extrémisme politique, autonomismes, mouvements sociétaux violents, etc.). En particulier, nos moyens consacrés à la cyberdéfense des administrations sont notoirement insuffisants, même si des efforts récents ont été entrepris.
Si les mesures annoncées à partir de 2015 sont positives, elles demeurent insuffisantes. Les évolutions de crédits et d'effectifs annoncés – comme celles des deux dernières décennies – restent en effet assez dérisoires. Ce ne sont pas quelques centaines de postes ou quelques millions d'euros supplémentaires qui modifieront la donne. Pour répondre aux défis futurs du renseignement, il est désormais nécessaire de changer d'échelle. Notre pays ne peut donc faire l'économie d'un dispositif de renseignement performant, au risque d'assister à l'inexorable recul de son influence internationale et de perdre la maitrise de son destin.

Éric Denécé

La communauté française du renseignement

Des services complémentaires aux compétences distinctes

Par **Éric Denécé**, directeur du Centre français de recherche sur le renseignement (CF2R).

La constellation des administrations françaises du renseignement compte une douzaine de services ou départements spécialisés, une demi-douzaine d'organes de coordination, ainsi que divers organismes de contrôle.

Les services de renseignement extérieur (services offensifs)

Un service « offensif » est une administration qui a pour but d'apporter aux autorités gouvernementales les informations qu'elles ont demandées (politiques, économiques, diplomatiques, militaires). Il a pour terrain d'action « l'étranger ». Il est généralement dénommé « service de renseignement ».

Dans notre pays, deux services sont chargés du renseignement extérieur ; ils dépendent tous les deux du ministère de la Défense :

• La *Direction générale de la sécurité extérieure* (DGSE). Forte de plus de 6500 femmes et hommes, la DGSE est le plus important des services français. Elle est chargée de rechercher, à l'étranger, les renseignements intéressant la sécurité de la France, ainsi que de détecter et d'entraver les activités d'espionnage et de terrorisme contre les intérêts français. L'une des caractéristique de la DGSE est d'être un « service intégré », c'est-à-dire qu'elle est, à elle seule, une petite communauté du renseignement, cumulant les fonctions de recherche humaine, de recherche technique, d'analyse et d'action. Autant de métiers qui relèvent, le plus souvent, de services différents à l'étranger.

• La *Direction du renseignement militaire* (DRM) – forte de 1700 personnels – a pour mission d'apporter aux forces armées – et au gouvernement – les renseignements nécessaires à l'engagement de nos forces et au succès de leurs opérations. Elle pilote et coordonne les moyens de renseignement des trois armées et est en charge du renseignement d'imagerie (satellites d'observation de la Terre).

Les services de sécurité (services défensifs)

Un service « défensif » est une administration dont la finalité est d'assurer la sécurité (nationale, économique, militaire, etc.). Il a pour terrain d'action le territoire national. On parle alors de « service de sécurité ».

Photo ci-contre : Bernard Bajolet, directeur de la DGSE depuis 2013. En 2017, en pleine élection présidentielle, quatre des plus importants services de renseignement français vont voir leur dirigeant arriver à la fin de leur mandat et de leur carrière dans la fonction publique. Outre Bernard Bajolet, dont le mandat avait déjà été prolongé, Patrick Calvar (DGSI), René Bailly (DRPP) et à priori Christophe Gomart (DRM) sont sur le départ. (© Claude Truong-Ngoc)

Les services défensifs sont plus nombreux et dépendent des ministères de l'Intérieur, de la Défense, de la Justice et de l'Économie :

• La *Direction générale de la sécurité intérieure* (DGSI) regroupe 3600 personnels. Elle a pour compétence la lutte, sur le territoire français, contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la nation : subversion, extrémisme violent, espionnage et terrorisme.

• La *Direction de la protection et de la sécurité de la Défense* (DPSD) compte 1100 personnels. Elle est présente sur l'ensemble du territoire national et sur tous les théâtres où les forces françaises sont engagées. Ses missions sont le renseignement de sécurité, la protection des forces, des systèmes d'information et du patrimoine industriel et économique lié à la Défense.

• La *Direction nationale du renseignement et des enquêtes douanières* (DNRED), (800 personnes) est chargée de la collecte du renseignement relatif aux trafics internationaux de toute nature (armes, drogue, contrebande).

• Le service *Traitement du renseignement et action contre les circuits financiers clandestins* (TRACFIN), est la cellule nationale de lutte contre le blanchiment des capitaux et le financement du terrorisme (100 personnes).

• Le *Service central du renseignement territorial* (SCRT) – 2000 personnels –, rattaché à la police nationale, est chargé de la surveillance des mouvements revendicatifs ou protestataires et de la contestation politique violente.

• La *Direction du renseignement de la préfecture de Police* (DRPP), regroupant 800 personnels, est chargée du renseignement antiterroriste et antisubversion en région parisienne (12 millions d'habitants).

• Le *Service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée* (SIRASCO, quelques dizaines de personnels), créé en

2009, est chargé de surveiller toutes les organisations criminelles transnationales opérant sur le sol français. Il est également rattaché à la police nationale.

• La Gendarmerie nationale participe à l'action de renseignement à travers sa *Sous-direction de l'anticipation opérationnelle* (SDAO, 100 personnes), qui est présente dans tous les départements français et son *Bureau de lutte antiterroriste* (BLAT).

• Le *Service de l'information stratégique et de la sécurité économique* (SISSE, une vingtaine de personnes) est en charge de l'intelligence économique.

• Le *Groupe interministériel de contrôle* (GIC), qui dépend de Matignon, est en charge des écoutes administratives et judiciaires sur le territoire national.

• L'*Agence nationale de sécurité des systèmes d'information* (ANSSI) – rattachée au Premier ministre et comptant 300 personnels – est en charge de la cybersécurité au niveau national.

• Enfin, l'administration pénitentiaire (ministère de la Justice) dispose d'un Bureau du renseignement (dénommé EMS3), ne comptant que quelques dizaines de personnels, chargé de surveiller les détenus les plus dangereux, notamment les islamistes radicaux.

Stricto sensu, seules la DGSE, la DRM, la DGSI, la DPSD, la DNRED et TRACFIN composent la « Communauté française du renseignement », qui compte près de 14 000 membres (une fois intégrés les renforts décidés après les attentats de janvier 2015, elle devrait en compter près de 16 000 en 2018). Avec les autres administrations listées, ce total s'élève à 18 000 personnels.

Les organes d'orientation, de coordination et de synthèse

Les services spécialisés ou contribuant au renseignement sont pilotés ou coordonnés au travers de différentes structures.

• Le *Conseil de défense et de sécurité nationale* (CDSN) présidé par le chef de l'État et réunissant le Premier ministre et les ministres de la Défense, de l'Intérieur, de l'Économie, du Budget et des Affaires étrangères, est chargé de définir les orientations et de fixer les priorités en matière d'opérations militaires, de renseignement, de sécurité intérieure ou de lutte contre le terrorisme.

• Le *Secrétariat général de la défense et de la sécurité nationale* (SGDSN) est un organisme de coordination interministériel chargé de l'ensemble des dossiers intéressant la sécurité intérieure et extérieure du pays. Il assure le secrétariat du Conseil de défense et de sécurité nationale.

• Le *Coordonnateur national du renseignement* (CNR), placé sous la responsabilité du président de la République, est son conseiller en la matière. Il est chargé de définir les orientations stratégiques et les priorités du renseignement, de s'assurer que les services disposent des moyens nécessaires (personnels, budget), de coordonner leurs actions et de veiller à la bonne coopération des services.

• L'*Académie du renseignement* – rattachée au Premier ministre – est chargée de développer des programmes de formation interagences, grâce auxquels les différents services apprennent à mieux se connaître afin de mieux travailler ensemble.

• Le ministère de l'Intérieur a mis sur pied un *État-major opérationnel de prévention du terrorisme* (EMOPT) afin de coordonner l'action de ses services (gendarmerie, police, sécurité civile, etc.).

• La police nationale dispose enfin de l'*Unité de coordination de lutte antiterroriste* (UCLAT).

Les organes de contrôle

Enfin, il convient de rappeler que les services de renseignement font l'objet d'un triple contrôle parlementaire et administratif.

• Avec beaucoup de retard sur les autres pays occidentaux, en 2007, la France a mis sur pied une *Délégation parlementaire au renseignement* (DPR), composée de huit parlementaires – quatre membres de l'Assemblée nationale et quatre du Sénat. Elle reçoit du gouvernement des informations sur les budgets, l'activité générale et l'organisation des services de renseignement. Chaque année, elle remet un rapport au président de la République, au Premier ministre et aux présidents de l'Assemblée nationale et du Sénat sur l'activité des services de renseignement et de sécurité français.

• La *Commission nationale de contrôle des techniques de renseignement* (CNCTR) contrôle – notamment – le bon usage des écoutes téléphoniques et vérifie que les services n'outrepassent pas leurs droits.

• Enfin, depuis les origines de la Ve République, les services font l'objet d'un contrôle financier étroit de la *Cour des comptes* et de la *Commission de vérification des fonds spéciaux* (CVFS).

Éric Denécé

Photo ci-contre : Dans les locaux de la DGSE, boulevard Mortier à Paris. Une étude établie par l'IFOP en septembre 2016 a montré que 71 % des Français estiment qu'il est justifié que le service de renseignement français ne soit pas soumis aux règles de transparence auxquelles l'État est tenu. Cette campagne de communication de la DGSE s'inscrivait dans la volonté de son directeur, Bernard Bajolet, « d'expliquer aux Français que nous sommes là pour les protéger, pas pour les surveiller ». (© AFP/Martin Bureau)

Avec la collaboration
de la Chaire Raoul-Dandurand
UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

Révélations, polémiques et nouvelles menaces : quels défis pour le renseignement américain ?

Entretien avec **Julien Tourreille**, directeur-adjoint de l'Observatoire sur les États-Unis, chaire Raoul-Dandurand, Université du Québec à Montréal (UQAM).

Fondée en 1947, la CIA constitue l'un des services de renseignement les plus connus au monde. Quelles sont ses principales missions et comment expliquer cette « popularité » ?

Julien Tourreille : La CIA fut créée par la loi sur la sécurité nationale de 1947, qui établit par ailleurs le Conseil de sécurité nationale (le NSC) et le département de la Défense. Sa mission principale est de fournir aux décideurs politiques – en premier lieu le Président – une évaluation de l'environnement stratégique et des menaces qui en émanent. Pour ce faire, elle collecte et analyse du renseignement de nature politique, économique, et scientifique. Cette mission d'analyse prévaut sur les opérations clandestines, domaine dans lequel les échecs (la Baie des Cochons) et les dérives (les prisons secrètes après le 11 septembre 2001) alimentent les fantasmes sur la puissance de l'organisation et, surtout, ternissent sa réputation.

L'agence est organisée en quatre grands secteurs : administration et gestion, science et technologie, opérations clandestines, et analyse. Le dernier directeur de la CIA du président Obama, John Brennan, a cherché à décloisonner ce fonctionnement au profit d'une approche plus transversale. Cette réforme est considérée comme la plus ambitieuse depuis la création de l'agence. Ses résultats restent néanmoins difficiles à évaluer (1).

Trois facteurs peuvent expliquer la « popularité » de la CIA. Tout d'abord, elle fait figure de « doyenne » d'une communauté du renseignement au sein de laquelle elle est la seule agence indépendante. Ensuite, la prééminence des États-Unis sur la scène internationale depuis la fin de la Deuxième Guerre mondiale a conféré au renseignement une place fondamentale dans l'élaboration et la conduite de la politique étrangère et de défense des États-Unis. Enfin, l'histoire de la CIA est riche et turbulente. Elle est faite de succès notables (la crise des missiles de Cuba), d'échecs retentissants (la mauvaise évaluation de la détermination nord-vietnamienne à combattre, le 11 septembre 2001, les armes de destruction massive de Saddam Hussein), et d'implications dans des épisodes sombres de l'histoire de certains pays (le renversement de Mossadegh en Iran en 1953, d'Allende au Chili en 1973, les vaines tentatives d'assassinat de Fidel Castro).

Le directeur de la CIA est nommé directement par le président américain. Quelles sont les relations entre la CIA et la Maison-Blanche ? L'agence a-t-elle un rôle ou une influence politique ?

Le directeur de la CIA est choisi par le Président et sa nomination doit être confirmée par le Sénat. L'influence de la CIA dépend essentiellement du talent de persuasion de son directeur et de la relation qu'il entretient avec le Président. L'histoire de la CIA démontre que la confiance ne fut pas toujours au rendez-vous entre ces deux personnages. Certains directeurs avaient l'oreille du Président et pouvaient donc défendre les intérêts et les points de vue de l'agence dans un jeu bureaucratique parfois rude (Allen Dulles sous Eisenhower ou plus récemment John Brennan sous Obama). D'autres en revanche n'étaient que très peu écoutés, tels Richard Helms sous Nixon ou James Woolsey sous Clinton. Dans ces cas, l'influence de l'agence dans le processus décisionnel en pâtit, souvent au détriment de la qualité de la décision. Malgré ses problèmes (inertie, ethnocentrisme, manque d'imagination… (2)) et ses défaillances, la CIA produit en effet des rapports considérés comme les plus justes parmi tous ceux émanant de la communauté.

Le risque le plus grand auquel fait face la CIA est la politisation du renseignement. D'une part, les décideurs politiques peuvent chercher à exploiter, à interpréter, ou même à orienter le renseignement afin de légitimer des positions préétablies. C'était par exemple le cas sous Reagan avec l'exagération de la menace des missiles soviétiques. Le cas récent le plus fameux est la pression exercée par le vice-président Cheney afin d'obtenir de la CIA qu'elle appuie l'argument de la présence d'armes de destruction massive en Irak à la veille de la guerre de 2003. Cet épisode fut l'un des moins glorieux pour l'agence et surtout pour son directeur George Tenet, qui fut incapable de protéger l'intégrité intellectuelle de ses personnels et de présenter un contre-argumentaire solide au Président afin d'éviter de commettre une erreur qui hante encore les États-Unis et le Moyen-Orient.

Avec la chute de l'Union soviétique, la CIA a perdu son « meilleur ennemi » et a dû s'adapter à une nouvelle situation mondiale. Comment s'est passée cette transition et quelle est l'efficacité de la CIA face aux nouvelles menaces ?

La disparition du « meilleur ennemi » soviétique a ouvert une période difficile pour la CIA dont l'expansion, tant au niveau de ses moyens que de son rôle dans le processus décisionnel, a été favorisée par la guerre froide. La transition vers le monde post-guerre froide fut hasardeuse. Non seulement elle n'avait pas anticipé l'implosion de

Photo ci-contre : Mike Pompeo, ancien militaire et critique virulent de l'administration Obama, est le nouveau directeur de la CIA depuis janvier 2017. Cet homme politique, proche du vice-président élu, Mike Pence, s'est notamment prononcé contre l'accord conclu avec l'Iran, et a apporté son soutien aux programmes de surveillance de la NSA. (© Gage Skidmore)

l'URSS, mais elle n'a pas su prévoir des évènements majeurs, tels que le génocide au Rwanda en 1994. La faillite la plus spectaculaire pour laquelle elle a été abondamment blâmée est sans conteste son incapacité à contrecarrer l'attaque terroriste du 11 septembre 2001. La communauté du renseignement avait pourtant perçu les bruits de la menace terroriste. Elle était au fait des velléités d'Oussama ben Laden de frapper les intérêts américains. Elle a été en revanche bien incapable d'anticiper et d'empêcher ces attaques.

Quelles sont ses priorités actuelles en matière de sécurité ?

Depuis plus de 15 ans, la lutte contre le terrorisme est au cœur des préoccupations de l'agence. Cela a donné lieu à des dérives, telles les prisons secrètes, les extraditions extra-judiciaires, ou encore le recours à des méthodes d'interrogatoire assimilables à de la torture. Barack Obama a voulu rompre avec ces dérives en interdisant clairement les méthodes d'interrogatoire améliorées, en acceptant que le Sénat enquête de manière exhaustive sur les exactions de la CIA et en publie un rapport volumineux en décembre 2014.

La longue et laborieuse traque de Ben Laden a illustré les lacunes du renseignement américain, mais aussi sa détermination.

Aujourd'hui, celui-ci gère même plutôt bien la menace terroriste et mériterait de rééquilibrer son attention sur des menaces plus classiques, provenant d'acteurs étatiques, tels la Chine, la Russie, ou la Corée du Nord. À divers degrés, les agissements de ces États méritent une analyse précise et rigoureuse afin de préserver la stabilité et la sécurité internationales. Or, après plus de 15 ans de lutte contre le terrorisme, il est tout à fait possible que la communauté du renseignement américaine ne dispose pas de l'expertise requise sur ces pays et soit prise au dépourvu par la multiplicité des menaces. C'est tout le défi auquel elle est confrontée.

Ci-contre : Emblèmes des 17 services de la communauté du renseignement des États-Unis. (© CIA)

La communauté du renseignement américain est composée de 17 entités appartenant à plusieurs ministères. Comment est gérée la coordination entre ces services ?

À l'origine, ce rôle de coordination était dévolu à la CIA et à son directeur. Elle n'est pourtant jamais parvenue à maîtriser et assurer la coordination de ces entités. La communauté du renseignement demeure largement une « fédération tribale » (3) dans laquelle chaque agence défend farouchement sa culture organisationnelle, ses intérêts, et est en compétition avec les autres pour l'attention du Président et l'octroi de ressources.

Ce manque de coordination a eu des répercussions majeures. L'exemple le plus éloquent est encore une fois le 11 septembre 2001. La Commission sur le 11-Septembre a essayé de corriger ce manque en créant un poste de directeur national du renseignement (le Director of National Intelligence, ou DNI) (4). Celui-ci est également nommé par le Président (et soumis à confirmation par le Sénat). Or, la situation n'est pas totalement réglée. Chaque agence a tendance à se tourner davantage vers le département auquel elle est rattachée plutôt que de jouer collectif et de faciliter la tâche du DNI.

La CIA est la seule agence de cette communauté qui soit indépendante. Les autres relèvent du département d'État (tel le Bureau of Intelligence and Research), de l'Énergie, du Trésor, de la Justice (en particulier la Drug Enforcement Agency et le Federal Bureau of Investigation) et de la Défense. Les agences rattachées à ce dernier département accaparent en fait 50 % du budget alloué au renseignement. Parmi les agences relevant du Pentagone, la National Security Agency (NSA), en charge du renseignement électronique, est sans conteste la plus connue et la plus controversée [voir p. 48 de ces *Grands Dossiers*, NdlR].

Une autre agence qui devrait susciter une attention soutenue est la moins connue National Geospatial-Intelligence Agency (la NGA, anciennement National Imagery and Mapping Agency). Dans la banlieue sud de Washington D.C., son quartier général est le troisième bâtiment le plus grand dans la région de la capitale fédérale. Chargée d'analyser les images et vidéos captées par les satellites espions et les drones, elle n'a pour l'instant pas été impliquée dans des scandales d'espionnage domestique, contrairement à la CIA et à la NSA. Mais compte tenu de la croissance constante de l'usage des drones au-dessus même du territoire américain, une telle possibilité est tout à fait envisageable (5).

Alors que la campagne présidentielle américaine a été marquée par des soupçons de cyberattaques russes, le nouveau président Donald Trump entretient une relation compliquée avec le renseignement américain. En janvier dernier, l'ex-directeur de la CIA, John Brennan, demandait à ce dernier de se « discipliner » et d'apaiser ses relations avec les agences de renseignement.

Photo ci-dessous : Manifestation organisée dans les rues de Washington pour demander la fermeture de la prison de Guantanamo, la plus célèbre des prisons secrètes (ou « *black sites* ») utilisées par la CIA. Le nouveau président américain Donald Trump serait favorable à ce que la CIA puisse à nouveau utiliser ces prisons secrètes en territoire étranger. (DR)

Photo ci-contre : Dianne Feinstein, sénatrice démocrate de Californie et présidente de la Commission spéciale du Sénat sur le renseignement de 2009 à 2015. En 2014, elle a jeté un pavé dans la mare fédérale en déclarant avoir découvert que la CIA aurait espionné les enquêteurs de sa commission qui « creusait » dans les archives de l'agence afin de dresser un inventaire des pratiques répréhensibles d'interrogatoires et de détention employées au nom de la « guerre contre la terreur » – pratiques abolies à l'arrivée de Barack Obama au pouvoir. (© US Senate/Becky Hammel)

Comment expliquer cette relation tendue ?
L'expression publique et virulente du mépris du président Trump pour les agences de renseignement est sans précédent – il a qualifié les fuites provenant de la communauté de comportement digne de « l'Allemagne nazie » (6). La cause de cette relation tendue est le rôle de la Russie dans la campagne électorale américaine. Trump s'est certes résigné à accepter les conclusions du renseignement américain selon lesquelles Moscou a interféré dans cette campagne. En revanche, il considère comme une attaque personnelle sans fondement l'évocation d'une collusion entre des membres de son entourage et Moscou, dossier sur lequel le directeur du FBI a reconnu en commission au Congrès que son organisation enquête.
Le risque de cette relation tendue, au-delà d'alimenter le feuilleton sur le rôle de la Russie dans les dernières élections, est qu'une présidence qui ne s'intéresse pas ou ne croit pas au travail du renseignement se retrouve bien mal outillée pour gérer une crise. Du côté du renseignement, le risque est que les personnels se protègent des foudres des décideurs politiques en faisant preuve d'un zèle bureaucratique et d'une prudence excessifs limitant leur imagination, leur prise de risque et leur capacité à anticiper des événements majeurs.

Donald Trump s'en est également pris au FBI, lui reprochant de ne pas avoir colmaté les fuites dans les médias et l'a qualifié de « totalement incapable » de mettre fin aux agissements de ceux qui laissent filtrer des informations ayant trait à la sécurité nationale du pays. En octobre dernier, le directeur du FBI était également dans la tourmente après avoir été accusé de s'être immiscé dans la campagne présidentielle à quelques jours du scrutin en dévoilant des détails portant sur l'affaire des emails d'Hillary Clinton. *Quid* de l'indépendance du FBI avec la sphère politique ?
La réputation parfois sulfureuse du FBI remonte à son fondateur et premier directeur, John Edgar Hoover. La sortie du directeur Comey sur les emails de Hillary Clinton continuera certainement d'alimenter les suppositions sur le rôle politique du Bureau, mais il ne faudrait pas exclure que le directeur ait tout simplement commis une maladresse en voulant se protéger d'une accusation de favoritisme politique. En d'autres termes, il aurait fait preuve d'un excès de zèle en matière de transparence. Par ailleurs, le fait que le FBI mène une enquête poussée sur le rôle de la Russie dans la campagne électorale de 2016 et sur les liens entre l'entourage de Trump et Moscou laisse à penser que le Bureau n'est pas nécessairement au service d'un parti ou d'un autre.

Début mars, Donald Trump a accusé son prédécesseur, Barack Obama, de l'avoir placé sur écoute pendant la campagne électorale. Cette accusation d'espionnage a été jugée sans fondement par le patron du FBI, James Comey. Est-il possible de mettre des candidats à la présidentielle sur écoute ? Le président américain en a-t-il le pouvoir ?
L'accusation de Trump à l'endroit d'Obama est sans fondement, comme l'a clairement exprimé à deux reprises James Comey. Un président ne peut tout simplement pas décider de la mise sur écoute d'un candidat à la présidentielle – pas plus que de tout autre citoyen – sans avoir l'autorisation de tribunaux spécialisés. La procédure est donc strictement encadrée et Obama n'aurait assurément pas eu l'autorisation pour de telles écoutes.
Ceci étant, une communication d'un citoyen américain avec un étranger peut être interceptée. Edward Snowden a révélé l'existence d'un gigantesque mécanisme de siphon des communications vis-à-vis duquel les citoyens américains ne sont pas totalement protégés. Par ailleurs, dans le cadre d'une surveillance d'acteurs étrangers, par exemple des diplomates de haut rang d'un pays rival (voire même ami), il est fort possible que les communications d'un citoyen américain avec une telle personne soient interceptées. C'est d'ailleurs ce sur quoi le FBI et les commissions du Congrès cherchent à faire la lumière dans l'affaire russe.

Quel est l'intérêt de Donald Trump à s'en prendre ainsi à son prédécesseur ?
Trump professe de telles accusations contre Obama pour deux raisons. D'une part, il considère depuis des mois que toute cette histoire russe est destinée à nuire à sa légitimité. Il y voit la main de démocrates, ou d'alliés de ceux-ci, désireux de justifier la défaite de Clinton. D'autre part, il cherche clairement à détourner l'attention d'une affaire autrement plus grave et sur laquelle il semble manifestement y avoir matière à enquêter et à se poser des questions, voire même entreprendre des actions en justice : c'est la question des liens entre l'entourage de Trump et la Russie. Il est avéré que Moscou a interféré dans le processus électoral, avec pour objectif de nuire à Hillary Clinton. Il reste à savoir s'il y avait une collusion entre l'entourage de Trump et la Russie dans cette histoire. Celle-ci est loin d'être terminée, des républicains éminents tels John McCain appellent même à une commission d'enquête indépendante et les répercussions sur la présidence Trump pourraient être catastrophiques, dignes du Watergate.

Entretien réalisé par Thomas Delage le 17 mars 2017

Notes
(1) Max Boot, « America's Spies Need to Watch Their Backs », *Foreignpolicy.com*, 5 janvier 2017.
(2) Sur ces problèmes, voir Amy Zegart, *Spying Blind: the CIA, the FBI, and the Origins of 9/11*, Princeton University Press, 2007.
(3) Loch Johnson, « Accountability and America's Secret Foreign Policy », *Foreign Policy Analysis,* mars 2005.
(4) Commission nationale sur les attaques terroristes contre les États-Unis, 11 septembre 2001, Rapport final, Paris, éditions Alban, 2005.
(5) James Bamford, « The Multibillion-Dollar U.S. Spy Agency You Haven't Heard of », *Foreignpolicy.com*, 20 mars 2017.
(6) Philip Rucker et Ashley Parker, « Trump admits to Russian hacking even as he attacks U.S. intelligence community », *The Washington Post*, 11 janvier 2017.

Photo ci-dessous : Le 20 mars 2017, le directeur du FBI, James Comey (à gauche) et le directeur de la NSA, Michael S. Rogers (à droite), s'apprêtent à répondre aux questions de la Commission sur le renseignement du Congrès. Ils ont reconnu qu'une enquête était en cours sur les tentatives russes d'influencer l'élection américaine de 2016 et sur d'éventuelles collusions entre « l'équipe de campagne Trump et le gouvernement russe ». Les deux hommes ont également affirmé que Barack Obama n'avait pas fait espionner la tour Trump, et que les services de renseignement américains n'ont pas demandé aux Britanniques de procéder à des écoutes. Quelques heures auparavant, le président Donald Trump affirmait qu'il n'y avait « aucune collusion » entre Moscou et son entourage – contrairement aux informations contenues dans le rapport de la CIA qui a fuité en janvier dernier – et conseillait au Congrès d'enquêter plutôt sur les fuites émanant du Renseignement à destination des médias. (© AFP/Nicholas Kamm)

analyse

Par **Claude Delesse**, directrice de recherche associée au Centre français de recherche sur le renseignement (CF2R). Elle est l'auteur de *NSA : National Security Agency* (Tallandier, mars 2016).

La NSA américaine : l'empire du renseignement

Créée en 1952, la National Security Agency (NSA) est aujourd'hui la plus grande agence de renseignement électronique au monde et son arsenal d'écoute et de surveillance est actif sur l'ensemble de la planète au service de Washington et de ses intérêts.

Fin 2016, les services de renseignement américains ont accusé les Russes d'avoir piraté les systèmes de communication du Parti démocrate durant la course à la Maison-Blanche. Diffusés sur Internet, les courriels et documents internes interceptés auraient eu une influence sur les élections présidentielles. Le vice-amiral Michael S. Rogers, patron de la National Security Agency (NSA, Agence nationale de sécurité) soutenait lors d'une conférence organisée le 15 novembre 2016 par le *Wall Street Journal* qu'un pays déterminé aux objectifs précis avait recouru à Wikileaks lors de la campagne électorale afin de fragiliser la candidature d'Hillary Clinton. Le gouvernement américain a également accusé Moscou de mener des cyberattaques contre des universités, des établissements financiers et d'autres institutions américaines. La démocratie serait en danger, mais les preuves manquent pour trancher définitivement entre supputations, allégations, mensonges d'ordre politique ou faits avérés. Les contre-espions de la plus grande agence de renseignement d'origine électromagnétique au monde auraient-ils tracé ces attaques avec fiabilité ? Ils surveillent en effet les opérations cyberintrusives du Kremlin depuis longtemps. Les historiens découvriront peut-être un jour les réels pouvoirs et l'efficience stratégique de cette titanesque organisation qui dispose d'un budget annuel avoisinant les dix milliards de dollars (1), emploie des dizaines de milliers de personnes patriotes, s'efforce de protéger ses secrets malgré la fréquence accentuée des révélations. Des sources ouvertes permettent toutefois d'en dresser un portrait.

L'ascension vers la démesure

La NSA a été créée secrètement en 1952 après l'abolition de l'Agence de sécurité des forces armées (AFSA). Cette dernière était censée apporter une cohésion entre les services cryptologiques militaires mais son directeur, Ralph J. Canine, bien que

Photo ci-dessus : Quartier général de la National Security Agency à Fort George G. Meade, dans le Maryland, sur une base militaire de l'US Army située à près de 16 kilomètres de Washington. (© nsa.gov)

coriace et compétent, n'avait pas réussi à résoudre les conflits internes et à gérer les mésententes avec le département d'État, le FBI et la CIA. Surnommée la « *No Such Agency* » ou « *Never Say Anything* », la NSA opéra clandestinement durant des années, aidant les États-Unis à traverser des crises (Canal de Suez, Cuba...) et des conflits tels ceux de Corée, du Vietnam, d'Irak ou d'Afghanistan. Au cours des années 1970, les Américains scandalisés apprirent l'existence des programmes de surveillance domestique Shamrock et Minaret (2). Cela déclencha la création de commissions de renseignement au sein de la Chambre des représentants et du Sénat, mais les dirigeants de la NSA,

> *« Surnommée la « No Such Agency » ou « Never Say Anything », la NSA opéra clandestinement durant des années, aidant les États-Unis à traverser des crises (Canal de Suez, Cuba...) et des conflits tels ceux de Corée, du Vietnam, d'Irak ou d'Afghanistan. »*

habiles menteurs, apprirent à composer avec les inquisitions du Congrès. La lutte contre le communisme poussa l'agence à rechercher le leadership dans les technologies de conquête de l'espace et dans les domaines informatiques. Projetée dans une période de restrictions et de crise existentielle après l'effondrement de l'ours soviétique dès 1989 et peu préparée à détecter de nouvelles menaces protéiformes, elle faillit à prévoir les attentats du 11 septembre 2001, qui furent néanmoins une « aubaine » pour elle. L'administration Bush lui octroya des moyens considérables, laissant à Michael Hayden puis à son successeur Keith Alexander les mains libres pour déployer une surveillance globale indiscriminée. Peu à peu, sous la présidence Obama, elle continua sa métamorphose et devint, selon James Bamford, l'appareil de surveillance le plus intrusif et le plus onéreux au monde (3).

Outre le site de Fort George G. Meade (Maryland), cité hautement sécurisée qui abrite le quartier général et des dizaines de bâtiments aux activités mystérieuses, la NSA possède des centres régionaux dans les États du Colorado (NSAC), de Géorgie (NSAG), du Texas (NSAT) et à Hawaï (NSAH). Son récent *data center* dans l'Utah, bâtiment de 9 hectares, engloutit et stocke données et métadonnées avec démesure. La NSA orchestre un système d'espionnage des communications (Comint) avec ses quatre partenaires de l'alliance UKUSA (1946) : le Government Communications Headquarters (GCHQ) britannique, qui jouit d'un statut privilégié, le Communications Security Establishment canadien (CSE), l'Australian Signals Directorate (ASD) et le Government Communications Security Bureau (GCSB) néo-zélandais. La coopération entre les « *Five Eyes* » évolue avec les avancées des technologies de surveillance.

Réparties sur les territoires de pays coopérants, des dizaines de stations d'écoute interceptent les communications relayées par des satellites de communication commerciale. La NSA dispose de ses propres satellites espions placés en orbite basse ou géostationnaire ; le dernier a été lancé en 2016. Elle exploite également des moyens mobiles d'interception (aéronefs, navires spécialement équipés). Les agents clandestins du Special Collection Service (SCS), unité spéciale conjointe avec la CIA, sont présents dans les ambassades ou consulats américains.

La NSA pirate les câbles terrestres ou posés dans les fonds sous-marins grâce à des sondes souvent installées avec la complicité d'opérateurs. Des sociétés de télécommunications facilitent le détournement des trafics de données via des stations d'atterrissement.

Au cœur de Manhattan, un immeuble sans fenêtres appartenant à AT&T (nom de code : Lithium) abriterait des activités secrètes de la NSA (4). Celle-ci renforce ses capacités en entretenant des collusions avec des géants du complexe militaro-industriel américain et des start-up high-tech spécialisées dans les technologies électroniques, l'intelligence artificielle, les sciences cognitives, la sécurité et la cryptologie. Ainsi n'hésite-t-elle pas à collaborer avec des firmes israéliennes. Au cœur de conjonctions d'intérêts, elle tisse des réseaux relationnels dont la porosité public/privé profite aux managers et à une jeune aristocratie qui maîtrise mathématiques, langages informatiques et technologies de pointe. Confrontés à une course technologique de portée stratégique, les hommes clés de la NSA sont obsédés par la physique quantique et obnubilés par le souci de dominer la globalité de la sphère informationnelle. L'investiture de Donald Trump augure le renforcement de l'« *America First* » et une ligne dure de sécurité nationale. Peu avant son départ, le directeur du renseignement national, James Clapper, démissionnaire, s'avouait préoccupé par les dérives de la génomique, des armes spatiales et antisatellites, de l'impression 3D, de l'intelligence artificielle et des armes biologiques. Plongés dans cette ambiance, les analystes de la NSA devront composer avec l'instabilité du monde, l'hybridation des menaces, l'accélération et l'explosion des communications, des réseaux sociaux, des

Photo ci-dessus :
L'Amiral Michael S. Rogers, directeur de la NSA depuis avril 2014. Nommé par Barack Obama, il occupe également le poste de commandant de l'USCYBERCOM, en charge de la sécurité de l'information pour l'armée. (© nsa.gov)

Photo ci-contre :
Situé au cœur de Manhattan, cet imposant immeuble de béton dépourvu de fenêtre, baptisé « *Long Lines Building* », passait pour être une antenne de AT&T, l'un des principaux opérateurs téléphoniques et fournisseurs d'accès américains. Selon une enquête de *The Intercept*, qui s'appuie sur des informations fournies par Edward Snowden, ce bâtiment serait une antenne majeure et un centre d'écoute de la NSA dont le but serait de filtrer les communications vers l'international et participer à des opérations de surveillance contre d'autres pays ou des organisations internationales. (© Mark Visosky)

Photo ci-dessus :
En 2015, des documents dévoilés par Wikileaks ont révélé que la chancelière allemande, Angela Merkel, et le président français, François Hollande, avaient été mis sur écoute par la NSA, à l'instar des présidents français Jacques Chirac et Nicolas Sarkozy à leur époque.
(© Shutterstock/360b)

outils connectés et de l'intelligence artificielle, mais aussi avec l'imprévisibilité d'un président versatile.

Un empire du renseignement

Décrite à l'origine comme responsable du renseignement des communications (COMINT) dans une directive du Conseil de sécurité nationale (5), les missions de la NSA consistent à intercepter et collecter le renseignement des signaux (SigInt) – y compris par des moyens clandestins – et déchiffrer les transmissions étrangères d'origine électromagnétique afin de soutenir les missions des autorités gouvernementales américaines, voire celles de leurs partenaires. Cryptologue hors norme, elle est également chargée, dans le cadre de l'*Information Assurance*, de protéger les données SigInt classifiées et sensibles ou émanant des activités militaires ainsi que les systèmes vitaux de sécurité nationale. Début 2016, Michael Rogers décida de renforcer l'efficacité, la coordination et l'agilité en fusionnant au sein d'une direction des opérations les services opérationnels de la direction du Renseignement des signaux (SID) et ceux de la direction Information Assurance (IAD), qui conçoivent des technologies sécurisées et protègent contre les tentatives d'intrusion et d'espionnage numériques. Avec cette initiative « NSA21 », Rogers a pris le risque de mélanger deux cultures qui devront apprendre à se faire confiance et à collaborer (6).

Les relations avec les opérateurs téléphoniques et les firmes co-partenaires de la cybersécurité risquent de se compliquer, car la diffusion de technologies ou de logiciels piégés ira à l'encontre de leurs intérêts commerciaux. Apple refusa de débloquer le téléphone de Syed Rizwan Farook, terroriste impliqué dans le massacre de San Bernardino en 2015. Inversement, une cryptologie forte entraverait les opérations SigInt. Les cryptologues et hackers de la NSA rivalisent avec des cyberespions ou des cybermercenaires qui opèrent pour le compte des États. Ils traquent des criminels, terroristes ou des hacktivistes qui n'hésitent pas à partager leurs expertises avec des internautes soucieux de leur vie privée ou en lutte contre des régimes répressifs. Autant dire qu'ils craignent plus que tout l'incapacité à décrypter, et leurs managers l'incapacité à déceler les menaces. La NSA utilise donc les ordinateurs les plus puissants du monde, impose des standards de chiffrement en opérant en coulisses via différentes entités dans le domaine normatif, piège les machines, les systèmes et les réseaux, recrute les hackers les plus ingénieux qui peaufinent leurs attaques au sein du Tailored Access Operations (TAO).

> *« Sous la présidence Obama, la NSA continua sa métamorphose et devint, selon James Bamford, l'appareil de surveillance le plus intrusif et le plus onéreux au monde. »*

Michael Rogers est également chef du Central Security Service (CSS), le système interarmées de cryptologie, et en tant que commandant de l'US Cyber Command, créé en 2010, il exerce une autorité sur tout le spectre des opérations militaires du cyberespace, défensives et offensives. Il est donc à la tête d'un empire aux missions clairement énoncées sur le site de la NSA : comprendre les menaces en étant à la pointe de la détection, apporter le renseignement utile à temps aux officiels et hauts gradés, soutenir les opérations militaires et protéger les soldats, sécuriser les réseaux et les données, développer la cybersécurité, protéger et déployer les armes stratégiques digitales, dominer la recherche et les avancées technologiques.

La scission NSA/USCYBERCOM envisagée sous la présidence Obama se concrétisera-t-elle ? Donald Trump pourrait confier la direction de la NSA à un civil, alors que cette fonction a toujours été occupée par un militaire secondé par un adjoint civil depuis 1956. Gagnant en autonomie, le Cyber Command se verrait doté d'une direction *ad hoc* restant sous commandement militaire. Barack Obama a déjà préparé le terrain en promulguant une loi qui autorise la scission entre les deux structures à condition que le secrétaire à la Défense et le comité des chefs d'état-major interarmées attestent que l'efficacité du Cyber Command, jusque-là bénéficiaire du savoir-faire de la NSA, n'en pâtirait pas.

La NSA dépend du département de la Défense. Elle reçoit des instructions gouvernementales : il lui faut renforcer les collaborations avec les autorités judiciaires, les forces de police et les agences chargées de veiller afin de contrecarrer

Photo ci-contre :
Manifestation à Washington, le 26 octobre 2013, contre les programmes d'espionnage de la NSA. Si les révélations d'Edward Snowden ont déclenché une vague d'indignation auprès des populations et des gouvernements étrangers, le mécontentement fut aussi perceptible à l'intérieur des frontières. La pétition du mouvement « *Stop Watching Us* » a ainsi recueilli, en octobre 2013, plus de 580 000 signatures pour demander au Congrès de faire toute la lumière sur la stratégie de la NSA, et notamment sur le programme de surveillance PRISM. (© Shutterstock/Rena Schild)

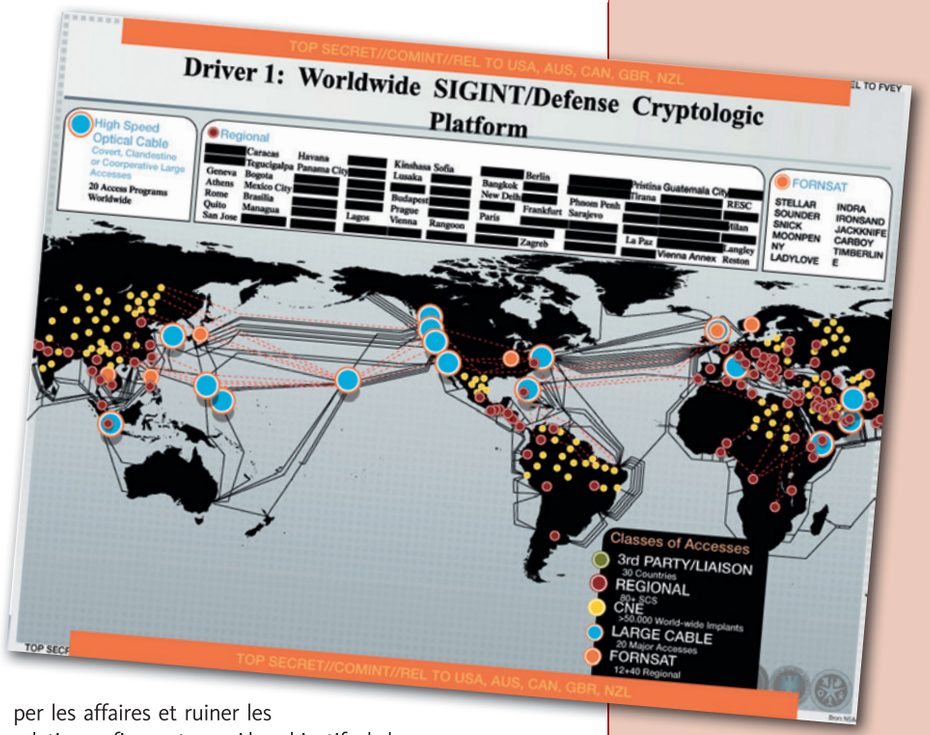
les activités terroristes, souvent liées à la criminalité transnationale. Selon le Conseil de sécurité nationale (NSC), les efforts doivent porter sur tous les types de renseignement : SigInt, HumInt (renseignement humain) et OSInt (sources ouvertes). Les principaux clients des analyses SigInt de la NSA sont en priorité la CIA, les autres agences de renseignement, le NSC, la Maison-Blanche, le Pentagone, les départements de la Sécurité intérieure, d'État, du Commerce, de l'Énergie, du Trésor, le bureau des chefs d'état-major interarmées (JCS), les commandements militaires.

Les orientations stratégiques de renseignement sont définies par le président des États-Unis en concertation avec la Maison-Blanche et les agences de renseignement, puis déclinées en besoins par le Director of National Intelligence (DNI) et mises en application dans le cadre du *National Intelligence Priorities Framework* (NPIF). Les priorités relatives au renseignement des signaux sont établies en conformité au *National SigInt Requirement Process* (NSRP). Rigueur procédurale oblige, les clients exposent leurs demandes dans un « *Information Needs* » (IN) qui est décliné en « éléments essentiels d'information » (EEI). La collecte et l'analyse sont facilitées par des outils de pointe (reconnaissance vocale, profilage, biométrie...). Seule une infime partie des centaines de programmes a été révélée grâce aux documents subtilisés par Edward Snowden. À la fin des années 1990, les Européens sidérés avaient découvert Echelon, devenu le symbole d'une surveillance tentaculaire planétaire. Outre une surveillance à large spectre, la NSA procède à l'exploitation de réseaux informatiques (CNE) par piratage et déploie

> *« Espionne universelle rompue à l'art d'opacifier et de tromper, la NSA légitime ses activités au nom des luttes contre les phénomènes terroristes, la criminalité organisée, les trafics en tous genres, la prolifération nucléaire et le risque NRBC. »*

des attaques réseaux (CNA) visant à corrompre, détruire des données ou à mener des dénis de service.

Les cyberhackers de la NSA et du Joint Threat Research Intelligence Group, unité clandestine du GCHQ, surveillent et analysent les réseaux sociaux (guerre pour l'information), ou propagent des virus destructeurs tel Ambassadors Reception, qui crypte tout ordinateur cible, efface les mails, bloque l'écran et l'accès à Internet (guerre contre). Ils s'incrustent dans les discussions en ligne, mentent, contre-argumentent, leurrent, manipulent ou compromettent leurs cibles. Maîtres dans l'art de la « déception » (7), ils créent de faux personnages accusateurs sur de faux blogs et diffusent de fausses informations sur les forums afin de porter atteinte à la réputation. Les opérations clandestines en ligne (OCA) utilisent un large spectre dont les moyens 4D's (*Deny, Disrupt, Degrade, Deceive* : empêcher, perturber, dégrader, tromper). « Discréditer une entreprise, stopper les affaires et ruiner les relations » figurent parmi les objectifs de la guerre par l'information.



Ci-dessus :
Document de la NSA datant de 2012, révélé par Edward Snowden et publié par le journal néerlandais *NRC Handelsblad*. La carte représente la localisation des installations du réseau Échelon, qui constitue un système mondial d'interception des communications privées et publiques élaboré par les pays signataires du traité UKUSA le 5 mars 1946 (États-Unis, Royaume-Uni, Canada, Australie, Nouvelle-Zélande) et qui est resté inconnu du grand public pendant plus de 40 ans. (© NSA)

Les guerres secrètes

Le renseignement SigInt a progressé avec l'évolution des transmissions et les transformations de la guerre. La NSA aide les militaires à traquer l'ennemi, à connaître ses intentions, stratégiques ou tactiques et ses capacités opérationnelles, tout en l'empêchant de faire de même. Les moyens mobiles d'interception jouent un rôle majeur sur le terrain. Elle sécurise les opérations (OPSEC), chiffre les communications, décrypte, déjoue les tactiques de renseignement ou de contre-renseignement ennemi. Le cyberespace est un domaine d'opérations propice à la guerre du sens (propagande, désinformation, « déception », etc.). Les analystes de la NSA participeraient également à des opérations « sales ». Ils appuieraient les assassinats ciblés menés par des tirs de drones. Ils participeraient aux interrogatoires de terroristes dans les prisons de Guantanamo et d'Abu Ghraib. Leur rôle : aider à préparer les questions, ou à interpréter les éventuelles réponses des hommes torturés (8).

Alors que guerres asymétriques, terrorisme intérieur et cyberconflits s'intensifient, les États continuent de rivaliser sur un échiquier diplomatique de plus en plus instable où prédominent la quête et le culte du secret. Zbigniew Brzezinski a ainsi avoué dans une interview accordée au *Nouvel Observateur* en 1998, à la suite des révélations sur le réseau Echelon, que l'Amérique espionnait le monde entier, ses amis comme ses ennemis. L'ancien conseiller de Jimmy Carter expliquait que le renseignement électromagnétique et l'imagerie spatiale sont des moyens techniques relativement « peu risqués » de recueil systématique... moins compromettants que le recrutement d'agents dont les agissements peuvent se révéler très périlleux ou « conduire à des scandales très dommageables » pour les relations avec les pays étrangers, amis en particulier (9). Organisations et rencontres internationales, institutions euro-

Pour aller plus loin

Claude Delesse, *NSA : National Security Agency*, Paris, Tallandier, 2016.

péennes, délégations diplomatiques de pays alliés, personnalités politiques, hauts fonctionnaires, candidats aux élections présidentielles telle celle de 2012 en France, hauts dirigeants, entourages (jusqu'au deuxième niveau selon les textes qui régissent les écoutes) sont dans la ligne de mire de la NSA. Des chefs d'État (Dilma Rousseff, Peña Nieto, François Hollande) et la chancelière Angela Merkel, en découvrant que leur téléphone personnel était écouté, ont dénoncé une violation des lois internationales, une atteinte inacceptable à la souveraineté nationale et aux relations entre amis. Le président Obama promit un réexamen des activités de l'agence en vue d'équilibrer sécurité, transparence et droits privés. Or les aménagements apportés au *Patriot Act* par l'*US Freedom Act* en 2015 ne concernent pas les citoyens étrangers. Les enjeux de sécurité ont cependant vite estompé les atermoiements. La France, engagée à l'étranger sur de nombreuses zones de conflits et menacée sur son propre territoire, collabore étroitement avec les services de renseignement américains et britanniques. Le GCHQ a espionné entre 2008 et 2011 présidents, ministres, partisans, chefs d'opposition et élites militaires dans au moins une vingtaine de pays africains.

Photo ci-dessus :
Au début de l'année 2017, Donald Trump annonçait souhaiter la prolongation de deux des plus importants programmes de surveillance de la NSA arrivant à échéance à la fin de l'année. L'un d'eux concerne l'analyse du trafic qui passe par les câbles internet transitant aux États-Unis ; l'autre est le programme PRISM, qui permet la collecte d'informations auprès d'entreprises américaines, dont la plupart des géants d'Internet (Microsoft, Google, Yahoo, Facebook, YouTube, Skype, Apple…). (© Xinhua/ Yin Bogu)

Mais les communications d'ambassadeurs, de personnes jouant un rôle clé au sein des institutions internationales ou des rencontres économiques et commerciales, celles de dirigeants, de financiers, de grands groupes internationaux (Total, Thalès) et d'opérateurs de télécommunications présents sur le continent étaient aussi interceptées (10). La NSA sert une machine de guerre et de diplomatie économiques qui met renseignements et moyens à disposition des intérêts privés américains. Les firmes US remporteraient ainsi de nombreux appels d'offres internationaux au détriment des étrangères. Prétextant veiller sur les embargos et dépister corruption et pratiques commerciales déloyales, la NSA espionne les négociations et discussions internationales ou d'hommes d'affaires, y compris lors des vols internationaux. Elle pille les informations commerciales ou technologiques, scrute les appels d'offres. Le cyberespace facilitant l'espionnage industriel, Chinois et Américains s'accusent mutuellement. En 2014, l'administration Obama déclara ne pas pouvoir tolérer des actions étatiques qui cherchent à saboter des entreprises américaines dans des secteurs sensibles (métallurgie, nucléaire, énergie solaire, etc.) et à miner l'intégrité d'une compétition équitable. Or, la NSA s'exclue de toute déontologie entre alliés et pointe son attention sur les pratiques commerciales et financières françaises, les relations économiques de Paris avec les pays étrangers et avec les institutions financières internationales, les positions de l'Hexagone sur les agendas du G8 et du G20, les grands contrats à l'export d'au moins 200 millions de dollars, les secteurs stratégiques (télécommunications, énergie, transports, santé, biotechnologies). Les entreprises du CAC 40, les opérateurs d'importance vitale (OIV), les avionneurs tels Airbus sont la cible d'attaques régulières (11). La curiosité des États s'étend néanmoins au-delà ! L'hégémonie digitale de la NSA se construit d'autant plus que l'idéologie techniciste se développe et que l'insouciance communicationnelle des individus s'accroît. Le nouvel exécutif américain en fera-t-il un usage encore plus coercitif, y compris sur son propre territoire ?

> « *La NSA sert une machine de guerre et de diplomatie économiques qui met renseignements et moyens à disposition des intérêts privés américains.* »

Claude Delesse

Notes

(1) La Communauté du renseignement américaine (USIC) compte dix-sept agences. La DNI (Director of National Intelligence) en a la direction. Le budget prévisionnel pour 2017 avoisine les 53 milliards de dollars, auxquels s'ajoutent 17 milliards pour le renseignement militaire.

(2) Le programme Shamrock fut mis secrètement en place durant la Seconde Guerre mondiale. Un temps interrompu, il put reprendre et permit à l'AFSA, puis à la NSA d'accéder sans mandat aux télégrammes entrant et sortant des États-Unis, grâce à la complicité des sociétés Western Union, RCA et ITT. Lancé dans les années 1960, le programme Minaret espionnait les communications internationales de citoyens américains épinglés sur une liste de personnes à surveiller (pacifistes, dissidents, militants, objecteurs de conscience). Parmi eux : Joan Baez, Jane Fonda, Malcolm X, Martin Luther King, etc.

(3) J. Bamford, « Every Move You Make », *Foreign Policy*, 7 septembre 2016.

(4) R. Gallagher, H. Moltke, « Titanpointe: The NSA's Spy hub in New York, Hidden in Plain Sight », *TheIntercept*, 10 novembre 2016.

(5) Memorandum, President Truman to Secretaries of State and Defense, *Communications Intelligence Activities*, 24 octobre 1952 et National Security Council Intelligence directive (NSCID) n° 9, Communications Intelligence, 29 décembre 1952.

(6) H. Nakashima, « National Security Agency plans major reorganization », *The Washington Post*, 2 février 2016. Une direction des capacités et de la recherche fut par ailleurs confirmée.

(7) En terminologie militaire : technique de tromperie, trucage, falsification, mise en scène, etc., destinée à amener l'adversaire à agir de façon préjudiciable à ses propres intérêts.

(8) C. Currier, « NSA closely involved in Guantánamo interrogations, documents show », *SidToday*, october 2003 ; « "A Unique Opportunity Awaits you" in Iraq », *SidToday*, décembre 2003 et juin 2003, TheIntercept.com, 16 mai 2016.

(9) V. Jauvert, « NSA : les confidences d'un ancien de la Maison-Blanche », *Le Nouvel Observateur*, 1er juillet 2013 (première publication : 16 décembre 1998).

(10) Simon Piel et Joan Tilouine, « La France et ses intérêts en Afrique sous surveillance », *Le Monde*, 9 décembre 2016.

(11) Espionnage Élysée, NSA Economic Spy Order, *Wikileaks.org*, 23 juin 2015.

analyse

Le Mossad israélien, meilleur service au monde ?

Par **David Elkaïm**, chercheur au CF2R. Il a travaillé au ministère des Affaires étrangères et du développement international (2012-2016) et enseigné à Sciences Po Paris (2010-2016). Il est le co-auteur de *Les services secrets israéliens* (Tallandier, 2014).

Dépourvu de profondeur stratégique et faible démographiquement (8 millions d'habitants environ), l'État d'Israël a fait de ses services de renseignement un pilier de son système de défense. Les « exploits » du Mossad ont été popularisés par un grand nombre de livres et de films. Il est également le plus redouté par les ennemis d'Israël : les plus dangereux se savent sous la menace du *Kidon*, son bras armé.

Connaitre les moyens dont disposent les ennemis d'Israël, prévenir leurs attaques, anticiper les bouleversements politiques dans les pays voisins mais aussi dialoguer discrètement avec des États avec lesquels il n'entretient pas de relations diplomatiques sont des questions de vie ou de mort. De plus, du fait de la mondialisation, ces services ont progressivement été conduits à protéger des ressortissants et des intérêts israéliens hors du territoire national (ambassades, touristes, entreprises, etc.). Pour ce faire, la communauté israélienne du renseignement s'organise autour de trois services principaux :

• *Aman*, la direction du renseignement militaire, dépend directement du chef d'état-major général et du ministre de la Défense.

• Le *Shin Beth* (acronyme de « Service général de sécurité », en hébreu), communément appelé *Shabak*, qui dépend du ministère de l'Intérieur, est chargé de la sécurité du territoire et du contre-espionnage. Il opère également dans les Territoires palestiniens sous contrôle israélien.

• Le *Mossad* (« institut » en hébreu), qui dépend directement du Premier ministre, constitue le service de renseignement et d'action à l'étranger. Le directeur du Mossad est simultanément coordinateur général de la communauté israélienne du renseignement.

Structure et organisation du Mossad

Le Mossad compte près de 3000 personnes, dont plusieurs centaines en poste à l'étranger. C'est une organisation civile.

Photo ci-dessus :
Le 3 juillet 2016, le directeur du Mossad, Yossi Cohen, participe aux funérailles d'un Israélien tué par un Palestinien au sud d'Hébron. Nommé en janvier 2016, ce proche de Benyamin Netanyahou a remplacé son prédécesseur, Tamir Pardo, en raison des divergences qui opposaient celui-ci au Premier ministre sur la question iranienne. (© AFP/Menahem Kahana)

Ses employés n'ont pas de grades militaires, bien que la plupart d'entre eux aient servi dans les Forces de défense israéliennes, notamment dans le renseignement militaire.

Pour mener à bien leurs missions, les officiers traitants (appelés *katsas*) ont besoin de soutien sur le terrain. C'est pourquoi le Mossad a développé un réseau de milliers de *sayanim* (pluriel de *sayan*, « qui veut apporter son aide »), recrutés parmi les communautés juives du monde entier. Il peut, par exemple, s'agir d'un loueur de voiture qui pourra fournir un véhicule sans formalités administratives ou d'un médecin qui soignera un agent en dehors des structures médicales officielles. Ces volontaires, qui ne sont pas rémunérés, transmettent également des renseignements dits « ouverts » : discussions entendues dans un cadre privé, articles de presse, etc (1).

Le Mossad compte sept divisions opérationnelles aux missions distinctes (2) :

• La plus importante, *Tsomet*, est responsable de la recherche clandestine du renseignement, via les postes officiels ou clandestins à l'étranger. C'est elle qui recrute et manipule ses sources à travers le monde, grâce aux *katsas*. Le Mossad n'emploierait qu'une centaine d'officiers traitants chargés de recruter des agents à travers le monde. Les plus expérimentés travailleraient sous couverture à l'étranger. Les autres n'effectueraient que des déplacements ponctuels dans des pays proches (Turquie, Chypre, etc.).

• Le *Neviot* est la division chargée de la recherche opérationnelle. Elle ne recrute pas d'agents mais se charge des filatures, des contre-filatures, de la surveillance et des écoutes clandestines.

• La division Renseignement est responsable de l'interprétation des informations collectées par les différentes branches du Mossad. C'est d'elle que dépend également le département de la guerre psychologique, chargé des opérations de propagande et d'intoxication des adversaires d'Israël.

• La division du Soutien technique crée les « légendes » des officiers envoyés en opération, leur fournit des faux papiers et met en place leur couverture (création d'une société d'export, par exemple).

• La division appelée *Tsafririm* a une double fonction : recruter les *sayanim* dans les pays où le Mossad conduit des opérations et aider les communautés juives partout dans le monde à faire face à des menaces éventuelles. Elle a ainsi joué un rôle actif dans l'exfiltration des Juifs d'Afrique du Nord et du Moyen-Orient (années 1950 et 1960) et d'Éthiopie (années 1980 et 1990).

• La division *Tevel* (« monde » en hébreu) est chargée de l'action politique et des liaisons internationales. Elle gère les contacts et les opérations communes avec les services amis, mais aussi les échanges avec les pays qui ne disposent pas de relations officielles avec Israël. *Tevel* fournit également instruction, financements et assistance logistique aux mouvements en lutte contre des régimes hostiles à Israël (Syrie, Iran, Irak etc.). Par ses échanges avec les services étrangers, cette division apporterait près de 70 % du renseignement dont dispose le Mossad. Enfin, elle a pour mission de faciliter l'« atterrissage en douceur » des agents qui rencontrent des problèmes dans un pays allié en les exfiltrant de la manière la plus discrète possible.

> *« Bien qu'il bénéficie toujours d'un soutien très large dans la société comme dans la classe politique israéliennes, le Mossad s'est retrouvé à plusieurs reprises au cœur de vives controverses au cours des dernières années. »*

• La dernière division est appelée *Metsada*. Chargée des opérations spéciales, elle dirige les opérations paramilitaires de sabotage, d'enlèvement et d'élimination physique des personnes considérées comme menaçant la sécurité du pays. C'est d'elle que dépend aujourd'hui le *Kidon* (« baïonnette » en hébreu), le département chargé des assassinats, appelés « traitements négatifs ».

Photo ci-dessus :
Le 15 mai 2007, l'ingénieur Mohammed Sayyed Saber est présenté devant la justice égyptienne, qui le soupçonne de s'être rendu à au moins trois reprises à Hong Kong afin d'y rencontrer deux agents du Mossad pour leur remettre des documents confidentiels sur le programme nucléaire égyptien. En 2002, c'est un autre ingénieur nucléaire égyptien qui avait été condamné à 15 ans de travaux forcés après avoir été reconnu coupable d'espionnage au profit d'Israël. (© AFP/ Chris Bouroncle)

Le « meilleur service de renseignement du monde »....

Depuis sa création en 1951, le Mossad a connu de nombreux succès, en matière de renseignement comme en matière de sabotage. La capture d'Eichmann (1961), l'implantation d'Eli Cohen au sommet de la hiérarchie militaire syrienne (3) (de 1961 à 1965), le raid sur Entebbe (1976) (4) ou l'exécution de membres de groupes terroristes (Yahia Ayache, un des chefs militaires du Hamas, en 1996 ; Imad Mughniyeh, en 2008) sont les opérations les plus spectaculaires.

Il a également subi un certain nombre d'échecs. Les plus connus sont certainement l'assassinat en 1973 à Lillehammer (Norvège) d'Ahmed Bouchiki, un jeune Marocain identifié à tort comme le leader de Septembre noir, l'organisation palestinienne à l'origine de l'attaque contre la délégation israélienne aux Jeux olympiques de Munich en 1972 ; la tentative ratée d'empoisonnement du chef du bureau politique du Hamas, Khaled Mechaal, en 1997, qui a conduit les autorités jordaniennes à menacer de rompre les relations diplomatiques si Israël refusait de fournir

l'antidote ; l'arrestation en 1998 d'une équipe du *Neviot* par la police suisse alors qu'elle posait des micros dans l'appartement d'un militant palestinien à Berne, qui conduira le directeur du Mossad, Danny Yatom, à démissionner.

Quoiqu'il en soit, la plus grande prouesse du Mossad est peut-être de réussir à réconcilier les admirateurs d'Israël avec ses ennemis – en particulier les plus complotistes ! – sur un point : ils voient derrière chaque mort ou accident suspect l'ombre du « meilleur service de renseignement du monde », réputation qui, qu'elle soit méritée ou non, constitue un atout considérable par la paranoïa qu'elle suscite parmi les ennemis du pays.

Au cours des dernières années, plusieurs opérations lui ont ainsi été attribuées : quand, en 2014, l'explosion d'un coffre-fort a provoqué la mort de Jamal al-Jamal, l'ambassadeur de l'Autorité palestinienne en République tchèque ou quand, en 2010, Mahmoud al-Mabhouh, un des chefs militaires du Hamas, a été assassiné à Dubaï, tous les regards se portés sur le Mossad, à tort ou à raison (5). Idem pour la mort dans les locaux de l'ambassade de l'Autorité palestinienne à Sofia (Bulgarie) dans des conditions non élucidées d'Omar Zayed, qui, membre du Front populaire de libération de la Palestine, avait participé en 1986 à Jérusalem à l'assassinat d'Eliyahu Amadi, un étudiant de 22 ans. Précision qui a son importance : après s'être échappé de prison en Israël, Zayed avait refait sa vie en Bulgarie à la même époque où Yossi Cohen, l'actuel directeur du Mossad, était chef de station en Europe. Avait-il un compte à régler avec celui qui avait vécu des années sous ses yeux sans être inquiété après avoir échappé à la justice israélienne ?

Et, de façon peu surprenante, les Brigades Ezzedine al-Qassam, la branche militaire du Hamas, après avoir confirmé que l'homme assassiné à Sfax (Tunisie) le 15 décembre 2016, Mohamed Zouari, avait rejoint le mouvement il y a dix ans, ont immédiatement accusé le Mossad. Ce n'est pas impossible vu le profil de cet ingénieur qui travaillait sur un programme de drones d'attaque, technologie dont Israël cherche à empêcher le Hamas de se doter. L'affaire a déclenché une crise en Tunisie : le mouvement Ennahda, partie prenante de la coalition gouvernementale, a parlé de « menace à la stabilité du pays ». Le directeur de la Sureté nationale au ministère de l'Intérieur, Abderahman Belhaj Ali, considéré comme l'artisan de l'amélioration de la situation sécuritaire en Tunisie depuis un an, a présenté sa démission, officiellement pour des « raisons personnelles » (6). De fait, il semblerait que Zouari ait fait l'objet d'une surveillance accrue : une femme hongroise, qui a pris contact avec lui il y a quelques mois pour réaliser une interview, serait revenue en Tunisie et aurait quitté le pays quelques heures avant sa mort, après avoir abandonné deux voitures de location en pleine ville. Deux Tunisiens ont également été arrêtés en Suède pour des faits similaires qui, d'apparence bénins, ressemblent manifestement à des préparatifs d'une opération. Pourtant, plusieurs spécialistes du Mossad ont émis des doutes (7). Ainsi, Yossi Melman, journaliste au quotidien *Maariv*, souligne que « les tireurs n'ont pas agi avec le professionnalisme qui caractérise le Mossad ». En effet, Zouari a été atteint de 20 balles alors qu'il était au volant de sa voiture ; or, il faut remonter à l'élimination de Fathi al-Shiqaqi, responsable du Djihad islamique, à Malte en 1995, pour trouver trace d'un tel mode d'exécution : depuis lors, le Mossad semble privilégier l'utilisation d'engins explosifs ou l'injection de poison. Mais d'autres, tel Alex Fishman dans le quotidien *Yedioth Ahronoth*, n'excluent pas que les espions israéliens aient précisément voulu cette fois-ci laisser des traces pour adresser un message clair au Hamas.

… pris dans les tourments de la vie politique israélienne

Bien qu'il bénéficie toujours d'un soutien très large dans la société comme dans la classe politique israéliennes, le Mossad s'est retrouvé à plusieurs reprises au cœur de vives controverses au cours des dernières années.

En effet, signe de vitalité démocratique, certaines de ses méthodes ont été fortement critiquées. C'est tout d'abord la pratique des assassinats ciblés (également appelés extrajudiciaires) qui est remise en cause. Théoriquement très strictement encadrées et officiellement approuvées par écrit par le Premier ministre, ces opérations sont exécutés sur la base des informations fournies par le Mossad quand elles se déroulent à l'étranger. Au-delà des questions non négligeables qu'elles posent en matière de droit de la guerre et de droits de l'homme (8), pour les cibles comme pour les victimes dites « collatérales », c'est leur efficacité qui est remise en cause : plusieurs études montrent que, si elles peuvent avoir un effet à court terme en décapitant un groupe particulièrement dangereux, elles conduisent en général à une radicalisation des populations ciblées, à des hausses des recrutements dans les mouvements hostiles à Israël et aboutissent à éliminer des individus qui, s'ils se sont livrés à des actes dont il est parfaitement normal d'exiger qu'ils répondent, auraient pu, dans certains cas,

Photo ci-dessus : Faux papiers utilisés dans les années 1950 par Adolf Eichmann. Cet ancien officier SS en charge des « affaires juives et de l'évacuation », qui avait réussi à échapper à la justice après la capitulation allemande, a été capturé en mai 1960 à Buenos Aires par des agents du Mossad. Il sera exfiltré en Israël pour y être jugé en 1961. (© Fundacion Memoria del Holocausto)

Photo ci-dessus : Eli Cohen, agent du Mossad mort pendu en place publique en Syrie en mai 1965, après avoir été démasqué. Ayant exercé pour le compte des services israéliens en Égypte puis en Syrie, et considéré comme un héros national par Israël, il a réussi à approcher de près les plus hautes autorités syriennes, facilitant notamment la victoire d'Israël dans la guerre des Six Jours. (DR)

L'opinion du renseignement israélien sur la menace iranienne

Ephraïm Halevy, directeur du Mossad de 1998 à 2002, qualifie de « terrible erreur » l'insistance du Premier ministre Benyamin Netanyahou à définir les ambitions nucléaires de l'Iran comme une question de vie ou de mort. (© Eli Itkin)

Yuval Diskin, ancien directeur du Shabak – le service de contre-espionnage israélien –, a déclaré que l'absence d'un accord de paix avec les Palestiniens est une menace autrement plus existentielle que le programme nucléaire iranien. (© Ziv Koren)

Pour aller plus loin

Éric Denécé, David Elkaïm, *Les services secrets israéliens : Aman, Mossad et Shin Beth*, Paris, Tallandier, 2014.

accepter sous certaines conditions une réduction du niveau des violences (9). À moyen et long terme, il n'est donc pas démontré que les exécutions extrajudiciaires renforcent durablement la sécurité d'Israël.

De même, la détention au secret pendant plusieurs années de Ben Zygier, un agent du Mossad d'origine australienne soupçonné de sabotage, qui a fini par se suicider, a suscité de vives réactions dans l'opinion. Après s'être abrité derrière le secret défense, le gouvernement israélien a fini par accepter d'indemniser la famille de celui qui n'a longtemps été connu que comme le « prisonnier X ».

Encore plus grave, les relations entre le Mossad et les plus hautes autorités gouvernementales ont traversé une zone de turbulence. Dès 2010, le Premier ministre Benyamin Netanyahou avait reproché au Mossad de devoir s'expliquer publiquement au sujet de l'opération de Dubaï : les visages des assassins de Mahmoud al-Mabhouh, filmés par les caméras de l'hôtel où les agents sont passés à l'action, étaient apparus sur toutes les télévisions du monde et le Canada et l'Australie, dont des faux

Photo ci-dessus :
Le 7 juillet 2010, des policiers polonais escortent Uri Brodsky, un prétendu agent israélien du Mossad, qu'un juge polonais a décidé d'extrader vers l'Allemagne. Il y est soupçonné d'avoir participé à la mise en place d'un commando responsable de l'assassinat de Mahmoud al-Mabhouh, membre du mouvement islamiste palestinien Hamas, retrouvé mort le 20 janvier dans un hôtel de Dubaï. Une semaine après son arrestation à l'aéroport de Varsovie, deux ministres israéliens avaient demandé à la Pologne de rapatrier Uri Brodsky en Israël. (© Grzegorz Jakubowski/PAP/AFP)

passeports fabriqués par le Mossad avaient été alors retrouvés, avaient exigé des excuses officielles. Quelques années plus tard, des rapports du Mossad allant à l'encontre des positions du Premier ministre sur le dossier nucléaire iranien sont apparus dans la presse quelques jours après son discours à l'Assemblée générale de l'ONU (2013) puis après la signature de l'accord de Vienne en 2015. En ces deux occasions, Benyamin Netanyahou, qui avait invoqué une menace nucléaire imminente et dénoncé la poursuite du programme nucléaire militaire par Téhéran, a été publiquement désavoué par ses services de renseignement (10). Une forme de défiance s'est alors installée.

Pour rétablir la confiance, le Premier ministre a choisi début 2016 de placer un proche, Yossi Cohen, à la tête du Mossad, en remplacement de Tamir Pardo. Selon Amir Rapaport, grâce à ses compétences unanimement reconnues et son lien privilégié avec Benyamin Netanyahou, Cohen a, depuis sa prise de fonctions, réussi à remettre son organisation au cœur du processus de décision de l'appareil sécuritaire israélien (11). Tout laisse à penser qu'il s'emploiera à démontrer que l'Iran joue un « double jeu » dans le dossier nucléaire : alors même que dans une grande majorité, la communauté internationale estime que l'Iran respecte ses engagements, obtenir du nouveau président américain Donald Trump une dénonciation, qui parait néanmoins très improbable, ou du moins un durcissement de l'accord de Vienne est une des priorités affichées de l'actuel gouvernement israélien. Seule ombre au tableau, Yossi Cohen fait l'objet d'une enquête au sujet de ses liens avec les propriétaires d'une société de sécurité, Blue Sky International (12).

Concernant les rapports du Mossad, et plus largement de la communauté du renseignement et de l'appareil sécuritaire israélien, avec l'actuel gouvernement, un dernier point mérite d'être mentionné. Un nombre croissant d'anciens chefs des services et de hauts gradés de l'armée critiquent la poursuite de l'occupation de la Cisjordanie. À l'instar des anciens chefs du *Shabak* dans *Gatekeepers* (13) et d'un ensemble de personnalités et d'organisation issues de la société civile israélienne, les Commandants pour la sécurité d'Israël (14) dénoncent l'absence de réelle volonté de négociation avec les Palestiniens et les dangers pour Israël de l'abandon de la solution à deux États (15). Compte tenu des parcours de ces hommes, leurs prises de position peuvent difficilement être qualifiées de « naïves » ou d'« antipatriotiques ». D'où l'embarras des tenants de la ligne dure, parmi lesquels le Premier ministre.

> « *À moyen et long terme, il n'est pas démontré que les exécutions extrajudiciaires renforcent durablement la sécurité d'Israël.* »

David Elkaïm

Notes

(1) Gordon Thomas, *Histoire secrète du Mossad : de 1951 à nos jours*, Paris, Nouveau Monde éditions, 2006.

(2) Le Mossad compte également six divisions fonctionnelles dont le rôle est de soutenir les divisions opérationnelles.

(3) Le film de son exécution à Damas, réalisé par la télévision officielle syrienne, a été retrouvé et diffusé sur Internet en septembre 2016.

(4) Sans les informations recueillies par le Mossad, grâce à ses contacts kenyans notamment, l'opération de sauvetage n'aurait probablement pas pu avoir lieu.

(5) Très vraisemblablement à raison en ce qui concerne Mahmoud al-Mabhouh.

(6) Piotr Smolar et Frédéric Bobin, « Le Hamas accuse le Mossad du meurtre en Tunisie de l'un de ses cadres », *Le Monde*, 18 décembre 2016.

(7) Cyrille Louis, « L'ombre du Mossad sur le meurtre d'un islamiste en Tunisie », *Le Figaro*, 19 décembre 2016.

(8) Jean-Paul Chagnollaud, « Les assassinats ciblés ou comment détruire un processus politique », *Confluences Méditerranée* 2013/3 (nº 86).

(9) Jean-Paul Chagnollaud va jusqu'à envisager que, pendant la Seconde Intifada, les tenants de la « ligne dure » aient délibérément approuvé certaines exécutions pour annihiler toute chance de dialogue avec les mouvements palestiniens et ainsi avoir les mains libres pour achever de détruire l'Autorité palestinienne.

(10) *Aman*, le renseignement militaire, a confirmé les analyses du Mossad.

(11) « Cohen's Mossad: One Year On », *Israel Defense*, janvier 2017.

(12) Ben Butler, « Israelis to probe Packer's Mossad tie », *The Australian*, 19 janvier 2017.

(13) Documentaire de Dror Moreh sorti en 2012.

(14) http://en.cis.org.il/

(15) Notamment dans http://en.cis.org.il/2017/01/25/the-dangers-of-annexing-the-west-bank.

Le *renseignement iranien* au service de la sauvegarde des mollahs

Par **Alain Rodier**, directeur de recherche chargé du terrorisme et de la criminalité organisée au Centre français de recherche sur le renseignement (CF2R).

Les services spéciaux, qui occupent une place privilégiée au sein de l'État iranien, ont pour mission de défendre le régime théocratique en place contre toute menace intérieure ou extérieure. Traditionnellement, leur premier objectif est l'influence ou la neutralisation des membres de l'opposition à domicile ou réfugiée à l'étranger. C'est ainsi que, depuis la révolution de 1979, des milliers d'opposants ont été liquidés, dont des centaines hors d'Iran (1).

Le VEVAK, ministère du Renseignement iranien

Entre 1981 et 1984, la SAVAMA a eu pour mission d'éliminer tout ce qui était considéré comme une opposition directe ou potentielle au régime des mollahs. Une fois que la situation a été jugée suffisamment stabilisée, le ministère du Renseignement et de la Sécurité nationale, VEVAK (ou MOIS) a été créé. Aujourd'hui, il porte le nom de ministère du Renseignement de la République islamique d'Iran. Tous ses chefs sont des religieux, comme actuellement le mollah Mahmoud Alavi. Il a repris les attributions de la SAVAK, le redoutable service spécial du Chah. Bien que nombre d'officiers de ce service aient été exécutés après la Révolution, le nouveau pouvoir en a retourné certains pour qu'ils apportent leurs compétences professionnelles à la constitution du nouveau service. En plus des missions traditionnelles, il doit approvisionner l'Iran en matériels soumis à embargo et préparer les représailles – particulièrement en utilisant le terrorisme d'État – au cas où les États-Unis ou Israël envisageraient une intervention armée.

Bien que ce ministère soit placé sous l'autorité du Conseil suprême de la Sécurité nationale (CSSN), il répond de ses actes directement auprès du Guide suprême de la Révolution, l'ayatollah Ali Khamenei. Son quartier général est situé à Téhéran, dans les anciens locaux de la SAVAK. Il comporterait 30 000 personnels civils dont plusieurs milliers seraient affectés à l'étranger. Cette estimation est imprécise car il est difficile de comptabiliser les officiers traitants (OT) présents pour des missions de courte ou moyenne durée à l'étranger. En général, un résident sous couverture diplomatique reste en place de trois à cinq ans. Un clandestin peut passer sa vie à l'étranger.

Le VEVAK est composé de cinq directions, placées sous l'autorité d'une direction générale qui porte le numéro 10 :

- la direction de l'Analyse et de la Stratégie (nº 11) remplit une mission d'analyse au profit des hautes autorités, mais s'occupe aussi des opérations de désinformation ;
- la direction de la Sécurité intérieure (nº 12) assure la protection des institutions étatiques et du contrôle des lieux de transit internationaux (aéroports, ports, frontières) ;
- la direction de la Sécurité nationale (nº 13) a pour mission de surveiller tous les mouvements d'opposition ;
- la direction du Contre-espionnage (nº 14) ;
- la direction du Renseignement extérieur (nº 15) regroupe la recherche et l'exploitation de renseignements. En son sein, le département nº 155 prend en charge les rapports avec les mouvements islamiques. Le département nº 157, qui est implanté au sein du ministère des Affaires étrangères, gère les postes implantés au sein des représentations diplomatiques.

À côté de ces directions se trouvent des départements, dont les affaires extérieures, le renseignement intérieur, la planification, l'étude des religions, la documentation ouverte, les opérations, la formation, l'administration, les approvisionnements, les services financiers, etc.

Les OT officiels servent à l'étranger sous couverture diplomatique. D'ailleurs, les services de renseignement iraniens agissent en étroite coopération avec leur ministère des Affaires étrangères. Pour leur part, les OT clandestins sont souvent des personnels d'Iran Air, de l'agence de presse IRNA, de la radiotélévision IRIB, d'associations culturelles ou caritatives, des étudiants, etc. Les banques iraniennes servent également à fournir discrètement les fonds nécessaires à la vie des réseaux clandestins. Traditionnellement, l'Irak, la Syrie, le Liban, la Jordanie, la Turquie, l'Égypte, les pays du golfe Persique et d'Asie centrale constituent des lieux d'implantation privilégiés pour les services iraniens. Enfin, l'importante diaspora libanaise répartie de par le monde sert de vivier humain pour recruter des collaborateurs via le Hezbollah (2).

Les services iraniens entretiennent des liaisons permanentes avec leurs homologues syriens, irakiens, soudanais, russes et tadjiks. En Europe, des postes importants ont été localisés à Paris, Bruxelles, Berlin, Vienne, Genève et Nicosie.

Photo ci-dessous : Croquis de l'audience du 2 novembre 1994 où comparaissaient les suspects de l'assassinat à Suresnes de l'ancien Premier ministre du chah d'Iran, Chapour Bakhtiar. Les services iraniens n'hésitent pas à aller jusqu'à l'élimination physique des opposants au régime iranien, même réfugiés à l'étranger. (© AFP/ Jean Chesnot)

Photo ci-dessus : Emblème du SAVAK, le service de renseignement du chah d'Iran fondé en 1957 avec l'aide de la CIA et du Mossad. La plupart de ses dirigeants furent exécutés sur l'ordre de Khomeini dès sa prise de pouvoir en 1979. (© Pajam)

Le ministère du Renseignement n'est pas doté d'un service « Action ». Ce type de mission est confié aux pasdarans, en particulier à la force Al-Qods. En règle générale, il apporte les renseignements nécessaires et les pasdarans s'occupent des opérations qui sont parfois violentes. Les actions les plus célèbres sont les attentats contre des détachements militaires français et américains au Liban en 1983, qui ont causé la mort de 299 personnes ; une série d'attentats à la bombe à Paris en 1986 (12 morts) ; les attaques contre l'ambassade d'Israël et la communauté juive à Buenos Aires, en 1992 et 1994 (125 tués) ; et vraisemblablement l'attentat des tours de Khobar en 1996 en Arabie saoudite (19 Américains tués et 372 personnes blessées). La dernière opération date de 2012, quand le Hezbollah s'est attaqué à un bus de touristes israéliens à Burgas, en Bulgarie (7 morts dont 5 Israéliens), pour venger les assassinats de scientifiques iraniens attribués au Mossad. Aujourd'hui, ces opérations sont mises en réserve car jugées contre-productives.

Les pasdarans, acteurs du renseignement iranien

L'Organisation du renseignement du Corps des Gardiens de la Révolution islamique est composée, quant à elle, de deux comités : celui du renseignement et celui de l'exécution des opérations. Étroitement liés au ministère du Renseignement, utilisant les mêmes couvertures, ses membres gardent cependant leur autonomie. On peut trouver certains d'entre eux à des postes d'attachés de défense. Ils servent alors ès qualité.

En Iran, les pasdarans ont des bureaux implantés dans tout le pays, et plus particulièrement au sein des unités militaires. Une partie de leur mission peut alors être apparentée à celle d'une « sécurité militaire ». En effet, les mollahs ont toujours gardé une grande défiance vis-à-vis des cadres de l'armée, même si aujourd'hui plus aucun officier n'a servi du temps du Chah. Le territoire est quadrillé par les milices Bassidji, une « garde nationale » à l'iranienne qui compterait plus de dix millions de membres. Elle est encadrée par des pasdarans détachés ou en retraite. Un certain nombre ont été dépêchés sur le front syro-irakien pour renforcer la force Al-Qods. Cette dernière, commandée par le général Qassem Suleimani, forte d'environ 20 000 hommes, a son état-major dans l'ancienne ambassade des États-Unis à Téhéran, rebaptisée « caserne Kazemi ». Elle est actuellement engagée sur le front syro-irakien et vraisemblablement au Yémen.

Il existe également de nombreuses autres structures de renseignement mais, généralement, elles sont pilotées par des officiers issus des pasdarans.

Quelles zones d'actions ?

Les cibles prioritaires actuelles sont l'Arabie saoudite et les mouvements sunnites extrémistes (salafistes/wahhabites). À ce titre, les fronts syro-irakien et yéménite ne sont que des guerres par procuration qui opposent Téhéran à Riyad et à ses alliés, voire aux ennemis mortels des Saoud : Al-Qaïda et Daech. Ainsi, depuis sa création, Al-Qaïda a été l'objet de toutes les attentions de la part des services iraniens. En 2001, ces derniers ont facilité l'exfiltration de membres d'Al-Qaida d'Afghanistan suite à l'intervention américaine. Depuis, Téhéran contrôlerait une branche d'Al-Qaïda basée en Iran (dont une partie de la famille de Ben Laden), ce qui a permis de ne pas trop subir la vindicte de la nébuleuse. Certains réfutent cette thèse en affirmant que les chiites et les sunnites ne peuvent s'entendre. C'est oublier un peu vite que l'imam Khomeiny a déclaré que les différences entre chiites et sunnites « sont plus historiques que théologiques ». En effet, l'Iran a soutenu des mouvements sunnites comme le Hamas ou le Jihad islamique palestinien qui se sont joints à la lutte contre l'« impérialisme judéo-chrétien ». Depuis, le Hamas a perdu l'aide iranienne suite à son soutien à la rébellion syrienne. Depuis 2015, il tente de retrouver la confiance de Téhéran. Al-Zarqaoui, le Jordanien qui est la référence historique de Daech, a été un temps traité par les services iraniens avant qu'il ne leur échappe et se mette à massacrer des chiites.

En Afghanistan, les tribus de l'Ouest du pays n'ont aucun secret pour les services iraniens depuis des décennies. Aujourd'hui, Téhéran s'appuie sur des ennemis d'hier, notamment le Hezb-e-Islami, qui fut combattu en son temps comme les talibans afin de contrebalancer l'influence d'Islamabad en Afghanistan.

Les mouvements kurdes sont par ailleurs une préoccupation permanente pour Téhéran. En premier lieu, le Parti pour une vie libre au Kurdistan (PJAK), la branche iranienne du Parti des travailleurs du Kurdistan (PKK), est considéré comme un danger et combattu en tant que tel. Cela étant, le PKK est parfois utilisé pour affaiblir le voisin turc. L'Iran entretient par ailleurs les meilleures relations avec l'Union patriotique du Kurdistan (UPK) de Jalal Talabani, qui bénéficie de son aide militaire et en matière de renseignement. En revanche, la méfiance est de mise avec le Parti démocratique du Kurdistan (PDK) de Massoud Barzani, le président du gouvernement régional du Kurdistan irakien, en raison des liens qu'il entretient avec l'Occident en général et les États-Unis en particulier, et plus secrètement avec Israël.

Photo ci-dessus : Site de l'attentat perpétré en juillet 1994 contre un bâtiment de Buenos Aires abritant plusieurs associations juives, et qui fit 84 morts et 230 blessés. Si l'attentat n'a jamais été revendiqué, les services iraniens constituent le principal suspect. (DR)

Enfin les services iraniens sont engagés dans une lutte sans fin contre Israël et les Américains, en particulier sur tout ce qui touche au programme nucléaire militaire. De plus, les mollahs, qui souhaitent la disparition de l'État hébreu, tentent de renforcer le Hezbollah dans la perspective d'une guerre à venir. Les réponses israélo-américaines sont musclées : sabotages (Stuxnet), opérations homo contre des scientifiques, etc.

Les services de renseignement iraniens jouent donc un rôle de tout premier plan pour soutenir le régime iranien confronté aux admonestations du président Donald Trump et à la lutte d'influence qui l'oppose aux Saoud au Proche-Orient. Ils sont très utiles tant la situation internationale est complexe et illisible et donnent à Téhéran une marge de manœuvre qui lui permet de naviguer à vue, nouant ou dénouant des alliances de circonstances (3). Tant qu'ils seront fidèles à leurs maîtres, il n'y a pas de raison de penser que le pouvoir en place à Téhéran risque d'être déstabilisé, car ils constituent une garde prétorienne particulièrement performante.

Alain Rodier

Photo ci-dessus : Un groupe de commandos des pasdarans participe à un exercice dans le détroit d'Ormuz. La force spéciale de ces derniers, la Force Al-Qods, fait office de branche action des services de renseignement iraniens, responsable des opérations clandestines dans le monde entier. (© Sayyed Shahab o din vajedi)

Notes

(1) Ce texte est une version remaniée et actualisée de la note d'actualité n° 200, « Les services iraniens », 5 janvier 2010, publiée sur le site du CF2R.

(2) Le Hezbollah libanais est une créature des services iraniens. Il leur sert de manière opérationnelle mais aussi financière, car ses liens avec le crime organisé mondial lui permettent de tirer de gros bénéfices des trafics auxquels il se livre directement ou indirectement.

(3) À titre d'exemple, si Téhéran intervient officiellement sur le front syro-irakien, ce n'est pas le cas au Yémen. L'emploi des services lui permet de démentir toute action qui tourne mal comme des cargaisons d'armes interceptées au large des côtes de ce pays, ce qui s'est déjà produit à plusieurs reprises.

analyse

Les services chinois à l'avant-poste des ambitions de Pékin

Par **François-Yves Damon**, sinologue, maître de conférences HDR honoraire, docteur de l'EHESS et chercheur au Centre français de recherche sur le renseignement (CF2R) (1).

Le parti communiste doit lutter sur les fronts extérieur – notamment contre les États-Unis – et intérieur, où il doit assurer la pérennité de son monopole politique, mettant en place des stratégies dans lesquelles les services de renseignement chinois ont une place déterminante.

Alors que l'expansionnisme chinois, dans les mers de Chine orientale et du Sud, se heurte aux résistances du Japon, des Philippines, de la Malaisie et du Vietnam, le « pivot » a concrétisé le soutien apporté à ces derniers par « l'adversaire principal » de Pékin : les États-Unis. En 2015, un ouvrage américain à sensation affirmait l'existence d'un plan chinois de cent ans devant conduire au remplacement des États-Unis par la Chine comme superpuissance mondiale. Une thèse aussitôt réfutée par le *Quotidien du Peuple*, l'organe officiel du Parti communiste chinois (2).

Face à cet adversaire principal, et afin d'éviter un affrontement direct qui lui serait défavorable, la Chine privilégie des stratégies indirectes mises en œuvre dans un espace non circonscrit, la « guerre hors limites » : « Pour la guerre hors limites, la distinction entre champ de bataille et non-champ de bataille n'existe pas. Les espaces naturels que sont la mer, l'air et l'espace sont des champs de bataille. Les espaces sociaux que sont les domaines militaire, politique, économique, culturel et psychologique sont des champs de bataille » (3). L'efficacité de la guerre hors limites suppose que des opérations soient menées conjointement dans ces différents espaces, dans lesquelles le rôle primordial revient aux services de renseignement.

Les opérations menées par les moyens déployés dans les quatre espaces réels – extra-atmosphérique, aérien, terrestre, et maritime – sont coordonnées et conduites par les deux espaces virtuels : électronique et réseaux, donnant ainsi une dimension stratégique à la guerre de l'information.

L'Académie des sciences militaires de l'Armée populaire de libération (APL), où est élaborée la stratégie chinoise, a, dans la dernière édition de sa *Zhanluëxue* (4), intitulé l'ensemble de ces opérations « Guerre des réseaux ».

Photo ci-dessus :
En juin 2015, le *Washington Post* révélait que les pirates informatiques chinois qui ont volé les données de millions de fonctionnaires américains avaient également réussi à récupérer des informations sur les personnels habilités à accéder à des données sensibles ou secrètes, ce qui représente une « catastrophe potentielle en matière de contre-espionnage » selon l'ancien conseiller général de la NSA et spécialiste en cybersécurité Joel Brenner. (© Shutterstock/BeeBright)

Lexique

Les Quatre modernisations
Introduites par Zhou Enlai en 1975, puis officiellement lancées en 1978 par Deng Xiaoping, les « Quatre Modernisations » marquent le début de l'ère des réformes destinées à faire de la Chine une grande puissance économique et indépendante. Elle couvrent les domaines suivants :
- l'agriculture,
- l'industrie,
- les sciences et technologies,
- la défense nationale.

Photo ci-contre :
Alors que la Chine a fait du renseignement une arme au service de son développement économique, Pékin a mis en place, dès la fin des années 1960, au sein de la communauté étudiante chinoise expatriée à l'étranger, un réseau d'espionnage dans le but de recueillir des informations de pointe classifiées. (© Shutterstock/ Darren Baker)

Photo ci-dessus :
En 2013 et 2016, le Comité central a créé deux commissions, toutes deux présidées par le président de la République et secrétaire général du parti, Xi Jinping, et destinées à coordonner les opérations de ses services de renseignement. (© Xinhua/Ding Lin)

La Guerre des réseaux

Cette guerre a pour objectif la neutralisation par intrusion dans les systèmes de communication et de transmission d'ordres de l'adversaire, et inversement, la sécurisation de ses propres systèmes face aux tentatives d'intrusion adverses.
Cette guerre est conduite par la Force de soutien stratégique (FSS), instituée à cet effet le 31 décembre 2015. Surnommée « Cloud Thinktank » de l'APL, la FSS doit fournir aux cinq commandements de théâtre les moyens informatifs appropriés à la conduite de la guerre électronique. Le général Gao Jin, jusqu'alors directeur de l'Académie des Sciences militaires, fut, dès janvier 2016, promu commandant de la FSS, assurant ainsi la continuité entre l'élaboration et la mise en œuvre de la guerre en réseaux (5).
Les trois services de renseignement militaire de l'APL – Deuxième Département (D2, 2000 personnels, renseignement humain ou HUMINT), Troisième Département (D3, 120 000 personnels, renseignement électronique ou ELINT) et Quatrième Département (D4, signaux ou SIGINT) –, qui dépendaient jusqu'alors de l'état-major général de l'APL, sont passés sous la tutelle de la FSS, qui les a répartis en trois composantes, bien que certains détails relatifs à l'organisation n'aient pas encore été communiqués (notamment la place du D2 (6)) :
- La *Cyberforce* ou *Département des systèmes de réseaux*, qui pourrait être une nouvelle appellation du D3, regroupe les hackers en charge de l'espionnage des réseaux adverses, ainsi que de l'attaque et la défense informatiques.
- La *Force spatiale*, chargée de la reconnaissance et de la navigation, gère les sites de lancement des satellites, leur lancement et leur pistage. La Seconde artillerie (missiles) lui aurait été subordonnée.
- La *Force électronique* (D4) doit encombrer et perturber les communications et radars ennemis.

La conduite de la « guerre en réseaux » procède de la doctrine de « défense active » (7) et doit être accompagnée des « Trois guerres légales » (8) (voir *infra*).

> *« Face à cet adversaire principal [les États-Unis], et afin d'éviter un affrontement direct qui lui serait défavorable, la Chine privilégie des stratégies indirectes mises en œuvre dans un espace non circonscrit : la « guerre hors limites ». »*

La doctrine de « défense active »

Cette doctrine prévoit deux phases d'opérations :

L'espionnage

Courante et non destructive, cette première phase consiste à pénétrer les réseaux de l'adversaire afin d'en détecter les points vulnérables. Elle consiste également à mener des attaques informatiques. C'est notamment la mission de l'unité 61398 (faisant partie du D3 et surnommée aussi APT1) qui serait, selon le rapport très médiatisé de la firme américaine de cybersécurité Mandiant (9), responsable de la plupart des attaques informatiques chinoises ciblant les États-Unis : « *APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations and has demonstrated the capability and intent to steal from dozens of organizations simultaneously* » [APT1 a méthodiquement volé des centaines de terabytes de données provenant d'au moins 141 organisations et a démontré sa capacité à voler ces données de douzaines d'organisations simultanément]. Si le site du ministère chinois de la Défense dénia tout fondement au rapport – « L'APL n'a jamais conduit de telles activités et le Gouvernement chinois est déterminé à poursuivre de tels crimes » (10) –, la revue *Zhanluëxue* précitée remet en question ce déni en reconnaissant l'existence de telles opérations et en listant (11) les trois types de forces à la manœuvre :
- les forces militaires de guerre en réseau, chargées de l'attaque et la défense ;
- les forces militaires mandatées, qui mènent des opérations de guerre électronique pour le compte des ministères civils de la Sécurité publique et de la Sécurité d'État ;
- les forces non gouvernementales, c'est-à-dire civiles, qui apporteraient spontanément leur appui à cette guerre électronique, et pourraient être mobilisées, organisées et intégrées à la guerre des réseaux. Le capital humain nécessaire aux opérations de guerre électronique se trouve en effet dans l'industrie civile, où l'APL va chercher ses hackers.

La destruction

Cette seconde phase, destructive, a pour but de rendre inopérants les réseaux adverses en attaquant les points vulnérables détectés au cours de la première phase. En cas de conflit avec les États-Unis en mer de Chine, deux unités de la Force électronique (D4), basées dans l'île de Hainan, auront, lors de cette deuxième phase, une mission de brouillage

des informations satellitaires destinées aux bâtiments de la VII[e] Flotte américaine.
L'unité 61398, qui contribue à la phase 1 d'espionnage, reçoit ses ordres de la Commission pour la science, la technologie et l'industrie de la défense nationale (COSTIND) de l'APL chargée de la réalisation du Plan 863. Lancé en 1983, le Plan 863 a pour objectif d'accélérer la modernisation des secteurs clés de la défense par le recours aux données étrangères acquises en sources ouvertes ou par espionnage. La Chine a d'ailleurs été accusée par le FBI de fournir par le biais de ce plan des fonds aux agents impliqués dans l'exportation illégale de données à partir du territoire des États-Unis. L'ouvrage *Chinese Industrial Espionage* citait notamment 31 cas dans lesquels les coupables ont, entre 2007 et 2011, été déférés en justice et condamnés (12).
L'apport du renseignement à la Recherche et Développement des secteurs clés programmés par le Projet 863 a même été officiellement reconnu : « Le renseignement est à la fois les yeux et les oreilles, le fer de lance et le conseiller des Quatre Modernisations (13) » (voir lexique en marge, NdlR).

> *« Depuis 2010 et le passage du taux de croissance annuel du PIB sous la barre des 10 %, le budget annuel destiné à la sécurité intérieure a dépassé celui destiné à la défense extérieure. »*

La doctrine des « Trois Guerres légales »

Adoptées en 2003 par la Commission militaire centrale, et conjointement lancées avec la « défense active », les « Trois Guerres légales » ciblent le domaine psychologique, le domaine médiatique et le domaine légal.
La cible de la guerre psychologique est l'opinion publique de l'adversaire principal et de ses alliés qu'il faut, en influençant ses perceptions, amener à douter de la légitimité de ses propres objectifs, voire de ses propres valeurs. Cette capacité d'influence de la propagande chinoise a été démontrée par le succès que rencontra en Occident la requalification en « révolution culturelle » du meurtrier coup d'État maoïste de 1966.
Les médias sont le moyen d'influence privilégié de la guerre psychologique. Des bots chinois auraient par exemple saturé les médias américains de messages pro-Trump et anti-Clinton pendant la campagne électorale (14). Inversement, une loyauté sans faille envers l'APL et le Parti est imposée aux médias chinois, ainsi que l'a rappelé en mai 2016 le président Xi Jinping.
Enfin, la guerre légale doit délégitimer l'adversaire en influençant le cadre légal tant que celui-ci est favorable à la Chine (transfert en 1971 du siège de membre permanent du Conseil de sécurité de Taïwan à la RPC) et en le rejetant dans le cas contraire (rejet en juillet 2016 de l'arbitrage de la Cour internationale de La Haye, dans le litige territorial en mer de Chine qui l'oppose aux Philippines).

Une lutte sur deux fronts

Si le parti communiste doit lutter sur le front extérieur, il doit faire de même sur le front intérieur, où il doit assurer la pérennité de son monopole politique. Or, la légitimité du parti apparait fragilisée : la corruption endémique qui le gangrène constitue la cause principale de cet affaissement et de la moindre pertinence idéologique de son discours. À côté des revendications démocratiques dont la figure emblématique demeure Liu Xiaobo, prix Nobel de la paix 2010, emprisonné depuis 2008, les protestations vont des émeutes rurales à la mise en ligne d'éléments d'information, visuels ou sonores, sur la corruption.
C'est pourquoi, depuis 2010 et le passage du taux de croissance annuel du PIB sous la barre des 10 %, le budget annuel destiné à la sécurité intérieure a dépassé celui destiné à la défense extérieure. Afin de mieux assurer la pérennité du monopole politique du parti communiste, le Comité central a, en novembre 2013, institué une « Commission de la Sécurité d'État » (CSE) inspirée du Directorate of National Intelligence (DNI) américain. La création de cette CSE aurait été évoquée dès 1997, mais empêchée par les résistances efficaces des organes et institutions menacés d'être dépouillés d'une partie de leurs attributions. Il a fallu attendre la détermination du nouveau président, Xi Jinping, et de sa faction, pour que soient muselées, au moyen d'une virulente campagne anticorruption, les oppositions les plus fortes.

Photo ci-dessous :
Le 25 septembre 2015, le président américain Barack Obama accueille son homologue chinois à Washington sur fond de tensions liées à des accusations d'espionnage, les deux pays s'accusant mutuellement d'arrestations pour espionnage jugées abusives d'Américains d'origine chinoise ou d'entrepreneurs et de scientifiques chinois. Parallèlement, Washington aurait haussé le ton au sujet de l'opération chinoise « *Fox Hunt* », qui consiste à faire traquer et intimider aux États-Unis, par des agents chinois munis de visas de tourisme, des « fugitifs économiques » ou des « fonctionnaires corrompus » chinois, afin de les forcer à rentrer au pays. (© Michael Buchanan)

Présidée comme la FSS par Xi Jinping, la CSE regroupe l'ensemble des services de police, renseignement, sécurité et judiciaires, et dispose de l'autorité nécessaire à la centralisation des informations et à la coordination de tous ces services, au premier rang desquels les ministères civils de la sécurité d'État (MSE) et de la Sécurité publique (MSP).
En effet, bien que le MSP n'ait pas vocation au renseignement, trois de ses 37 services y contribuent :
• le *Bureau 610*, « Dissidences religieuses », qui a pour première tâche l'infiltration et la traque des membres du Falun Gong (15), et pour seconde, celle de veiller à l'application des « Nouvelles

Photo ci-dessous :
Le 16 mars 2017, un représentant du groupe chinois Huawei présente ses activités liées au *cloud* lors d'un salon en Allemagne. Le *Canard Enchainé* a révélé qu'à la fin de l'année 2016, une réunion « ultra-secrète » s'est tenue au Palais de l'Élysée avec les responsables du renseignement français pour évoquer la protection d'un *cloud* souverain : l'administration française s'inquiète d'un récent partenariat mondial conclu entre le français Orange et le chinois Huawei sur le *cloud,* prévoyant que le groupe chinois fournira des équipements matériels et logiciels qui pourraient lui donner par la suite accès à des données sensibles. Le journal français rappelle également que Huawei a été créée « par un ex-colonel de l'armée chinoise » et que la firme est « abreuvée de contrats militaires par Pékin ». (© Xinhua/ Shan Yuqi)

Régulations sur la Réincarnation du Dalaï Lama » qui criminalisent depuis 2007 le rôle des religieux en exil – dont le 14e Dalaï Lama – et exigent que toute réincarnation soit approuvée par le Conseil d'État ;

- le *Bureau du contreterrorisme* cible les djihadistes et les séparatistes ouïghours (16), en vertu de la loi de décembre 2015, qui donne une définition large du terrorisme : « Toutes propositions et actions visant à générer la panique sociale, mettre en danger la sécurité publique, porter atteinte aux personnes et à la propriété ou contraindre les organes nationaux et les organisations internationales par l'usage de la violence de la destruction et de l'intimidation dans le but d'atteindre leurs objectifs politiques, idéologiques, et autres » ;
- le *Bureau de supervision du réseau internet,* plus connu sous l'appellation de « Grande muraille pare-feu », créé en 2007, est destiné à guider l'opinion. Acteur essentiel de la guerre des médias sur le front intérieur, ses filtres censurent les accès aux données considérées comme susceptibles d'affecter la stabilité sociale. La loi de juillet 2015 sur la cybersécurité interdit, entre autres délits, de perturber l'ordre social sur le réseau.

Le ministère de la sécurité d'État (MSE) est, lui, subdivisé en 18 bureaux parmi lesquels :

- les B2 et B3, qui sont affectés au renseignement à l'étranger. Le B2 se consacre au recueil de renseignements internationaux collectés sur les décisions à caractère stratégique des gouvernements étrangers en envoyant des agents clandestins sous couverture (banques, assurances, sociétés commerciales, compagnies aériennes ou de navigation, ambassades et consulats, correspondants de presse, professeurs chinois invités, étudiants chinois dans les universités étrangères) ou en recrutant des agents au sein des membres de la diaspora chinoise. Le B3 se focalise sur le renseignement économique et technologique. Lors d'une conférence de cadres du MSE en 1996, le vice-Premier ministre Zou Jiahua saluait « les camarades en missions spéciales et les dizaines de milliers de héros anonymes qui servent loyalement leur mère patrie en occupant leurs postes à l'étranger » ;
- les B7 et B8, qui se consacrent à l'espionnage et au contre-espionnage sur le territoire chinois ;
- le B18, qui est attaché au contre-terrorisme ;
- le B12, dont la mission est la surveillance de l'opinion publique : c'est lui qui a réglé le sort de la centaine d'intellectuels libéraux qui, le 27 février 2013, ont diffusé sur les réseaux sociaux un appel à la ratification par l'Assemblée nationale populaire du Pacte international relatif aux droits civiques et politiques.

La Corée du Nord, source de renseignement

Enfin, les services chinois bénéficient des relations privilégiées entre Pékin et Pyongyang. Nucléarisée, donc sanctuarisée, la Corée du Nord demeure en effet un élément clé de la stratégie de défense chinoise. Comparables à l'ex-Stasi en Allemagne fédérale, les services de renseignement nord-coréens disposent de réseaux d'espionnage en Corée du Sud et parmi la vaste communauté coréenne présente au Japon. La transmission de ces renseignements au service du renseignement humain de l'APL peut ainsi être marchandée contre la continuation de la bienveillance chinoise envers l'imprévisible Corée des Kim.

La Chine, dans cette guerre des réseaux, a l'avantage du nombre : elle dispose en effet, avec ses 500 millions d'internautes, d'une réserve considérable de hackers aptes à se porter en appui de l'Unité 61398. Cet avantage suffira-t-il à compenser le handicap d'avoir à tenir deux fronts, et notamment le front intérieur, où nombre de gens aspireraient à une vie qui ne soit plus « dominée par le caractère passif » (17) ?

François-Yves Damon

Notes

(1) Également chargé des études de l'association régionale Nord-Pas-de-Calais-Belgique-Luxembourg (AR 15) de l'Association des anciens auditeurs de l'IHEDN, membre de l'AASSDN (Amicale des anciens des services spéciaux de la défense nationale) et ancien collaborateur d'un service de renseignement français.

(2) Michael Pillsbury, *The Hundred-Year Marathon*, New York, Henry Holt and Co, février 2015. « Qudai Meiguo ? Zhongguo mei gongfu xiang zhei shi » (« La Chine n'a pas pris la peine d'y penser »), *Le Quotidien du Peuple*, 2 février 2015.

(3) Qiao Liang et Wang Xiangsui, *La guerre hors limites* (Chao xian zhan, 1999), traduit en français par Hervé Denès, Paris, Rivages, 2003, p. 288.

(4) *Zhanluëxue* (« The Science of Military Strategy »), 2013.

(5) http://jz.chinamil.com.cn/gd/2016-01/01/content_6839727.htm

(6) Les quatre missions du D2 étaient : l'analyse des publications étrangères contenant des renseignements de nature militaire ; l'affectation d'officiers de renseignement dans les services des attachés militaires de toutes les représentations diplomatiques chinoises à l'étranger ; le recrutement d'agents extérieurs de renseignement ; l'organisation des opérations clandestines.

(7) *Zhanluëxue* 2013, *op. cit.*, p. 103.

(8) *Ibid.*, p. 131.

(9) https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf. .

(10) *Guofangbuwang*, 20 février 2013.

(11) *Zhanluëxue* 2013, *op. cit.*, p. 196.

(12) William C. Hannas, James Mulvenon, Anna B. Puglisi, *Chinese Industrial Espionage*, Londres, Routledge, 2013, Chapitre 9, p. 216-229, et Appendix 1, « Case Histories of Chinese Industrial Espionage », p. 256-273.

(13) *Zhonguo qingbao* (*Chinese Intelligence*), Bao Changhuo ed., Keji chubanshe, 2013, p. 66.

(14) « Automated Pro-Trump Bots Overwhelmed Pro-Clinton Messages, Researchers Say », *The New York Times, 17 novembre 20*16 et Liveleak, « New York Times, Washington Post get 50-60% of Site Traffic from Chinese Bots ».

(15) Le Falun Gong est une méthode de *qi gong* – gymnastique traditionnelle chinoise basée sur la respiration – recherchant le développement physique et spirituel. Après en avoir soutenu la pratique, les autorités chinoises ont tenté (en vain) de noyauter le mouvement. Ses membres sont depuis persécutés et réduits à la clandestinité. (NdlR)

(16) Marc Julienne, Moritz Rudolf, Johannes Buckow, « The Terrorist Threat in China », *The Diplomat*, 26 mai 2015.

(17) Evan Osnos, *Chine : l'âge des ambitions*, Paris, Albin Michel, 2015, p. 432. La phrase passive est, en langue chinoise, introduite par une particule grammaticale (« *bei* »), employée ici métaphoriquement pour caractériser l'absence de démocratie qui contraint les citoyens chinois à une vie politiquement passive.

Le *renseignement indien* en quête d'efficacité

Par **Alain Lamballe**, général de brigade et ancien diplomate, spécialiste de l'Asie du Sud ayant effectué l'essentiel de sa carrière militaire dans le renseignement et les relations internationales, et président d'honneur de l'association Asie Moyen-Orient (AMO) à l'Institut des hautes études de défense nationale (IHEDN).

Les services de renseignement indiens ont été organisés relativement tard. Il a en effet fallu deux guerres avec le Pakistan en 1947 et en 1965 et une guerre avec la Chine en 1962 pour que les autorités indiennes prennent enfin conscience de l'importance du renseignement et reconnaissent la nécessité de créer un véritable service spécialisé destiné à recueillir l'information au-delà des frontières. Les domaines privilégiés concernent les problèmes politiques et sécuritaires, la lutte contre le terrorisme constituant une priorité. La recherche du renseignement porte en tout premier lieu sur les pays voisins, surtout le Pakistan et la Chine. Mais pour les informations scientifiques, elle s'étend aux autres pays, principalement occidentaux. La diaspora présente sur tous les continents possède en son sein quelques éléments hostiles qu'il convient de surveiller (1), mais elle sert aussi à accroitre l'influence indienne dans le monde.

Des services encore jeunes et inexpérimentés

Aujourd'hui, l'Inde possède trois principaux services de renseignement :

• **L'Intelligence Bureau (IB)** s'occupe du renseignement intérieur. C'est le plus ancien des services de renseignement puisqu'il date de l'époque coloniale. Jusqu'en 1968, il s'occupait aussi bien du renseignement extérieur que du renseignement intérieur mais ses effectifs étaient essentiellement composés de policiers. Depuis sa création, l'IB est rattaché au ministère de l'Intérieur. Son directeur est toujours un policier. Ses effectifs seraient de l'ordre de 11 000 personnes, dont près de 5000 chargées du recueil d'informations, ce qui est très peu pour un pays de plus de trois millions de km² et peuplé de presque un milliard trois cents millions d'habitants, confronté à d'énormes défis sécuritaires. Si l'IB est bien implanté sur l'ensemble du territoire indien, un nombre insuffisant de ses membres parle les langues des indigènes tribaux, les *adivasis*, qui alimentent les rangs des mouvements maoïstes.

À certaines reprises, ce service a été accusé d'ingérences dans le fonctionnement démocratique des institutions, en contribuant au remplacement de gouvernements provinciaux.

• **La Research and Analysis Wing (R&AW)**, créée en 1968, est rattachée au Premier ministre. Elle a pour vocation de rechercher le renseignement politique, économique, scientifique et militaire à l'extérieur, de manière ouverte ou clandestine, et de détecter les activités d'espionnage à l'encontre du pays. Ses effectifs seraient de l'ordre de 10 000 personnes, civils et militaires. Des difficultés de recrutement de personnels de qualité ont gêné l'expansion du service. L'insuffisance du nombre de linguistes est criante, même pour opérer dans les pays géographiquement proches du Moyen-Orient et d'Asie centrale. Peu d'experts comprennent le chinois.

La R&AW dispose en outre d'un bras armé, la **Special Frontier Force (SFF)** créée en 1962, donc bien avant la naissance de la R&AW, et qui avait initialement incorporé des Tibétains car elle avait pour but d'aider une éventuelle guérilla au Tibet. Depuis, ses missions se sont diversifiées. Elle est, par exemple, intervenue pendant la guerre de 1971 dans le Pakistan oriental d'alors.

• Il existe également au sein de l'état-major interarmées, qui n'est en fait qu'un embryon, un service de renseignement, la **Defence Intelligence Agency (DIA)**, mais elle ne remplit pas vraiment son rôle, l'armée de terre, la marine et l'armée de l'air ayant conservé leurs services spécialisés, dénommés respectivement **Directorate of Military Intelligence (DMI)**, **Directorate of Naval Intelligence (DNI)** et **Directorate of Air Intelligence (DAI)**. Ces organismes souffriraient tous d'un manque de cadres de qualité.

Une coordination difficile

La suspicion entre civils et militaires, très fréquente en Inde, s'étend au domaine du renseignement. Elle s'est renforcée au fil des ans. Les dysfonctionnements ont été pris en compte. La coordination et la supervision des différents services de renseignement civils et militaires sont assurées par le Joint Intelligence Committee (JIC), créé en 1990. Le JIC sert de secrétariat pour le National Security Council (NSC), établi également en 1990, qui définit les grandes options stratégiques. Le JIC est rattaché au secrétariat du Cabinet interministériel, donc au niveau du Premier ministre. Son directeur provient en général de l'un des services de renseignement.

Le National Security Adviser (NSA) joue aussi auprès du Premier ministre un rôle majeur en matière de renseignement mais ses responsabilités dépassent largement ce domaine puisqu'elles incluent celles de conseiller le chef du gouvernement sur tous les problèmes de sécurité, de négocier avec les pays étrangers sur les affaires stratégiques et de présider le conseil exécutif de la Nuclear Command Authority (NCA). Le poste a été créé en 1998.

Deux organismes, le Multi Agency Centre (MAC) et la Joint Task Force on Intelligence (JTFI) ont été créés au sein de l'IB. Le MAC a pour mission de recueillir et coordonner les informations relatives au terrorisme et le JTFI doit transmettre les informations aux gouvernements provinciaux en temps réel et renforcer les capacités antiterroristes des polices provinciales. En réalité, ces deux organismes font preuve d'inefficacité à cause d'un manque de personnels et d'équipements.

Sur le terrain, au niveau des provinces, des contacts réguliers ont lieu entre les services civils et militaires. Mais ils sont souvent de médiocre qualité. De plus, la police locale ne coopère pas toujours en ce qui concerne la recherche et l'échange d'informations sur les diverses insurrections qui agitent le pays.

Enfin, les services de renseignement indiens éprouvent des difficultés à pénétrer les mouvements extrémistes, particulièrement ceux qui se réclament de la mouvance islamiste. Ils ne disposent en général que d'un nombre insuffisant de musulmans au sein de leurs effectifs, qui s'explique sans doute par la crainte d'être infiltrés. Mais pourtant, sans musulmans, toute pénétration des organisations djihadistes est impossible.

Alain Lamballe

Note

(1) Notamment les militants cachemiris et sikhs actifs à l'étranger, en particulier dans les pays européens et nord-américains ainsi qu'en Australie.

Photo ci-dessous : Photographie du faux passeport de Kulbhushan Yadav, accusé par le Pakistan d'être un espion indien du RAW, arrêté au Baloutchistan en mars 2016 et soupçonné de participer de manière directe ou indirecte à des activités subversives au Pakistan, notamment dans le but de saboter le projet sino-pakistanais de corridor économique. (© Muhshusa)

L'ISI pakistanais : un État dans l'État ?

Par **Alain Lamballe**, général de brigade et ancien diplomate, spécialiste de l'Asie du Sud ayant effectué l'essentiel de sa carrière militaire dans le renseignement et les relations internationales, et président d'honneur de l'association Asie Moyen-Orient (AMO) à l'Institut des hautes études de défense nationale (IHEDN).

Le service de renseignement extérieur pakistanais, l'ISI, véhicule les fantasmes les plus divers en raison de ses relations ambiguës avec certains groupes islamistes. Fondé en 1948, il n'en demeure pas moins le plus important et le plus puissant des services de renseignement pakistanais, et un acteur incontournable de la politique pakistanaise et de sa politique étrangère.

Quels sont les services de renseignements pakistanais ?

Les services de renseignement pakistanais sont composés d'un service de renseignement intérieur, un service de renseignement extérieur et de services de renseignement propres aux armées.

• **Le Directorate General for Inter-Services Intelligence (ISI)** est responsable du renseignement extérieur. C'est de loin le service le plus important du pays. Son appellation possède une connotation militaire puisque « *Inter-Services* » évoque les trois armées. Mais les attributions de l'ISI vont bien au-delà des seuls renseignements d'ordre militaire. Elles s'étendent à tous les domaines politique, économique, scientifique... L'interception des communications est de son ressort. La surveillance des personnels militaires, des diplomates pakistanais servant à l'étranger et des diplomates étrangers servant au Pakistan relève également de sa compétence

• **L'Intelligence Bureau (IB)**, créé au début des années 1950, s'occupe du renseignement intérieur. Son appellation est identique à celle du service indien équivalent. Il est rattaché au ministère de l'Intérieur. L'IB, chargé du contre-espionnage, surveille les agents étrangers et les terroristes présumés. Il s'intéresse aussi au trafic de drogue. Son directeur rend compte directement au Premier ministre. Très souvent, l'armée de terre a imposé la désignation du directeur qui, dans le passé, venait de ses rangs.

• Les trois armées (terre, air et mer) possèdent chacune un service de renseignement. Celui de l'armée de terre, le **Directorate of Military Intelligence (DMI)**, dispose de cellules sur l'ensemble du territoire pakistanais : les Field Intelligence Units (FIU). Le **Directorate of Naval Intelligence (DNI)** et le **Directorate of Air Intelligence (DAI),** d'importance moindre, complètent le système de renseignement militaire. Le président du Joint Chiefs of Staff Committee, un embryon d'état-major interarmées, n'exerce aucune responsabilité en matière de renseignement.

L'ISI, un service omnipotent ?

L'ISI dépend du ministère de la Défense. Une vaine tentative a été faite par le Premier ministre en 2008 pour rattacher au ministère de l'Intérieur ce service omnipotent aux missions étendues. Le directeur de l'ISI est censé informer directement le Premier ministre. Mais en réalité, il rend compte d'abord au chef d'état-major de l'armée de terre qui décide de ce qui peut être communiqué au chef de l'exécutif.

Le directeur de l'ISI est toujours un général de corps d'armée de l'armée de terre. L'alternance entre les trois armées ne joue pas. Mais les subordonnés directs du directeur peuvent appartenir à la marine et à l'armée de l'air aussi bien qu'à l'armée de terre. Des affectations à l'ISI favorisent les carrières. Plusieurs directeurs de l'ISI sont ensuite devenus chef d'état-major de l'armée de terre.

Les effectifs de l'ISI ont été longtemps majoritairement militaires, mais ce n'est plus le cas. Aujourd'hui, il y a autant de civils que de militaires et anciens militaires. Les militaires détachés n'y restent généralement que quelques années avant de rejoindre leurs affectations d'origine. Les civils au contraire, peuvent y faire carrière. Les effectifs globaux sont évalués à 4000 personnes mais des chiffres supérieurs sont parfois donnés. Ils étaient de l'ordre de 20 000 à l'époque de Zia-Ul-Haq (1977-1988), lors de l'occupation de l'Afghanistan par les Soviétiques.

Le budget dont dispose l'ISI est inconnu. Le chiffre avancé de 300 millions de dollars est sans doute inférieur à la réalité. Aux fonds officiels se sont ajoutées, et s'ajoutent peut-être encore, des ressources complémentaires apportées par le trafic de drogue avec l'Afghanistan, où la culture du pavot est courante.

Enfin, les activités de l'ISI ne se limitent pas à la recherche et à l'exploitation du renseignement à l'extérieur des frontières. Le service s'intéresse en effet également à la situation intérieure du pays. Tous les gouvernements, civils et militaires, ont utilisé l'ISI pour tenter de neutraliser leurs adversaires politiques. Mais c'est en définitive l'armée de terre qui décide des actions à mener.

L'ISI, acteur clef de la diplomatie pakistanaise

La plupart des analystes politiques considèrent que l'ISI oriente la politique étrangère du Pakistan – même si les militaires ne sont pas au pouvoir –, tout particulièrement à destination de l'Inde et de l'Afghanistan. Pour ramener la paix en Afghanistan, l'ISI apparaît comme un interlocuteur indispensable lors de négociations avec les talibans et leurs associés, car ces groupes militants lui sont parfaitement connus.

Parallèlement, alors que l'Inde et le Pakistan se sont affrontés au cours de trois guerres majeures et que les sujets de tensions sont aujourd'hui encore nombreux, l'ISI mène depuis sa création de nombreuses actions à destination de son voisin indien.

Déjà, à l'époque précédant le démembrement du Pakistan, l'ISI pouvait à partir de l'aile orientale intervenir facilement dans les provinces indiennes du Nord-Est pour soutenir les insurrections diverses conduites par de nombreux groupes ethniques minoritaires. Son action s'est prolongée après 1971, date de la création du Bangladesh, lorsque le Bangladesh National Party (BNP) (1), formation politique anti-indienne, était au pouvoir à Dacca. Elle est aujourd'hui plus limitée car l'Awami League (AL), qui dirige le gouvernement, est pro-indienne.

Les actions de l'ISI en Inde sont faites d'échecs et de succès. En 1965, lors de la guerre indo-pakistaise, ses informations sur l'Inde et son armée étaient insuffisantes et parfois inexactes. En 1967, il ne détecte pas une tentative de coup d'État fomenté par de jeunes officiers de marine, qui sera dévoilée par la police de Karachi. Le service de renseignement a également été inefficace lors des événements qui ont conduit au démembrement du pays et à la création du Bangladesh en 1971. L'ISI a même échoué

dans sa tentative de créer un Pendjab sikh indépendant, le Khalistan, malgré les efforts déployés dans les années 1980 et au début des années 1990 en faveur des insurgés actifs sur le sol indien (2). L'aide fournie aux militants indépendantistes opérant au Jammu-et-Cachemire indien n'a pas non plus été couronnée de succès. Des camps existent encore au Pakistan pour héberger, entrainer et armer les militants destinés à combattre au Cachemire contre les forces de sécurité indiennes (3).

Historiquement, l'ISI a toujours cherché à infiltrer les forces de sécurité indiennes, notamment par le recrutement de musulmans. Il entretient également des contacts avec les insurgés maoïstes agissant dans le centre de l'Inde, peut-être en liaison avec son homologue chinois. Le service est aussi en liaison avec diverses organisations islamistes indiennes, étudiantes en particulier. Il a été accusé d'avoir commandité les actes terroristes qui ont frappé Mumbai en mars 1993 et en novembre 2008. L'ISI mènerait en outre lui-même des opérations contre les Indiens en Afghanistan (4). Il serait ainsi responsable de la mort de techniciens indiens qui ont construit un réseau routier dans le Sud de l'Afghanistan pour le raccorder au réseau iranien desservant le port de Chabahar.

L'ISI est actif ailleurs à l'étranger. C'est notamment le cas au Népal ou au Bangladesh que l'ISI utilise pour faire passer en Inde de la fausse monnaie indienne en vue de désorganiser l'économie. Dubaï et les pays du Sud-Est asiatique servent également à cette fin. L'ISI affirme par ailleurs sa présence à Sri Lanka et aux Maldives.

À l'étranger, l'ISI surveille également les éléments qui lui sont hostiles, c'est-à-dire en tout premier lieu les services de renseignement indiens et les nationalistes baloutches. Il ne se contente pas de missions défensives mais mène des offensives, par exemple en aidant les Cachemiris indiens souhaitant le rattachement de leur région contestée au Pakistan.

Enfin, la coopération dans le domaine scientifique avec les pays occidentaux a permis à certains experts pakistanais d'avoir accès à des informations confidentielles. On peut supposer qu'ils agissaient pour leur propre compte à des fins de notoriété ou/et financières ou bien qu'ils opéraient dans le cadre de l'ISI. Le cas le plus célèbre est celui du physicien nucléaire Abdul Qadeer Khan, qui avait réussi à subtiliser des données secrètes alors qu'il travaillait dans un centre de recherche néerlandais dans les années 1980.

Photo ci-contre : Benazir Bhutto, Première ministre du Pakistan en visite à Washington, en juin 1989. Dans les année 1990, l'ISI fut impliqué dans le scandale politique du Mehrangate, qui visait à empêcher la réélection de Benazir Bhutto en mobilisant des fonds pour financer la campagne de ses adversaires politiques. (© Gerald b. Johnson, DoD)

L'ISI, acteur d'un double jeu avec les Américains et les islamistes

Dans la décennie 1980, c'est l'ISI qui a orienté et aidé les moudjahidines dans leur lutte contre l'occupant soviétique en Afghanistan. Les armes et les équipements fournis en grande partie par les États-Unis transitaient sous son contrôle par le territoire pakistanais et les insurgés trouvaient refuge tout le long de la frontière afghano-pakistanaise, notamment dans les zones tribales. Pendant la période d'occupation de l'Afghanistan par les troupes soviétiques, les relations entre l'ISI et la CIA étaient excellentes. Elles sont aujourd'hui tendues.

En effet, les Américains accusent l'ISI d'instrumentaliser les talibans. Ce n'est pas l'ISI qui se trouve à l'origine de la création des talibans mais dès que ceux-ci ont consolidé leur pouvoir, plus précisément lorsqu'ils ont conquis Kandahar en novembre 1994, il s'est intéressé à eux et les a soutenus. Dans les années qui ont suivi, l'ISI a contribué à former de nouveaux talibans dans les écoles religieuses pakistanaises (les *madrasas*). C'est lui qui a aidé les talibans à prendre le pouvoir à Kaboul en 1996 et à consolider leur emprise sur le pays. Et c'est lui, qui, aujourd'hui, tout en luttant contre les talibans dits pakistanais, héberge et soutient les talibans dits afghans et les membres du réseau afghan Haqqani, lequel a été qualifié par l'ancien président du Joint Chiefs of Staff américain de « bras armé de l'ISI ».

Ainsi l'ISI a-t-il fourni des informations à la CIA pour permettre aux drones de cibler des dirigeants islamistes radicaux. La recherche de certains objectifs aurait été faite en commun par l'ISI et les services de renseignement américain et britannique, grâce à un réseau de sources humaines. Simultanément, les autorités pakistanaises s'insurgent contre ces attaques de drones pour apaiser l'opinion publique. L'ISI joue en réalité un double jeu, en donnant des renseignements pour éliminer des éléments qui commettent des attentats sur le sol pakistanais et en n'en donnant pas s'il s'agit de militants agissant en Afghanistan et au Cachemire. Certains analystes l'accusent même de fournir des armes aux talibans afghans et à leurs associés et d'être responsable d'attentats ayant coûté

Photo ci-contre : Le 5 février 2014, l'ancien chef de l'ISI, Hamid Gul (à gauche), participe avec le clerc islamiste Maulana Sami ul-Haq (à droite) – considéré comme le « Père des Talibans » – à un rassemblement organisé pour la Journée de Solidarité avec le Cachemire. Directeur général de l'ISI de 1987 à 1989, Hamid Gul a joué un rôle déterminant dans le soutien de l'ISI aux insurgés du Cachemire indien et à la résistance afghane contre les forces soviétiques, car il pensait pouvoir s'appuyer sur des éléments non étatiques pour déstabiliser un ennemi – même supérieur – et maximiser les gains géopolitiques et diplomatiques du pays. (© AFP/Aamir Qureshi)

la vie à des étrangers, dont des Indiens. Des membres d'organisations islamiques radicales centre-asiatiques et ouïghours s'entraîneraient dans les zones tribales pakistanaises en bénéficiant du soutien, ou tout au moins de l'indifférence, de l'ISI.
Des accusations ont aussi été portées par le Bundesnachrichtendienst (BND) contre l'ISI qui aurait espionné le détachement d'instructeurs de la police allemande déployé en Afghanistan. Ces implications donnent quelques fondements au sobriquet attribué à l'ISI par certains de ses détracteurs : « *Invisible Soldiers of Islam* ».
Selon toute vraisemblance, l'ISI savait où le chef d'Al-Qaïda, Oussama ben Laden, se trouvait. Peut-être même l'a-t-il aidé à se loger et à se mettre à l'abri des recherches menées par la CIA, tout au moins pendant quelques années. Néanmoins, le raid américain qui a abouti à la mort du chef d'Al-Qaïda le 2 mai 2011 à Abbottabad, ville au nord de la capitale, montre une défaillance de l'ISI, à supposer, bien sûr, qu'il n'était pas au courant.
Les nombreux attentats qui ensanglantent le pays montrent aujourd'hui l'inefficacité des services de renseignement pakistanais vis-à-vis de la menace terroriste.

Une coordination assurée par l'ISI et un fonctionnement opaque

Les cinq services de renseignement, Intelligence Bureau, Inter-Services Intelligence, Directorate Military Intelligence, Directorate Air Intelligence et Directorate Navy Intelligence agissent de manière indépendante et leurs activités se chevauchent parfois. Plusieurs réformes du renseignement ont toutefois été proposées. Elles incluent toutes la création d'un organisme coordinateur, un Joint Intelligence Committee. Mais celui-ci n'a jamais vu le jour en raison de la réticence des différents services à partager l'information. Dans les faits, c'est donc l'ISI qui assure la coordination des activités de renseignement, tout particulièrement celles qui concernent les pays étrangers.
Si une réforme a été possible dans la lutte contre le terrorisme, qui est aujourd'hui centralisée au niveau d'un organisme nouvellement créé, la National Counter Terrorism Authority (NACTA), les pratiques du renseignement pakistanais demeurent encore largement opaques. Les écoutes téléphoniques effectuées par les divers services de renseignement sont en principe encadrées par des textes législatifs, mais ceux-ci ne sont pas appliqués. Elles se pratiquent donc communément. Les arrestations sont parfois arbitraires. Les tortures ne sont pas rares pour obtenir des renseignements et des morts suspectes ont été constatées. Aucun contrôle parlementaire des activités de l'ISI et de celles des autres services de renseignement n'a jamais été exercé. Pour la première fois, l'exécutif réclame des comptes à l'ISI, même si cela reste timide.
Le pouvoir judiciaire, en l'occurrence la Cour suprême, se montre plus audacieux en exigeant la présentation des personnes disparues, pour la plupart des agents subversifs de la mouvance islamiste ou des mouvements indépendantistes baloutches. La Cour suprême demande des explications sur la disparition des personnes non retrouvées. Elle exige des justifications précises que l'ISI et le DMI ont parfois du mal à fournir, se contentant de dire que les personnes arrêtées recevaient des fonds de l'étranger et présentaient un danger pour l'État. Bien souvent, les personnes disparues sont mortes dans des conditions non élucidées.
Aujourd'hui, les organisations non gouvernementales jouent également un rôle pour renforcer la transparence et dénoncer la violation des droits de l'homme. Fait nouveau, la presse n'hésite plus à critiquer l'armée et les services de renseignement. Elle dénonce même parfois leurs pratiques extra-judiciaires illégales.

Alain Lamballe

Notes

(1) L'ISI a financé le BNP lors de la campagne électorale de 1991.

(2) Le Pakistan servait de base arrière aux militants sikhs qui recevaient des fonds, des armes et des munitions.

(3) Ces militants, appartenant à divers mouvements dont le Hizb-ul-Mujahideen, seraient au nombre de plusieurs milliers prêts à franchir la ligne de contrôle qui sépare les deux parties du Cachemire administrées par l'Inde et le Pakistan.

(4) L'attaque de l'ambassade indienne à Kaboul en 2008 est communément imputée à l'ISI.

Photo ci-dessous : Le 14 mai 2011, des Pakistanais défilent dans les rues de Karachi pour soutenir l'armée nationale et les services de renseignement (ISI) dont le chef, Riaz Fatyana, a offert sa démission au Parlement pakistanais suite au raid américain contre Oussama ben Laden, le 1er mai. Alors que le Pakistan et l'ISI sont suspectés d'avoir fermé les yeux sur la présence de l'homme le plus recherché au monde dans une ville de garnison située à 50 km de la capitale, Islamabad a condamné une telle accusation ainsi que la « violation de la souveraineté pakistanaise ». (© AFP/ Rizwan Tabassum)

analyse

Russie : un retour vers le KGB d'antan ?

La rumeur laisse entendre que l'ancien KGB, le Comité pour la sécurité d'État, la principale agence de sécurité de l'ex-Union soviétique dissoute en 1991, pourrait renaître de ses cendres. En effet, par souci d'efficacité, le Kremlin étudierait la possibilité de regrouper la majorité des services spéciaux en une seule entité. Elle pourrait retrouver le nom de ministère de la Sécurité d'État ou MGB, abandonné en 1953.

Par **Alain Rodier**, directeur de recherche auprès du Centre français de recherche sur le renseignement (CF2R).

Ce nouveau ministère regrouperait :

- le Service de renseignement extérieur (SVR), héritier du prestigieux « Premier directorat » du KGB ;
- le Service fédéral de sécurité de la Fédération de Russie (FSB), chargé des affaires de sécurité intérieure, mais également compétent pour le contre-espionnage sur toute la planète, et plus généralement dans les pays considérés comme faisant partie de la sphère d'influence russe ;
- le Service fédéral de protection (FSO), chargé de la protection des hautes personnalités et des installations gouvernementales (à l'exclusion du Service de sécurité présidentiel – SBP – qui resterait rattaché directement au Kremlin) (1).

Comme par le passé, la Direction générale des renseignements de l'État-Major des Forces Armées (GRU) conserverait son indépendance.

Aujourd'hui, les services de renseignement russes sont extrêmement actifs, avec pour objectifs désignés l'OTAN, le terrorisme d'origine islamique et le crime organisé. En outre, le SVR est aussi chargé du renseignement économique et industriel. Mais une question se pose : que font vraiment ces services en dehors de tous les phantasmes développés dès que l'on parle de l'espionnage russe ? Rien de tel que des cas concrets pour tenter de le découvrir.

Photo ci-dessus :
Logo du KGB. Créé en 1954 et dissout en 1991, le KGB (Comité pour la Sécurité de l'État) constituait le principal service de renseignement de l'URSS post-stalinienne, en charge de missions étendues (l'espionnage extérieur, le contre-espionnage, la liquidation des opposants politiques et des organisations contre-révolutionnaires en URSS et à l'étranger, la surveillance des frontières, la sécurité du Parti communiste, des chefs de l'État, et des propriétés de l'État soviétique) et pouvant s'appuyer sur des moyens et un effectif très importants, à l'image de son influence dans le pays. (© tlegend)

Photo ci-dessus :
Le 19 décembre 2016, le président russe Vladimir Poutine rencontre, en présence de son ministre des Affaires étrangères, Sergueï Lavrov (à gauche), le directeur du SVR, Sergueï Narychkine (à droite) et celui du FSB, Alexandre Bortnikov, pour évoquer l'assassinat de l'ambassadeur russe à Ankara. En octobre 2016, l'un des principaux journaux russe, *Kommersant*, annonçait une réorganisation des services de renseignement qui réunirait le FSB et le SVR au sein d'un grand service qui deviendrait le ministère de la Sécurité d'État. (© kremlin.ru)

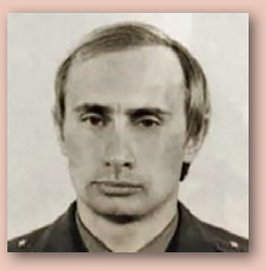


Photo ci-dessus :
Photographie de Vladimir Poutine, actuel président de la Fédération de Russie, alors qu'il était officier du KGB. Après y avoir fait carrière, il fut nommé directeur du FSB par Boris Eltsine en 1998. (© Kremlin.ru)

Le SVR, le service d'« espionnage » extérieur de Russie

Les 13 000 fonctionnaires du SVR sont responsables du recueil à l'étranger et par moyens illégaux de tout renseignement pouvant intéresser le Kremlin dans les domaines politique et économique.

L'échange de Vienne

Le 9 juillet 2010, une scène surréaliste se déroule sur le tarmac de l'aéroport de Vienne, largement couverte par la presse. Dix agents de renseignement du SVR sont échangés contre quatre « traîtres » russes qui viennent d'être graciés par le président Dmitri Medvedev. Les « traîtres » russes étaient les suivants :

- Alexandre Zaporojski : Cet ex-colonel du SVR a fait défection aux États-Unis en 1997. Or, en 2001, il est ramené en Russie lors d'une opération d'exfiltration. Il est condamné en 2003 à dix-huit ans de prison pour haute trahison. Il paye le fait d'avoir renseigné les Américains sur la présence de taupes aux États-Unis dont les plus connues sont Aldrich Ames et Robert Hanssen.
- Guennadi Vassilenko : Cet ancien colonel du GRU a contacté l'ambassade des États-Unis à Moscou pour proposer ses services. C'est un classique dans le monde du renseignement. Il a été condamné à huit années d'incarcération en 2002.
- Sergueï Skripal : Cet ancien colonel des forces armées russes, arrêté en 2004, a été condamné à treize ans de prison en 2006 pour avoir collaboré avec le MI6. Comme il aurait été recruté par les Britanniques dans les années 1990, il a eu le temps de fournir des informations intéressantes.
- Igor Soutiaguine : Ce spécialiste en armement nucléaire a été arrêté en 1999. Jugé en 2000, aucune charge n'avait alors été retenue contre lui. Mais il avait finalement été condamné en 2004 à quinze ans de camp de travail pour avoir communiqué des informations sensibles aux Britanniques, qui les auraient retransmises à la CIA.

Les dix agents du SVR rendus à la Russie, quant à eux, constituaient un réseau clandestin d'officiers de renseignement russes qui s'était implanté aux États-Unis dans les années 1990. Ces derniers devaient s'infiltrer discrètement puis fournir des renseignements à la centrale installée dans le quartier de Iassenevo à Moscou.

- Richard et Cynthia Murphy, de leurs vrais noms Vladimir et Lydia Gouriev. Arrivés dans les années 1990 aux États-Unis, ils étaient surveillés depuis 2001. Leur officier traitant (OT) était un troisième secrétaire de la représentation de Russie auprès de l'ONU. Ils ont été arrêtés alors qu'ils tentaient de fuir les États-Unis.
- Donald Howard Heathfield et Tracey Lee Ann Foley prétendaient être d'origine canadienne et avoir obtenu la nationalité américaine. La véritable identité de ces Russes était Andreï Bezroukov et Elena Vavilova. Ils étaient sous surveillance du FBI depuis janvier 2001. Le couple communiquait directement avec Moscou par radio. Heathfield a tenté de pénétrer des organismes de veille géopolitique privés en proposant des logiciels trafiqués.

> *« Aujourd'hui, les services de renseignement russes sont extrêmement actifs, avec pour objectifs désignés l'OTAN, le terrorisme d'origine islamique et le crime organisé. »*

- Michael Zottoli et Patricia Mills. Zottoli, qui se prétendait américain, s'appelait Mikhaïl Kutzik et Mills, qui se disait canadienne, avait pour identité Natalia Pereverzeva. Le FBI a eu l'attention attirée sur ce couple en 2004, lorsqu'il est entré en contact avec Richard Murphy, qui était déjà sous surveillance. Il s'est avéré que le couple communiquait avec Moscou par voie électronique.
- Juan Lazaro et Vicky Pelaez. Lazaro affirmait être né en Uruguay mais a reconnu être russe, sans jamais toutefois dévoiler son identité réelle. Son épouse Vicky était d'origine péruvienne. Ils avaient tous deux obtenu la nationalité américaine. Le couple a été repéré dans un pays sud-américain en 2000, alors qu'il était en contact avec des « diplomates » russes. Il communiquait avec Moscou par moyens électroniques.
- Anna Chapman est devenue britannique en épousant Alex Chapman en 2002, dont elle a divorcé en 2006. Elle a attiré l'attention du FBI en juin 2010 à Manhattan alors qu'elle rencontrait un OT russe en poste auprès des Nations Unies. Elle est tombée dans un piège du FBI.
- Mikhail Semenko. Identifié en juin 2010 comme membre du SVR, il a accepté le paiement clandestin de 5000 dollars d'un agent du FBI se faisant passer pour un diplomate russe en poste au sein de la mission des Nations Unies. Il ne se méfiait pas car il avait déjà été traité par un « deuxième secrétaire » de cette même structure diplomatique.
- L'agent passé entre les mailles du filet : Christopher Robert Metsos. Cet individu installé outre-Atlantique depuis plus de dix ans jouait un rôle important dans le réseau du SVR implanté aux États-Unis. Il était en contact avec un deuxième secrétaire de la représentation de Russie à New York. Metsos a attiré l'attention du FBI en 2001. Vraisemblablement d'origine russe (son identité réelle n'est pas connue), il utilisait la

nationalité canadienne. Il a été en contact direct avec Richard et Cynthia Murphy, Michael Zottoli et Patricia Mills. Peut-être a-t-il rencontré les autres membres du réseau en qualité de « pourvoyeur de fonds ». Il a quitté les États-Unis en juin 2010 et a été appréhendé à l'aéroport international de Larnaca à Chypre le 29 juin, alors qu'il était en partance pour Budapest. Laissé en liberté sous contrôle judiciaire, il a filé.

• Le « douzième clandestin » : Alexey Karetnikov. Le cas de ce dernier, extradé le 13 juillet 2010 vers la Russie, est peu connu. Ce jeune mathématicien de 23 ans arrivé aux États-Unis en octobre 2009 a travaillé pendant neuf mois comme testeur de logiciels chez Microsoft.

> *« Les 13 000 fonctionnaires du SVR sont responsables du recueil à l'étranger et par moyens illégaux de tout renseignement pouvant intéresser le Kremlin dans les domaines politique et économique. »*

Certains de ces agents de renseignement sont entrés aux États-Unis dans les années 1990 alors que d'autres n'y sont arrivés qu'en 2009. Si tous n'utilisaient pas une identité fictive, ils bénéficiaient d'une légende et le SVR leur fournissait des comptes approvisionnés pour assurer leur subsistance. Une conversation interceptée entre Lazaro et Pelaez a démontré que leur direction n'était pas satisfaite de la qualité des fournitures reçues. Lazaro a conseillé à Pelaez de « tomber n'importe quel politicien » pour ensuite lui attribuer l'origine des « renseignements » collectés. Richard Murphy s'est par ailleurs attiré la remarque suivante de Metsos, qui lui remettait 40 000 dollars en liquide et une carte de crédit : « heureusement que je ne suis pas ton officier traitant... ».

Le SVR semblait savoir que les légendes adoptées par les membres du réseau étaient trop faibles pour résister à des enquêtes approfondies. Il leur a donc été demandé de ne pas tenter de faire une carrière qui aurait nécessité des accréditations particulières, mais plutôt de nouer des relations « amicales » avec de hauts responsables politiques pour pouvoir décrypter l'ambiance de la politique américaine.

En matière de transmissions, le réseau utilisait Internet pour y créer des boîtes aux lettres mortes qui permettaient à Moscou d'y récupérer les différents rapports. Chapman et Semenko utilisaient des radios à ondes courtes.

À l'origine de la découverte de ce réseau se trouve un agent russe passé à l'ennemi : Sergueï Tretiakov, OT du SVR surnommé le « camarade Jean ». Il était attaché à la mission de Russie auprès des Nations Unies. Il a commencé à passer secrètement des renseignements au FBI à partir de 1997. Il a fait officiellement défection en 2000. C'est à ce moment-là que la surveillance des suspects a débuté. Par un curieux hasard, il est décédé à son domicile aux États-Unis, le 13 juin 2010.

Le cas Buryakov

Le 25 mai 2016, le Russe Evgeni Bouriakov a été condamné à trente mois de prison par le tribunal du district sud de New York. Il est arrivé avec sa femme et ses deux enfants aux États-Unis en 2012 pour travailler au sein du bureau new-yorkais de la banque russe Vnesheconombank. Employé modèle du lundi au vendredi, il se livrait à des activités d'espionnage durant son temps libre. Il avait comme contacts deux OT agissant sous statut diplomatique. Bouriakov aurait été mis sous surveillance par le FBI au printemps 2014. Deux agents agissant sous couverture prirent contact avec lui sous le prétexte d'un projet d'implantation de casino en Russie. Lors de ces rencontres, ils lui remirent des documents provenant prétendument d'une agence gouvernementale américaine et censés contenir des informations sur les sanctions américaines à l'égard de la Russie. Bien sûr, l'occasion était trop belle pour Bouriakov d'obtenir des renseignements exclusifs et il est tombé dans le panneau. Cette opération a permis au FBI de remonter le réseau russe.

Photo ci-dessus :
Le 22 décembre 2010, l'ancienne espionne russe Anna Chapman s'apprête à prononcer un discours devant un groupe de jeunes pro-Kremlin. Véritable symbole de l'espionnage russe et égérie de la jeunesse poutinienne, Anna Chapman, fille d'un cadre du KGB, fut arrêtée aux États-Unis et échangée, avec neuf autres personnes soupçonnées d'intelligence avec la Russie, contre quatre Russes accusés d'espionnage pour les États-Unis et le Royaume-Uni. Devenue la coqueluche de la presse nationale russe, Vladimir Poutine l'a reçue personnellement au Kremlin et lui a prédit un « brillant avenir ». (© AFP/ Alexander Nemenov)

Frederico Carvalhão Gil

Le 21 mai 2016, Frederico Carvalhão Gil, un membre des services intérieurs portugais (SIS) est appréhendé dans un bar de Rome alors qu'il échangeait une enveloppe de documents classifiés contre de l'argent liquide avec un OT clandestin du SVR. Les deux hommes, arrivés à Rome la veille, avaient été suivis par des membres de la Division d'investigation générale et des opérations spéciales italienne, assistés de collègues portugais. Cette arrestation a été permise par une enquête de deux ans, entamée lorsque Lisbonne avait commencé à penser qu'il y avait une taupe au sein de ses services. Carvalhão Gil les avait intégrés dans les années 1980 au sein du contre-espionnage. Il parlait couramment le français, l'anglais et le russe. Son compte Facebook révélait son attrait personnel pour les pays d'Europe de l'Est. Plusieurs liaisons amoureuses avec des ressortissantes de ces pays furent découvertes. Enfin, il avait connu un divorce houleux qui semblait l'avoir déstabilisé psychologiquement et financièrement. Une surveillance rapprochée fut décidée à

Photo ci-dessus :
Barack Obama rencontre le président russe dans sa datcha près de Moscou, en juillet 2009. Le 29 décembre 2016, le président américain annonçait une série de mesures contre la Russie, accusée d'ingérence dans l'élection présidentielle américaine, en déclarant *persona non grata* 35 membres des services de renseignement russes. Il promettait également une série d'autres mesures via des opérations « qui ne [seraient] pas révélées au public ». (© White House/ Pete Souza)

Photo ci-contre :
Alexandre Bortnikov, entré au KGB en 1975, dirige le FSB depuis mai 2008. En 2015, il a participé au sommet sur la lutte contre l'extrémisme organisé à Washington et a déclaré à la presse russe que, alors que 1700 Russes combattraient dans les rangs de l'État islamique, il était « important de comprendre le besoin de travailler ensemble en dépit des problèmes politiques » et que l'échange de renseignement entre la Russie et les États-Unis sur cette question-là était « tout à fait possible ». (© Kremlin.ru)

l'automne 2015. Elle permit de constater qu'il se rendait souvent dans des capitales européennes. C'est à l'occasion de son voyage à Rome qu'il fut décidé de mettre un terme à ses activités d'agent de renseignement. Le SVR rémunérait 10 000 euros ses productions. Pour un service de renseignement, recruter un agent au sein d'un homologue étranger est toujours considéré comme un bon point, même si ce service n'est pas très important.

Le FSB, l'outil des basses œuvres du Kremlin

En dehors de ses missions de contre-espionnage, de contre-terrorisme et de protection du régime, le FSB, créé en 1995 et qui emploie de 200 000 à 300 000 personnes, a également sous sa responsabilité les interceptions des communications depuis qu'il a récupéré le FAPSI, l'Agence fédérale des communications gouvernementales et de l'information, dissous en 2003. Contrairement à la légende, le FSB n'est pas un « État dans l'État », mais une administration dévouée au Kremlin. Seuls quelques officiers dépassent parfois leurs prérogatives pour des intérêts personnels.

Depuis la fin 2016, le FSB est confronté à un certain nombre de problèmes. En effet, les médias font le rapprochement avec les accusations portées par l'administration américaine sortante concernant des intrusions survenues lors de la campagne présidentielle de 2016.

C'est notamment le cas avec la mort étrange d'Oleg Erovinkin. Selon la presse russe, le corps sans vie de ce dernier, âgé de 61 ans, a été retrouvé à Moscou le 26 décembre 2016, à l'arrière d'une voiture de la société Rosneft, par son chauffeur. Cet ancien général a servi au sein du KGB, puis du FSB, avant d'être désigné en mai 2008 comme chef de cabinet au sein de la société d'État russe Rosneft. Le dirigeant de Rosneft est Igor Setchine, ancien Premier ministre adjoint et proche conseiller du président Vladimir Poutine. Les autorités affirment qu'Erovinkin est mort d'une crise cardiaque. Mais il aurait été la principale source russe de Christopher Steele, l'ancien officier du MI6 qui a rédigé un rapport controversé sur Donald Trump daté du 19 juillet 2016...

Une purge au sein du FSB

Début décembre 2016, le colonel Serguei Mikhailov est arrêté lors d'une réunion à la Loubianka (siège du FSB). Il est menotté, la tête recouverte d'un sac et emmené à la prison de Lefortovo. Son subordonné, le commandant Dmitri Dokouchaïev, subit le même sort peu de temps après. Les deux officiers appartiennent au Centre de la sécurité des informations du FSB (FSB-CSI, dit unité n° 64829) chargé de la lutte contre la cybercriminalité au sein du deuxième Directorat du contre-espionnage. Des autorités russes les accusent de trahison. Presque simultanément, Rouslan Stoïanov, le responsable du département des enquêtes de la société de sécurité informatique Kaspersky Lab, est appréhendé. Stoïanov y avait été embauché en 2012 après avoir servi au sein du bureau de la police chargé de lutter contre la cybercriminalité. Toutes les personnes inculpées dans cette affaire sont soupçonnées d'avoir espionné dans le passé de hautes personnalités russes dont Dmitri Medvedev. Elles auraient utilisé un groupe de hackers appelé « Shaltai-Boltai » ou « Anonymous International ».

> *« En dehors de ses missions de contre-espionnage, de contre-terrorisme et de protection du régime, le FSB, créé en 1995 et qui emploie de 200 000 à 300 000 personnes, a également sous sa responsabilité les interceptions des communications. »*

Plus précisément, le colonel Serguei Mikhailov aurait été l'OT chargé au sein du FSB-CSI de la pénétration de Shaltai-Boltai. Les deux OT auraient été placés sous surveillance depuis septembre 2016, quand le FBI a accusé la société King Servers

d'avoir hébergé des hackers qui ont mené des cyberattaques contre les systèmes électoraux aux États-Unis. Le président Barack Obama avait nommément désigné le FSB et le GRU comme responsables de ces attaques. Plus grave pour Moscou, Mikhailov serait soupçonné d'avoir fourni des informations à la CIA, ce qui expliquerait les « certitudes » de la centrale américaine sur les attaques informatiques russes. C'est sur cette base, mais aussi en raison du harcèlement que subiraient des personnels des représentations diplomatiques américaines en Russie, que 35 diplomates russes et leurs familles ont été expulsés des États-Unis fin décembre 2016. S'il s'avère que Mikhailov a été recruté par la CIA, il est aussi possible qu'il l'ait abreuvée en informations croustillantes, non vérifiées, mais généralement très rémunératrices... Ce ne serait pas la première fois que la CIA se serait auto-intoxiquée en demandant à une source de « haut niveau » des renseignements qu'elle souhaitait entendre.

> *« Actifs dans de nombreux domaines, les services russes, comme toute organisation humaine, ne sont pas infaillibles et peuvent être combattus avec efficacité. »*

L'Estonie pénétrée par le FSB

En décembre 2014, l'Estonien Uno Puusepp raconte dans une interview diffusée à la télévision russe NTV son passé d'espion à la solde du FSB. Dans les années 1970, il intègre le SSR-KGB estonien. Il est spécialisé dans le domaine des écoutes. En août 1991, alors que les pays baltes accèdent à l'indépendance, le SSR-KGB disparaît littéralement en une nuit, emportant avec lui les archives les plus sensibles. Or les nouvelles autorités ne peuvent se passer de services secrets, mais c'est un métier qui ne tolère pas l'improvisation. De nombreux jeunes diplômés sont recrutés mais quelques anciens viennent apporter leurs savoir-faire. Uno Puusepp est l'un de ceux-là. Il rejoint le Kaitsepolitseiamet (KaPo) pour poursuivre ce qu'il sait faire : les écoutes. Les enquêtes de sécurité ne trouvent rien puisque les Russes ont mis Puusepp en sommeil. Quand il travaillait pour le SSR-KGB, il avait rencontré le chef de poste clandestin du KGB à Tallin, Nikolaï Ermakov, qui tenait une boulangerie. En 1996, Puusepp est « réveillé » par Ermakov. Sa motivation est purement idéologique car il ne supporte pas la politique pro-occidentale de l'Estonie qui a intégré l'OTAN et l'Union européenne en 2004. Puis Puusepp prend sa retraite en 2011 et rejoint tranquillement la Russie. Plus personne n'entend parler de lui jusqu'à une retentissante émission de télévision. Bien qu'il ait soutenu n'avoir pas nui aux intérêts de son pays, il semble qu'il ait livré des renseignements intéressants aux Russes. De l'aveu de son traitant, « dans les années au cours desquelles Uno a travaillé pour nous, les activités de renseignement estoniennes contre la Russie ont été réduites de 80 % ». Pendant près de 15 ans, pratiquement tout ce qui atterrissait sur le bureau du directeur du Service de sécurité intérieur estonien arrivait en même temps sur ceux du FSB ! Le fait d'avoir volontairement dévoilé l'existence de la taupe au sein des services intérieurs estoniens était destiné à déconsidérer les services des pays baltes en démontrant qu'il n'est pas « sûr » de collaborer avec eux.

L'Estonie avait déjà connu un autre scandale d'espionnage de grande ampleur avec l'arrestation de Herman Simm, conseiller du ministre de la Défense arrêté en 2008 et condamné à douze ans et demi de prison. Il avait espionné pour le compte du SVR durant douze années.

Le GRU à la pointe de la guerre contre le terrorisme

Si le FSB est à la pointe du combat dans le domaine de l'antiterrorisme à l'intérieur de la Fédération de Russie, le GRU y joue aussi un rôle de première importance avec ses 12 000 personnels renforcés d'un nombre indéterminé de forces spéciales (*Spetsnaz*). Tout le monde se rappelle les « petits hommes verts » qui ont conquis la Crimée en 2014 ou les batailles d'Alep et de Palmyre de 2016-2017 qui ont vu s'activer les Spetsnaz. Toutes les missions militaires implantées dans les ambassades dépendent totalement du GRU et se livrent à de l'espionnage militaro-industriel. Enfin, il est aussi chargé des interceptions des transmissions électromagnétiques (SIGINT).

Actifs dans de nombreux domaines, les services russes, comme toute organisation humaine, ne sont pas infaillibles et peuvent être combattus avec efficacité. Si l'on se réfère au passé, dans les années 1950-1980, le KGB savait à peu près tout sur le monde occidental mais une grande partie des renseignements recueillis ont fini au fond des tiroirs. Les dirigeants politiques qui devaient les utiliser ne leur ont pas accordé l'importance qu'ils avaient car ils voyaient la situation à travers leur prisme idéologique. C'est souvent là le maillon faible du renseignement et cela ne concerne pas que Moscou !

Alain Rodier

Note

(1) Étant donné ses spécificités, le FSO ne sera pas traité dans cet article.

Photo ci-dessus :
Le 28 novembre 2016, le journaliste Roman Sushchenko attend dans la prison du tribunal de Moscou après avoir été arrêté par le FSB et accusé d'être un responsable du renseignement ukrainien cherchant à s'emparer d'informations secrètes sur l'organisation de la défense et de la sécurité russes. Si les services ukrainiens (SBU) ont démenti cette accusation, ils ont annoncé, quelques jours après, avoir pris en flagrant délit un Ukrainien accusé de travailler pour le GRU. Son identité aurait été révélée après avoir offert la citoyenneté russe à un haut responsable militaire ukrainien en échange de documents confidentiels. (© AFP/Vasily Maximov)

analyse

Par **Gérald Arboit***, directeur de recherche au Centre français de recherche sur le renseignement (CF2R).

Les services de renseignement britanniques en pleine mutation

L'année 2014 fut celle de la transition pour les services de renseignement britanniques, après une série d'échecs (attentats) et de révélations (Snowden). Mais elle a également marqué le début d'une adaptation à de nouveaux modes de surveillance administrative.

Photo ci-dessus :
Siège du MI6 à Londres, sur les bords de la Tamise. Les services secrets extérieurs britanniques furent le service le mieux loti dans le cadre du « plan de défense stratégique et de sécurité » annoncé en novembre 2015. D'ici à 2020, il devrait en effet voir ses effectifs passer de 2500 à 3500, soit la plus forte hausse depuis la fin de la guerre froide. (© Garry Knight)

S'il est une nation qui a bien intégré un esprit propice au renseignement, il s'agit à coup sûr du Royaume-Uni. La légende veut que ses services soient nés à la fin de l'ère élisabéthaine (1558-1603). Malgré les révélations par le scandale ou le roman, dès les années 1960, le renseignement britannique resta dans l'ombre la plus totale en raison de l'impératif de sécurité nationale jusqu'en 1994. Ce ne fut qu'à partir de cette époque que la communauté britannique du renseignement (IC), réellement mise en place au début du XX^{e} siècle, se révéla autour de quatre pôles :

- le *Security Service* (MI5), rattaché administrativement au *Home Office*, est chargé du renseignement intérieur ;
- le *Secret Intelligence Service* (SIS ou MI6), responsable du renseignement extérieur, et le *Government Communications Headquarters* (GCHQ), chargé des interceptions de communication, dépendant hiérarchiquement du *Foreign Office* ;
- enfin, le *Defence Intelligence* (DI), s'occupant du renseignement au bénéfice des armées, est la seule entité à n'être qu'un organe du *Ministry of Defence*.

Si le DI a toujours existé, MI5 et MI6 résultent de la prise de conscience par les autorités britanniques de la menace allemande en 1909. Le GCHQ est apparu quant à lui dix ans plus tard, résultat combiné des avancées technologiques induites par la Première Guerre mondiale et de la nécessité de communiquer avec l'ensemble de l'Empire colonial britannique. Dès 1936, ces services ont vu leurs missions orientées par le *Joint Intelligence Committee* (JIC), véritable interface entre l'IC et les décideurs politiques et militaires, qui sont ses « clients ». En

L'évolution du budget des services britanniques de renseignement (2010-2021)

En millions de livres sterling (£)

2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	*2016-2017*	*2017-2018*	*2018-2019*	*2019-2020*	*2020-2021*
1960	1968	2113	2123	2228	2469	2412	2366	2500	2623	2300

Sources : Cabinet Office, *Security and Intelligence Agencies: Financial Statement* 2015-16, p. 16 et 2013-14, p. 16 ; articles de la presse britannique.

outre, depuis l'*Intelligence Service Act* (1994), qui a levé le secret de polichinelle entourant l'existence de cette IC, une commission parlementaire examine les dépenses, l'administration et la stratégie de ces services.

Une nécessaire rénovation

La fin de l'année 2014 semble ouvrir une nouvelle page pour ces institutions, avec l'arrivée d'Alex Younger à la tête du MI6, et celle de Robert Hannigan, à la tête du GCHQ. Ils remplaçaient respectivement Sir John Sawers et Sir Iain Lobban, dont la probité avait été salie par les révélations de Julian Assange et d'Edward Snowden. Toutefois, il s'agissait moins d'une sanction que de la volonté du gouvernement britannique de restaurer son renseignement après cinq années difficiles. Les révélations de sa politisation dans l'affaire irakienne de 2003, au sujet des prétendues armes de destruction massive de Saddam Hussein, avaient fortement ébranlé la réputation de l'IC. Deux ans plus tard, sa myopie devant la démonstration de la radicalisation de la communauté musulmane britannique éclatait au grand jour avec les attentats londoniens du 7 juillet 2005 et la tentative du 21 juillet suivant (1) et elle fut constatée de nouveau lors de l'assassinat du tambour Lee Rigby, du 2nd Battalion, Royal Regiment of Fusiliers, le 22 mai 2013.

> *« Afin d'offrir aux MI5 et MI6 les moyens de s'attaquer à l'islamisme radical, le gouvernement de David Cameron a débloqué une rallonge de 344 millions de livres sterling. »*

À chaque fois, les manquements du *Security Service* (MI5) ont été pointés par les médias. Mais les commissions d'enquête parlementaires rendirent toujours grâce à l'action du renseignement intérieur, estimant que si la menace était patente, les cibles n'étaient pas prévisibles. Un peu à l'image de Mohammed Merah (2012) en France, l'assassin de Rigby était sous surveillance du MI5, mais il n'était qu'un « sujet à faible niveau d'intérêt (*low level subject of interest*) ». Autrement dit, que l'assassin eût été arrêté ou pas, l'attentat aurait de toute façon eu lieu (2).

D'ailleurs, la population britannique n'en tint pas rigueur à son IC, ainsi que le démontra un sondage de janvier 2015, pointant une popularité de 64 % des personnes interrogées pour le MI6 et de 72 % pour le MI5. Nul doute que le saut en parachute de James Bond, en compagnie de la reine Elizabeth, sur le stade olympique, le 27 juillet 2012, avait fini de convaincre les Britanniques des capacités de leurs services de renseignement. Plus sérieusement, afin d'offrir aux MI5 et MI6 les moyens de s'attaquer à l'islamisme radical, le gouvernement de David Cameron a débloqué une rallonge de 344 millions de livres sterling pour les deux dernières années du *Single Intelligence Account* 2013-2016 (3). Au lendemain des attaques contre Paris du 13 novembre 2015, rappelant que l'IC avait déjoué sept tentatives d'attentat en Grande-Bretagne, Cameron décida même d'augmenter de 15 % les effectifs du MI5, du MI6 et du GCHQ d'ici à 2020. À terme, les 2479 officiers du MI6 devraient se voir augmenter de 1000 hommes, tandis que le MI5, fort de 4037 agents, et le GCHQ, avec ses 5564 fonctionnaires, se partageraient les 900 hommes restants ; les 3697 militaires du DI ne devraient pas être concernés (4). Cette décision faisait écho à la démarche du gouvernement français.

Un budget sous contrainte

En fait, bien que considéré comme une priorité nationale, le budget des services de renseignement avait été, sinon revu à la baisse, du moins gelé après la crise de 2008. Le Royaume-Uni innova en 2010 en instituant le *Single Intelligence Account*, un organe de financement commun de l'IC. Ce compte unique du renseignement britannique a été adopté comme « un moyen d'amener la Grande-Bretagne du sauvetage à la reprise » (5). Depuis le 7 septembre 2005, sous la direction du conseiller en sécurité nationale auprès du Premier ministre, le diplomate Sir Mark Justin Lyall-Grant, il permet de financer les trois

Photo ci-dessous :
Le 3 août 2016, des forces de police prennent part à un exercice de lutte antiterroriste sur la Tamise. Alors que le terrorisme constitue l'un des trois risques prioritaires – avec la prolifération et la cybersécurité – contre lesquels luttent les services du renseignement extérieur britanniques (MI6), le directeur de ce service, Alex Younger, révélait en décembre dernier, lors de l'arrestation de six individus soupçonnés de projeter un attentat, que ses services avaient contribué à déjouer 12 attentats depuis juin 2013. (© AFP/ Stefan Rousseau)

agences en fonction des priorités fixées par la *National Security Strategy* et la *Strategic Defence and Security Review*. Il s'agit aussi de permettre aux trois services de fonctionner plus efficacement et d'encourager leur collaboration (6). Derrière la dialectique, il apparaît toutefois que ces synergies sont recherchées avant tout pour des raisons d'économie, et non d'efficience.
Les coûts de fonctionnement des trois services sont ainsi maintenus à 1 %, les dépenses d'investissement à 1 %, tandis que les opérations absorbent 64 % du budget et les salaires des officiers de renseignement représentent 35 %. S'il est impossible de connaître la répartition de budgets entre les différents membres de l'IC, il est notable que le MI6 et le GCHQ mobilisent 24 % de leurs ressources – humaines et financières – pour des missions « corporate », incompressibles et différentes selon les services. Elles comprennent la sécurité des installations, les services administratifs (sécurité, juridique, finances, ressources humaines, audit, communication), le service extérieur y faisant également figurer l'entretien des biens immobiliers et le fonctionnement de bureaux privés, tandis que le service de renseignements électroniques y porte la gestion de ses moyens informatiques. Pour le MI6, s'ajoutent encore ses services informatiques (12 %), et pour le GCHQ, son maintien capacitaire (26 %) et son ingénierie (18 %). Ainsi, respectivement 36 % et 68 % du budget de fonctionnement de chacun de ces deux membres de l'IC concernent des missions administratives. Le MI5 semblerait n'avoir que la sécurité de ses installations (5 %) comme dépense ne concernant pas sa mission de renseignement proprement dite (7).

Photo ci-dessus :
Le « donut », siège du Government Communications Headquarters (GCHQ), où travaillent quelque 6000 employés du service de renseignement électronique du Royaume-Uni, placé sous la responsabilité du ministre des Affaires étrangères, et dont le rôle est de fournir des informations au gouvernement et aux forces armées britanniques. (© GCHQ)

Anciennes et nouvelles menaces

Cybermenaces

Depuis 2010, la cybersécurité est devenue une priorité pour le MI6 et le GCHQ (8). Edward Snowden a mis au jour l'existence du programme de surveillance électronique Tempora, qui permet depuis 2008 à l'agence britannique d'intercepter les données transitant par les câbles en fibre optique entre l'Europe et les États-Unis (9). Mais le GCHQ dispose également des moyens d'interception électromagnétiques lui permettant de prélever des données « non sélectionnées » (brutes), sans autorisation légale, s'il n'a pas été « techniquement faisable » de les récupérer en vertu d'un mandat et s'il est « nécessaire et proportionné » pour l'IC d'avoir ces informations (10). Autrement dit, il peut « chaluter » et garder sans restrictions significatives ces données numériques, qui comprennent à la fois le contenu des communications et les métadonnées.
Alors que le GCHQ assure une double mission de cyberdéfense et de cyberattaque, essentiellement au bénéfice de la sécurité économique, tout en luttant contre la prolifération et la grande criminalité (y consacrant 18 % de ses ressources (11)), le MI6 utilise les données de la cybersécurité au service de la lutte contre le terrorisme. Pour cela, le GCHQ mobilise spécifiquement les ressources du Joint Threat Research Intelligence Group (JTRIG), qui unit ses personnels à ceux de sa consœur américaine, la National Security Agency (NSA). Depuis juillet 2013, même s'il n'a pas subi d'attaque, le Royaume-Uni a échappé à douze attentats (12).

Terrorisme

Naturellement, même si l'antiterrorisme est une activité mutualisée, tous les services de l'IC n'y jouent pas le même rôle. Le MI5 y consacre ainsi une grande part de son activité (64 %), tandis que le MI6 et le GCHQ remplissent cette mission parallèlement à d'autres. Pour ce dernier, elle est incluse dans ses missions liées au renseignement économique, à la contre-prolifération, au contre-espionnage et à la cybersécurité (le tout représentant 24 % de son activité). Pour le MI5, elles font partie de ses activités de contre-prolifération et contre-espionnage (pour 13 %), distinctes de ses activités en lien avec la « vieille plaie » de l'Irlande du Nord, qui compte encore pour 18 % (13).

> *« Depuis 2010, la cybersécurité est devenue une priorité pour le MI6 et le GCHQ. »*

Montée en puissance de la Russie et de la Chine

Plus généralement, l'IC doit s'adapter à la mutation des relations internationales mise en pleine lumière par la crise ukrainienne (2014). Aux révélations concernant la dépendance accrue de certaines économies européennes à la Russie à la suite des sanctions prises par l'Union européenne, s'étaient déjà ajoutés des relents de guerre froide depuis la crise géorgienne (2008), s'accompagnant d'une recrudescence de l'espionnage mené par la Russie. Cette menace s'est amplifiée avec l'intervention russe en Syrie en septembre 2015 (14). À tel point qu'un groupe d'experts du renseignement, dont l'ancien chef du MI6 Sir Richard Dearlove (1999-2004), a démissionné du *Cambridge Intelligence Seminar* – un forum universitaire pour anciens praticiens occidentaux et chercheurs actuels sur le renseignement –, auquel ils participaient, en raison de craintes qu'ils puissent faire l'objet d'une opération soutenue par le Kremlin pour compromettre le groupe (15). Un nouvel acteur, pour des raisons essentiellement économiques cette fois, la Chine, s'avère également une menace grandissante.

Tensions avec les pays européens

Dans le même temps, depuis les révélations de Snowden, les services allemands et italiens sont moins désireux de travailler avec le MI6 ; c'est peu dire que l'Allemagne a peu apprécié que le GCHQ et la NSA ciblent ses entreprises de télécommunications (16) ! Depuis mars 2014, MI5 et MI6 peuvent néanmoins compter sur le service qatari. En effet, pour les Britanniques, une des solutions au terrorisme se trouve en Syrie et en Irak, des zones où les services du Qatar sont mieux introduits que les services occidentaux. Cela étant, la recrudescence du risque terroriste islamique en Europe, notamment en France et en Belgique, depuis janvier 2015, a ramené la concorde entre les différents membres de la « communauté européenne » du renseignement. Et ce n'est pas le *Brexit* qui changera quoi que ce soit ! En effet, les échanges de renseignements dans les enceintes *ad hoc*, en place depuis 1972 tant pour les services extérieurs qu'intérieurs, sont la meilleure chance de succès contre cet ennemi mouvant qu'est le terrorisme.

Les difficultés actuelles

Augmentation du travail de cyberinvestigation

Finalement, les révélations de Snowden n'eurent qu'une portée somme toute limitée. Déjà, en décembre 2014, l'*Investigatory Powers Tribunal*, instance judiciaire indépendante ayant compétence pour examiner les plaintes concernant l'utilisation de la surveillance par un organisme doté de pouvoirs (donc des services de renseignement et de sécurité), en vertu du *Regulation of Investigatory Powers Act 2000*, a jugé légales, en principe, les interceptions du GCHQ. Depuis 2009, ces dernières ont augmenté de 7000 % (17). Depuis, le service de renseignement électromagnétique a vu ses missions s'accroître, entraînant une augmentation des délais de réponse. Avant 2013, elle était de quinze jours ; aujourd'hui, il faut compter au moins six semaines (18). Et cette tendance n'est pas destinée à se réduire, à budgets constants, avec le vote de la nouvelle *Investigatory Powers Bill*, en mars 2016, qui permet aux forces de police de hacker les appareils électroniques pour enquêter ou prévenir les « crimes graves » (19).

Nécessité de trouver des financements

Pour réduire ces délais, comme sa consœur américaine, le GCHQ parraine des recherches susceptibles de contribuer à sa mission. Un exemple parmi d'autres : l'Université de Lancaster propose une thèse (2014-2017) en analyse comportementale cherchant les moyens d'identifier des employés malhonnêtes (20). Sans relation avec d'éventuelles défections d'employés au sein de l'IC – comme dans les années 1960 notamment –, cette recherche semble destinée à cibler les candidats au djihad tapis au sein de la société multiculturelle britannique. En raison de l'évolution des technologies de cryptage, induite autant par les révélations de Snowden que par le refus des grands groupes de communication américains de continuer leur collaboration avec la NSA ou encore les mesures prises par tous ceux qui ont quelque chose à se reprocher, le GCHQ est, enfin, obligé de recourir aux ressources des entreprises privées.

Si l'affaire Snowden reste dans les esprits des Britanniques, la perception de la menace terroriste en a effacé les traces. Pour l'IC, cela signifie que ses méthodes sont admises par la société britannique. Cette légitimité retrouvée lui est d'autant plus nécessaire que les conditions de la transparence administrative placent les services sous la surveillance du Parlement et de la justice britannique. À ce prix, la démocratie est défendue par l'IC.

Gérald Arboit

*Cet article est une version remaniée et actualisée du Focus paru dans *Les Grands Dossiers de Diplomatie* n° 25, « Géopolitique du Royaume-Uni », p. 90-91.)

Notes

(1) Christopher Andrew, *The Defense of the Realm: the Authorized History of MI5*, Londres, Penguin Books, 2010, p. 857-858.

(2) Patrick Wintour, Ewen MacAskill, Vikram Dodd, « Lee Rigby: internet firms providing safe haven for terrorists, says PM », *The Guardian*, 25 novembre 2014.

(3) Voir : Cabinet Office, Security and Intelligence Agencies, *Financial Statement 2015-16 (For the year ended 31 March 2016)*, 14 juillet 2016.

(4) *Intelligence and Security Committee of Parliament - Annual Report 2015-2016.*

(5) HM Treasury, *Spending Round 2013*, juin 2013, p. 5.

(6) *Ibid.*, p. 54.

(7) Intelligence and Security Committee of Parliament, *op. cit.*

(8) David Cameron, *Securing Britain in an Age of Uncertainty: the Strategic Defence and Security Review*, octobre 2010, p. 10 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf) [consulté le 19 février 2017].

(9) Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davis et James Ball, « GCHQ taps fibre-optic cables for secret access to world's communications », *The Guardian*, 21 juin 2013.

(10) James Ball, « GCHQ views data without a warrant, government admits », The Guardian, 29 octobre 2014.

(11) Intelligence and Security Committee of Parliament, *op. cit.*

(12) Richard Wheatstone, « MI5 chief says intelligence service has disrupted 12 terror attacks in UK since June 2013 », *Daily Mirror*, 31 octobre 2016.

(13) Intelligence and Security Committee of Parliament, *op. cit.*

(14) Guy Faulconbridge, « British spy chief says Islamic State plotting attacks as Russia makes "desert" of Syria », Reuters, 8 décembre 2016.

(15) Sam Jones, « Intelligence experts accuse Cambridge forum of Kremlin links », *Financial Times*, 13 décembre 2016.

(16) Laura Poitras, Marcel Rosenbach, Holger Stark, « NSA: A wie Angela », *Der Spiegel*, n° 14, 31 mars 2014.

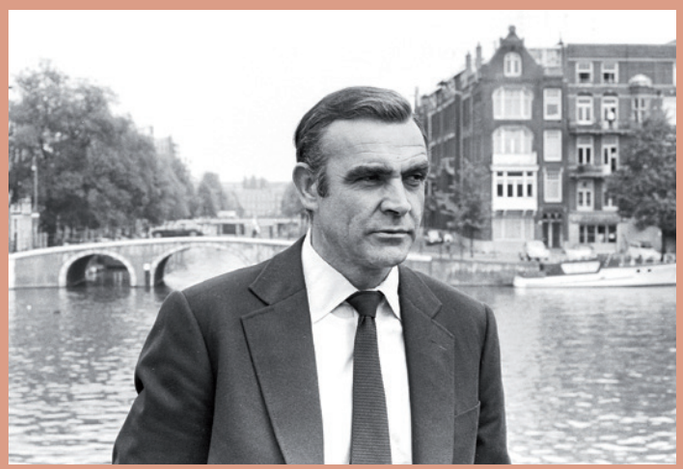
(17) Sooraj Shah, « GCHQ's Tempora programme deemed legal by Investigatory Powers Tribunal », *Computing News*, 5 décembre 2014.

(18) Charles Moore et Tom Whitehead, « Edward Snowden leaks mean GCHQ takes three times as long to track terrorists », Daily Telegraph, 11 octobre 2014.

(19) Tom Whitehead, « Snoopers' charter: Police have been able to hack into phones and computers for routine investigations for years », *Daily Telegraph*, 1er mars 2016.

(20) Jack Crone, « GCHQ to snoop through office emails: anti-spy agency will monitor disgruntled employees in danger of threatening UK security by going rogue », *The Mail on Sunday, 7 décembre 2014.*

James Bond, vices et vertus d'un mythe



Lors d'un entretien en janvier 2017, l'actuel directeur du MI6, Alex Younger, appelait à « dépasser le mythe » de James Bond (dont l'interprète le plus connu reste Sean Connery, ici à Amsterdam en 1971, lors du tournage des *Diamants sont éternels*). Selon lui, le stéréotype qu'il a créé pèse sur le recrutement de ses services. En revanche, il lui reconnaît « un bon côté » : « les adversaires pensent qu'il y a un officier du MI6 derrière chaque buisson et que nous sommes 10 000 fois plus importants qu'en réalité ». (© Dutch National Archives, The Hague, Fotocollectie Algemeen Nederlands Persbureau)

Photo ci-dessus :
Sir George Mansfield Smith-Cumming (1859-1923), premier directeur du Secret Intelligence Service (ou MI6). Au sein du Secret Service, il était connu sous son initiale « C », et ce titre désigne depuis lors le chef du MI6. C'était également la seule personne du Service à écrire en vert, autre tradition qui perdure. (DR)

Vers une *(r)évolution* du renseignement belge ?

La nécessaire *émergence* d'une *communauté* du renseignement

Par **Patrick Leroy**, commissaire divisionnaire honoraire, doctorant en science politique, Université de Liège (ULg) et collaborateur scientifique de l'unité de recherche ESU (European Studies Unit, ULg).

Une histoire

L'histoire du renseignement belge se confond avec la naissance de l'État, en 1830. La Sureté publique, appellation qui précède celle de Sureté de l'État, apparait dès l'annexion française de 1794 (Fouché et Vidocq), puis sous le régime hollandais (Guillaume Ier), avant d'être placée tout d'abord sous la tutelle du ministère de l'Intérieur, puis de la Justice (1832) (1). Ce qui fait de la Sureté de l'État aujourd'hui le seul service de renseignement en Europe à pouvoir prétendre à une existence ininterrompue de plus de 180 ans. Le renseignement militaire a plus de mal à naitre. Il faut attendre 1915 pour voir un service de sécurité militaire créé par un arrêté royal (1er avril 1915), bien que des missions de contre-ingérence, entre autres, aient été mises en œuvre par des administrations sans existence officielle, pendant une période dite « préhistorique » du renseignement militaire belge (1830 – 1910) (2).
Les deux services de renseignement belges – la Sureté de l'État (VSSE), qui dépend du Service public fédéral de la Justice et le Service général du renseignement et de la sécurité (SGRS), qui dépend du ministère de la Défense – ont ensuite connu dans l'histoire des évolutions structurelles internes, bien souvent à la suite d'événements marquants, comme la chute du mur de Berlin et du bloc de l'Est, et des attentats de 2001, 2004 et 2005.

Un événement

Par la loi du 18 juillet 1991 (3), le législateur crée un organe autonome de contrôle des services de renseignement qui dépend du Parlement et qui fait rapport à la commission du suivi du Comité R, à la Chambre [voir également p. 36 de ces Grands Dossiers, NdlR].
Parce que les services de renseignement évoluent dans la discrétion, dans le secret et parce qu'ils disposent de compétences spécifiques, la confrontation entre les missions des services et les normes constitutionnelles et légales nécessite de trouver un équilibre entre transparence (ou plutôt ouverture), efficacité, efficience et légitimité (4).
Si la Belgique doit attendre 161 ans pour se doter d'un contrôle parlementaire, elle patiente sept années de plus pour voir l'adoption d'une base légale pour les deux services de renseignement reconnus par la loi organique du 30 novembre 1998. L'intention du législateur est de combler les besoins présents et futurs de l'État en matière de renseignement (5), les travaux préparatoires révèlent cependant qu'il s'agissait avant tout de consolider un « *statu quo* » (6). La loi en effet n'offre pas de grandes innovations dans le monde du renseignement belge.
Elle est actualisée en 2010 et les deux services de renseignement se voient enfin attribuer les « méthodes particulières de renseignement » (MPR-BIM). Les services belges sont jusqu'alors trop tributaires de leurs homologues étrangers au regard de l'accroissement des risques et menaces. En outre, la collecte – secrète – de données est encadrée par une base légale explicite au regard de la Convention européenne des droits de l'homme (7).
Ces méthodes particulières de recueil de données sont réparties sur trois types de compétences – ordinaire, spécifique et exceptionnelle – groupées selon le degré potentiel de gravité de la violation des droits et des libertés du citoyen, par exemple : « le recours à des sources humaines » (art. 18) comme méthode ordinaire, « la pénétration et l'inspection de lieux accessibles au public à l'aide de moyens techniques » (art. 18/2 §1,2° et 18/5) comme méthode spécifique, et « la création de personnes morales et le recueil d'information sous couverture » (art. 18/2 §2, 3° et 18/13) comme méthode exceptionnelle. L'utilisation de ces MPR est soumise aux principes de proportionnalité et de subsidiarité. Les méthodes spécifiques et exceptionnelles sont assorties d'un contrôle dans leur exécution, selon les cas *a priori,* par un organe administratif (la commission BIM) composé de trois magistrats et *a posteriori,* par le Comité R, en tant qu'organe juridictionnel.
Le SGRS engrange aussi de nouvelles missions : la protection du potentiel économique, scientifique et industriel, la défense contre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministère de la Défense gère, avec une capacité de réaction immédiate, ce qui lui offre – c'est nouveau pour un service à vocation défensive – une mission offensive.

Une crise

Les attentats de Paris (2015) et de Bruxelles (2016) ont provoqué la mise sur pied d'une commission d'enquête parlementaire (dont un volet consacré au renseignement) qui doit sortir ses conclusions et propositions à la fin du mois d'avril de cette année 2017.
Déjà, une nouvelle adaptation de la loi organique de 1998 est sur le point d'être votée à l'heure où nous écrivons ces lignes (mars 2017). L'analyse du projet de loi montre un renforcement des compétences des services, notamment en légalisant de nouvelles méthodes particulières et en offrant une nouvelle capacité offensive au SGRS en matière d'influence. Sans attendre, les deux services de renseignement ont aussi entamé de nouvelles restructurations internes.
Au moment où nous écrivons ces lignes, nul ne connait les conclusions précises de la commission d'enquête parlementaire, mais la tentation est grande pour nos

Photo ci-contre : Au lendemain des attentats de Bruxelles de mars 2016, le Premier ministre belge, Charles Michel, a rappelé qu'il plaidait pour la création d'un « FBI ou [d']une CIA à l'européenne » qui permettrait la mise en place d'une plateforme systématique d'échange d'informations entre les services de renseignement européens. (© Andrej Klizan / EU2016 SK)

politiques de combler les « failles » du renseignement par des mesures radicales :

• **L'abandon de certains champs d'actions**, à des fins de rationalisation des ressources, reproduit l'erreur du passé. Certains services de renseignement avaient supprimé ou réduit drastiquement les départements de contre-espionnage, au lendemain de l'effondrement de l'URSS et du pacte de Varsovie, départements que les responsables de l'époque ont dû recréer de toutes pièces, l'espionnage n'ayant pas baissé d'intensité, au contraire.

• **Le « tout-sécuritaire »** ou l'abandon de l'ADN du renseignement, que sont l'aide à la décision et sa complémentarité avec les actions policières, par l'anticipation et la prospective. Si le « tout-sécuritaire » se justifie par l'accroissement des menaces et des risques, surtout en matière de terrorisme, le renseignement doit effectivement y jouer un rôle, sans perdre ses critères identificateurs (le secret ou la discrétion, la finalité, le temps, la prévention et la prospective). Soulignons la clairvoyance de Patrick Calvar et Bernard Bajolet, respectivement directeurs du renseignement intérieur et extérieur français, qui déclaraient il y a plus d'un an : « La réponse sécuritaire ne peut, à elle seule, régler le problème du terrorisme. » (8)

• **La fusion des services de renseignement en un bloc monolithique ou l'absorption par la police fédérale.** Les arguments généralement invoqués sont la rationalisation et la mutualisation des ressources, l'amélioration de l'échange des informations, et sans doute une facilité de contrôle des actions. Ici, la question de séparation des pouvoirs se pose par la proximité, sinon l'absorption du renseignement par le judiciaire.

Une opportunité

L'opportunité est la création d'une véritable communauté du renseignement basée sur une culture du renseignement, une réelle démarche incluant le renseignement dans le processus décisionnel politique (y compris la défense bien entendu) et économique.

Des administrations fédérales belges jouent un rôle dans ce que nous appelons le « champ d'actions » du renseignement et de la sécurité, chacune avec leurs compétences propres. Citons la Cellule de traitement de l'information financière (CTIF), l'Organe de coordination de l'analyse de la menace (OCAM), la police fédérale, l'Autorité nationale de sécurité (ANS), le Centre pour la cybersécurité, les différentes structures de reconnaissance et de renseignement au sein de la Défense, la Belgian Intelligence Academy (BIA), par exemple. D'autres organisations sont apparues sur le lit de plus anciennes : le Conseil national de sécurité (CNS), le Comité stratégique, le Comité de coordination du renseignement et de la sécurité et les acteurs qui composent ces organes. Toutes complètent ce que Sébastien Laurent (9) appelle un « dispositif de renseignement », une architecture politique et administrative complexe, « déjouant toute idée de rationalité ».

La culture du renseignement est ce qui nous fait le plus défaut, soulignait Alain Winants, ancien administrateur général de la Sureté de l'État (10). Culture et communauté du renseignement sont indissociables et entretiennent une relation paradoxale.

Est-ce la culture du renseignement qui nait d'une communauté préexistante ou, au contraire, la communauté du renseignement qui émerge d'une culture déjà présente dans un État donné ? Satgin Hamrah (11) écrit que la clé de la réussite de l'évolution d'une communauté du renseignement, c'est la culture. Et il faut l'y insuffler si elle n'existe pas. Chaque agence, chaque service possède des compétences, des règles et une culture propres (rites, mythes, vocabulaire…) qu'il faut à tout prix dépasser et partager, en vue de favoriser les échanges de renseignement au-delà du cercle traditionnel, tout simplement parce que les risques que les services doivent affronter, s'ils sont différents, s'inscrivent dans un continuum de la menace et nécessitent une conception intégrée de la sécurité. En Belgique, il faut un « printemps du renseignement », pour reprendre l'expression de Yannick Pech (12), une révolution culturelle, qui est celle qui amène la reconnaissance du renseignement par le politique et qui gagne le citoyen (13), qui amène la considération de sa juste utilité et de sa juste valeur, mais qui, assez paradoxalement, intègre le renseignement dans un processus sécuritaire.

> La gestion politique de l'insécurité en effet n'échappe pas – faut-il le déplorer ? – à la notion de « rentabilité immédiate ».

La culture du renseignement, poursuit Yannick Pech, souligne les dimensions sociale, académique et politique de cette culture (14). La Belgian Intelligence Academy (BIA) créée en 2014 et le Belgian Intelligence Studies Centre (BISC) créé en 2010, doivent participer à l'émergence de cette culture.

Patrick Leroy

Notes

(1) Robin Libert, « De geschiedenis van 175 jaar veiligheid van de Staat », *La Sureté, essai sur les 175 ans de la Sureté de l'État*, Bruxelles, Politeia, 2005, p. 23.

(2) Francis Balace, « 1915, la difficile naissance d'un service centenaire », *1915-2015 : l'histoire du service de renseignement militaire et de sécurité belge*, Anvers, Maklu, 2015, p. 35.

(3) Loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

(4) Sabine de Bethune, présidente du Sénat, *Regards sur le contrôle : vingt ans de contrôle démocratique sur les services de renseignement*, Anvers, Intersertia, 2013, p. vii (préface).

(5) Doc.parl., Ch., sess.ord.1995-1996, n°49-638/1, p. 3, cité par Pascale Vandernacht, conseiller d'État, *Quelles évolutions pour le SGRS ?*, 2016, p. 12.

(6) Doc.parl., Ch., sess.ord.1997-1998, n°1-758/10, p. 13, cité par Pascale Vandernacht, *op. cit.*, p. 13.

(7) Rapport d'activités 2010, Comité permanent de contrôle des services de renseignement et de sécurité, p. 49.

(8) Laurent Lagneau, « Pour les chefs de la DGSE et de la DGSI, la «réponse sécuritaire seule» ne suffit pas pour lutter contre le terrorisme », Opex360.com, 26 février 2016 (http://bit.ly/2luWOLK), consulté le 28 février 2016.

(9) Sébastien Laurent, *Politiques du renseignement*, Pessac, Presses universitaires de Bordeaux, 2009, p. 300.

(10) Entretien au *Soir* du 26 novembre 2015.

(11) Satgin Hamrah, « The role of culture in intelligence reform », *Journal of strategic security*, vol. 6, n° 5, automne 2013, p. 164.

(12) Yannick Pech, « Le poids des dispositifs et cultures de renseignement dans la formulation de la politique étrangère. Approche comparée des cas américain et français », *Stratégie et Renseignement*, Institut de stratégie comparée, n° 105, 2014, p. 123.

(13) David Omand, *Securing the State,* Ed Hurst&Co, 2010, p. 291.

(14) Yannick Pech, *op. cit.*, p. 109.

Photo ci-dessous : Siège des institutions de l'Union européenne et de l'OTAN, Bruxelles, qui accueille également de nombreuses ambassades, constituerait un véritable « nid d'espions » en raison de la multitude de journalistes étrangers, de lobbyistes et de diplomates qui y circulent. Selon certains observateurs, la capitale belge serait la deuxième capitale mondiale de l'espionnage après New York. (© Shutterstock/artjazz)

Le renseignement esp
Un modèle singulier en mutation

Le renseignement espagnol n'occupe pas une place de premier plan dans la « hiérarchie » des services étrangers couramment établie par les experts en la matière. L'Espagne est perçue, depuis la Guerre civile (sans oublier la Grande Guerre), bien plus comme un champ d'(inter)action des services étrangers que comme la matrice d'une culture spécifique du renseignement, fondée sur la fusion des services intérieur et extérieur en une seule institution centrale : le CNI (Centro nacional de inteligencia) (1).

Une organisation singulière

Le CNI a été créé sous le mandat du président (2) José María Aznar en 2002, sur le modèle du service unique déjà incarné par le CESID (Centre supérieur d'information de la Défense, créé en 1977). Depuis 2011, suite à une réforme menée par le président Mariano Rajoy, le CNI est rattaché au ministère de la Présidence.

Le renseignement militaire est assuré par le Centro de Inteligencia de las Fuerzas Armadas (CIFAS, Centre de renseignement des forces armées), intégré au sein de l'État-major de la Défense. Les armées de terre, de l'air, et la marine (*la Armada*) ont également leurs propres sections et divisions du renseignement.

On doit y ajouter les services des polices dépendant des Communautés autonomes (essentiellement Ertzaintza, au Pays basque, et Mossos d'Esquadra, en Catalogne) et les services de renseignement criminel (Commissariat général de Police judiciaire, Commissariat général au renseignement, Direction de Police judiciaire de la Guardia Civil et Service de vigilance douanière de l'Agence d'État d'administration fiscale, AEAT). Le Centre national de coordination antiterroriste (CNCA) a été créé à la suite des attentats du 11 mars 2004 à Madrid (191 morts, 1900 blessés) puis dissous en octobre 2014, avant d'intégrer le Centre de renseignement contre le crime organisé (CITCO).

Le CNI, on le voit, est le principal (et non réellement l'unique) service de renseignement en Espagne : il prend en charge le renseignement extérieur, le contre-espionnage, le renseignement économique et technologique et l'antiterrorisme. Il est l'interlocuteur désigné des services de renseignement étrangers et des organisations internationales. Le directeur du CNI est, en sa qualité d'« autorité nationale de sécurité », le destinataire de l'information classifiée OTAN, ainsi que de celle émanant de l'Union européenne. Le CNI prend en charge la sécurité des communications, à travers le Centre national de cryptologie (CCN), intégré au Centre. L'Office national de sécurité (ONS) gère l'information classifiée et accorde des habilitations de sécurité, afin de parer à toute fuite, comme celles de 1995, liées à des écoutes illégales du CESID. Enfin, le directeur du CNI, qui a rang et fonction de secrétaire d'État, doit gérer et coordonner la communauté espagnole du renseignement.

Le djihadisme, priorité absolue du renseignement espagnol

Si le spectre de l'ETA n'a pas tout à fait disparu, la principale menace en Espagne, depuis le 11 mars 2004, est le terrorisme islamiste. La lente atténuation du péril basque a d'ailleurs permis au CNI de redéployer ses personnels sur les terrains de la lutte contre la menace djihadiste. Début juin 2016, pour mieux faire face à cette menace, le CNI a engagé 500 experts supplémentaires, notamment des mathématiciens, des ingénieurs en télécommunications et des informaticiens. Le CNI a triplé ses effectifs, et engagé des spécialistes des dialectes de la langue arabe et du touareg. Le CNI forme désormais ses agents à une meilleure approche de la culture et de la religion islamiques, pour mieux en saisir la complexité.

Le directeur du CNI, le général d'armée Félix Sanz Roldán, privilégie une « approche intégrale » de ce qu'il dénomme le « cycle djihadiste » : recrutement, départ pour les zones de combat (Irak, Syrie, Libye…), entrainement de plusieurs mois, et parfois, en fonction de multiples parcours personnels, retour dans le pays d'origine. C'est alors que le danger est maximal, avec un risque d'attentats, ou bien une volonté chez l'ancien « combattant », de se lancer dans le recrutement prosélyte, un processus qui relance sans fin l'engrenage mortifère…

Les réseaux sociaux sont devenus pour l'État islamique (EI) un précieux outil d'élaboration stratégique ainsi qu'une formidable caisse de résonance à ses discours de

Photo ci-dessous : Le 28 septembre 2016, dans l'enclave espagnole de Melilla, un homme est escorté par la police espagnole dans le cadre d'une opération antiterroriste internationale qui a entrainé l'arrestation de 5 personnes en Espagne, en Allemagne et en Belgique, comme membres présumés d'une cellule de propagande du groupe État islamique (EI). Pour les services de renseignement espagnols, l'EI représente la menace numéro un dans le pays. (© AFP/Angela Rios)

agnol face à la menace djihadiste

Par **Gaël Pilorget**, hispaniste, professeur de l'Enseignement militaire supérieur scientifique et technique (Centre de doctrine et d'enseignement du commandement), commandant (RC) auprès du Gouverneur militaire de Paris, formateur en sécurité globale et chercheur au CF2R (renseignement, forces spéciales et terrorisme).

propagande et à sa « force de frappe » médiatique. Les experts du renseignement espagnol ont saisi combien Daech « synchronise » les actions terroristes et leur « publicité » (dans toutes les acceptions du terme), une démarche bien rodée dans laquelle ils ont acquis une redoutable expertise. La Direction du renseignement de la Guardia civil souligne le grand « professionnalisme » démontré dans l'élaboration des vidéos et des différents supports, notamment le souci d'une construction narrative très étudiée et, par là même, très « impactante »... Les services espagnols ont noté que l'EI « plagie » les formats de séries américaines et de jeux vidéos, délaissant le langage liturgique d'Al-Qaïda, principalement destiné aux imams, pour une rhétorique plus propre à séduire les jeunes, moins instruits religieusement mais encore plus radicaux et fanatisés. Pour parfaire cette propagande très ciblée, les vidéos sont traduites dans de multiples langues... dont l'espagnol.

Le CNI a bien saisi que l'objectif stratégique essentiel du terrorisme islamique est de conduire les sociétés visées à une confrontation violente avec les communautés musulmanes. Au fur et à mesure des reculs de l'EI sur les fronts irakien et syrien, Daech a recours au terrorisme « téléguidé » et à des « cyberterroristes », un phénomène qui, selon des experts de la Guardia civil, aurait succédé à celui des loups solitaires, étape qui serait désormais dépassée. D'autres experts soulignent les rapides mutations dans le choix des réseaux sociaux utilisés : Daech, soucieuse d'une sécurité maximale dans ses communications, chercherait à disposer de ses propres applications. Par ailleurs, des consignes sont données aux kamikazes : avant de commettre leur attentat, ils doivent « s'effacer » en tous points, en ne laissant derrière eux aucune trace numérique, afin de compliquer ensuite au maximum la tâche des enquêteurs et des services de renseignement.

La surveillance sur le terrain

La surveillance des services espagnols ne concerne pas que les réseaux sociaux. Ils se penchent sur les cas suspects au passé djihadiste, les lieux fréquentés en général par les communautés musulmanes (mosquées, centres culturels et religieux, magasins d'alimentation halal, associations...). Au sein de ces communautés, l'attention des services se concentre tout spécifiquement sur les personnes y ayant acquis un certain poids. Le ministère de l'Intérieur contrôle par ailleurs une soixantaine d'imams soupçonnés de propager une idéologie radicale.

Les services rencontrent d'autres difficultés dans la surveillance des mosquées illégales : garages, domiciles de particuliers, arrière-boutiques, salles de prières clandestines... autant d'espaces hors de contrôle. Selon les services de renseignement, certains de ces lieux secrets sont devenus, plus encore que les réseaux sociaux, les principaux centres de recrutement de Daech en Espagne. Mais, dans le cas où ils sont réellement des foyers de radicalisation, ils n'ont pas, pour l'heure, de réel contact avec Daech et n'ont pas les moyens techniques et financiers de représenter une menace de grande ampleur. Il existerait en Espagne 800 de ces « mosquées » illégales, en plus de la centaine qui ont déjà été démantelées par la police et la Guardia civil. Tous ces lieux clandestins ne sont pas forcément des vecteurs de prosélytisme radical, mais le manque de contrôle laisse toujours planer le doute, pour les services antiterroristes... La *Comunitat* valencienne semble agglomérer la plus grande part de ces « mosquées » illégales (devant même Madrid et la Catalogne). La région de Valence rassemble une très importante communauté musulmane, et donc un nombre potentiellement élevé de « proies » pour les réseaux de recrutement djihadistes.

Certes, le chiffre approximatif d'une centaine d'Espagnols partis combattre en Syrie et en Irak aux côtés de Daech est très réduit par rapport aux autres pays européens, comme la France, l'Allemagne ou le Royaume-Uni. Mais le ministère de l'Intérieur espagnol est bien en peine de dire ce qu'ils sont devenus. Quant à ceux qui pourraient partir aujourd'hui, les services de renseignement comptent également sur la mise en place, suite aux attentats de Paris de novembre 2015, du dispositif *Stop radicalismos* et de l'application mobile *Alertcops* pour détecter des cellules djihadistes ou de potentiels « loups solitaires ». Les alertes qui parviennent à ces plateformes se comptent aujourd'hui par centaines...

L'appel au crime

Les forces de sécurité et les services de renseignement ont détecté un nouvel aspect du recrutement djihadiste des plus préoccupants : des Espagnols partis combattre en Syrie et en Irak font parvenir de manière récurrente à leurs « frères » radicalisés demeurés en Espagne, le pressant message suivant : « Attaquez, attaquez, attaquez ! Nous devons faire quelque chose. Que doit-il se passer de plus pour que vous passiez à l'action ? » Les messages font ici allusion à la pression croissante imposée aux cellules djihadistes par les différents services, en Espagne et jusque sur les fronts irakien et syrien. Selon les services de renseignement, une centaine d'individus radicalisés vivant en Espagne seraient susceptibles de passer à l'acte si les conditions étaient favorables... Même si, selon certains rapports confidentiels, l'Espagne n'est pas citée spécifiquement comme une cible.

Il n'en demeure pas moins qu'en tant que porte d'entrée de l'Europe et ancienne terre du « Califat », l'Espagne ne saurait baisser la garde, d'autant que des experts avertissent du déplacement du péril djihadiste vers l'Afrique du Nord. Pour mieux répondre à la menace, les services de renseignement et de sécurité en appellent à la mobilisation de tous, y compris des acteurs sociaux et éducatifs, dans une prise de conscience commune et une collaboration nationale, dans le plein sens du mot.

L'ancienne terre d'Al-Andalus compte, elle aussi, sur son sol comme sur des fronts de chaos, ses « enfants perdus de l'islam » qu'elle doit savoir arracher à l'emprise de la haine. En cela, « il n'y a plus de Pyrénées », comme il n'y a plus de détroit de Gibraltar : la réponse appartient, pour une grande partie, à une Europe en permanent dialogue avec l'ensemble du vaste monde méditerranéen. Et au croisement de ces ensembles entremêlés, une Espagne modelée en partie, pendant des siècles, par une brillante culture islamique. C'est peut-être là, paradoxalement, que peut naitre une vraie Reconquête inversée : dire et assumer cet héritage de bâtisseurs et de savants pour mieux contrer la destruction et l'ignorance.

Gaël Pilorget

Photo ci-dessus : Felix Sanz Roldan, directeur des services de renseignement espagnols (CNI) depuis 2009, annonçait en juillet 2016 lors d'un séminaire sur la sécurité que son service souhaitait engager plusieurs centaines de nouveaux agents d'ici 2020, notamment afin de surveiller et repérer l'activité djihadiste sur le web. (© Security & Defence Agenda)

Notes

(1) Le terme « *inteligencia* » a en espagnol les mêmes acceptions que l'anglais « *intelligence* ».

(2) En Espagne, l'exécutif est placé sous l'autorité du « président du gouvernement ». Les services de la « présidence » espagnole sont donc assimilables, en France, à ceux du Premier ministre.

Les *services* secrets *allemands*

Par **Wolfgang Krieger**, spécialiste international du renseignement et professeur d'histoire à l'Université de Marbourg.

Depuis le 4 novembre 2011, jour de la découverte d'une série de crimes racistes commis par un groupe néo-nazi, le NSU, le renseignement intérieur allemand, qui a totalement échoué dans sa mission, doit procéder à une réforme de fond. Peu après, en juin 2013, Edward Snowden rend publics des documents ultra-secrets d'origine américaine qui révèlent la coopération étroite entre le service extérieur allemand et la NSA en matière d'écoutes téléphoniques et d'exploitation des communications par Internet. Si, d'un côté, l'efficacité du renseignement antiterroriste est mise en doute, c'est l'illégalité (présumée) qui fait scandale de l'autre. Ainsi des ministres et de hauts fonctionnaires au sein de l'Union européenne (UE) et de grandes sociétés comme EADS auraient été espionnés – au profit des Américains de surcroit ! Plusieurs enquêtes parlementaires s'ensuivent, toujours en cours, ainsi qu'une nouvelle législation destinée à « mieux contrôler » les services secrets. Résultat : leur prestige est au plus bas aujourd'hui, du moins dans la presse allemande et parmi les militants de la gauche politique.
S'il est aujourd'hui assez difficile de connaitre précisément les effectifs totaux du renseignement allemand (1), celui-ci se décompose en trois principaux services :

Le renseignement intérieur

Afin d'assurer le renseignement intérieur, c'est en 1950 que la République fédérale crée le Bundesamt für Verfassungsschutz (BfV) (Office fédéral pour la protection de la Constitution) [sur les origines plus lointaines du renseignement allemand, voir p. 8 de ces *Grands Dossiers*, NdlR]. Parallèlement, les Länder, auxquels la Constitution de 1949 accorde une compétence exclusive en matière de police, prennent en charge, eux aussi, le renseignement intérieur sur leur terrain. D'où le « système » actuel composé de 17 bureaux de renseignement intérieur (un au niveau fédéral et 16 pour chacun des Länder). Pour la même raison, la compétence du BfV se limite à la coordination de la surveillance des mouvements politiques extrémistes (communistes révolutionnaires, néo-nazis, islamistes, racistes) ainsi que d'organisations criminelles (drogues, armes, blanchiment d'argent, trafic de femmes et d'enfants, etc.). En dehors de la coordination des 17 services, le BfV mène aussi ses propres opérations, principalement contre des menaces qui touchent l'Allemagne dans sa totalité (ou presque) et contre des menaces de nature transnationale (on dénombre environ 3000 personnes travaillant pour le BfV auxquelles s'ajoutent environ 2900 personnes dans les Länder). Globalement, le BfV dirige aussi les opérations de contre-espionnage, souvent en coopération avec ses homologues dans les Länder, pour protéger les institutions publiques et l'industrie privée.

Le renseignement extérieur et militaire

Le Bundesnachrichtendienst (BND) (Service fédéral de renseignement) assure le renseignement extérieur (environ 6500 personnes) Créé en 1956, peu après l'adhésion de la République fédérale à l'OTAN et la création de l'armée fédérale (la Bundeswehr), il a pour prédécesseur « l'organisation Gehlen », établie en 1946, qui travaillait pour les Américains (d'abord pour l'armée américaine en Europe, puis à partir de 1949 pour la CIA). Son chef, Reinhard Gehlen, ainsi que bon nombre de ses collaborateurs, sont des anciens de la Wehrmacht, de l'Abwehr et du renseignement de la SS (le RSHA d'Heinrich Himmler). À la différence des services en France, au Royaume-Uni et dans bien d'autres pays membres de l'OTAN – pour ne pas évoquer les vastes effectifs du renseignement américain –, le BND assure en même temps et d'une manière assez compliquée une double mission de renseignement extérieur et de renseignement militaire (2). En sont absents tous les moyens armés (service action) et toute capacité de monter des opérations clandestines non armées (propagande, intoxication, financement secret, etc).

Photo ci-contre : Le 16 février 2017, la chancelière allemande, Angela Merkel, est entendue par une commission d'enquête parlementaire chargée d'établir à quel point l'exécutif allemand était au courant et partie prenante des écoutes massives de la NSA américaine. La presse allemande a en effet révélé en avril 2015 que le service de renseignement allemand (BND) était soupçonné d'avoir écouté ses voisins européens – notamment français – pour le compte de la NSA, sans en alerter son autorité de tutelle. Cette affaire a suscité une intense polémique dans le pays. (© Jonas Schoenfelder)

Après 1990, au moment où est mise en place une structure militaire nationale à Berlin/Potsdam et où l'Allemagne participe à des missions extérieures internationales comme en ex-Yougoslavie, en Afghanistan et en Afrique, beaucoup de chefs militaires souhaitent la création d'un service de renseignement militaire au sein du ministère de la Défense. Cette « bataille de compétences » se termine pourtant en décembre 2007 par une défaite écrasante de l'armée. Depuis, seul le vice-président militaire assure de manière visible la représentation au sommet du BND de la fonction « renseignement militaire ».

Le contre-espionnage militaire

Le troisième service de renseignement au niveau fédéral, le Amt für Militärischen Abschirmdienst (MAD) (Service de protection de la Bundeswehr) se limite à la sécurité du personnel et des installations de la Bundeswehr, y compris les bases temporaires de mission (en Afghanistan etc.) et leurs employés locaux. Il s'agit donc d'un service de contre-espionnage militaire et non pas de renseignement militaire proprement dit. Il a été créé en 1956, au même moment que l'armée elle-même (et compte environ 1200 personnels).

Les autres services

Au niveau fédéral, deux autres bureaux s'ajoutent à cette architecture, qui emploient des moyens du renseignement, humains et autres, mais qui ont généralement d'autres compétences. Le Bundeskriminalamt BKA (Police criminelle fédérale) (environ 5500 personnels) et le Zollkriminalamt (ZKA) (police criminelle des Douanes fédérales) (environ 400 personnels). De même, la Bundespolizei (police fédérale) a pour mission la sécurité des frontières, des aéroports et des gares ferroviaires. Mais seule une fraction de ses 41 000 membres travaille dans le renseignement. Au niveau des Länder, l'on trouve aussi certaines unités de la police qui travaillent avec des moyens du renseignement (indicateurs, écoutes etc.).

Répartition des responsabilités et coopération

Dans la plupart des cas, la répartition des responsabilités ministérielles suit les conventions de l'État moderne.

Le ministère de l'Intérieur s'occupe du renseignement intérieur et de la police (BfV et BKA, LfV, police), le ministère des Finances s'occupe des douanes, et le ministère de la Défense de la protection de l'armée. Seule exception : le BND, qui est sous la tutelle de la chancellerie ou plutôt de son ministre fédéral (Peter Altmaier), appuyé par un secrétaire d'État (Klaus-Dieter Fritsche) qui surveille globalement le renseignement fédéral. Cette attribution soulève des questions « de philosophie constitutionnelle » car la chancelière n'est ni le commandant en chef des armées (comme le sont les présidents français et américain), ni le chef de la diplomatie.

Plusieurs comités de liaison et de coopération assurent la cohérence du renseignement fédéral et la coopération avec les Länder (selon le modèle des « *fusion centers* » américains) : Gemeinsames Terrorismusabwehrzentrum (depuis 2004), Nationales Cyber-Abwehrzentrum (depuis 2011) et quelques autres pour traiter des migrations et de l'extrémisme politique. S'y ajoute la coopération internationale très étroite avec les services homologues (américains, français, britanniques, israéliens et bien d'autres). Comme nulle part ailleurs dans le monde, la coopération étroite avec la NSA fit l'objet d'un scandale suite à la fuite d'Edward Snowden en 2013.

Photo ci-dessus : Siège du BfV (renseignement intérieur) à Cologne, en Allemagne. En novembre 2016, un agent du renseignement intérieur allemand chargé de surveiller la scène islamiste nationale a été arrêté car il était soupçonné de préparer lui-même un attentat islamiste contre le siège du BfV. (© Bundesamt für Verfassungsschutz)

Quel encadrement légal ?

Au début, seul le travail du BfV s'appuyait sur une loi parlementaire – loi effective en 1950 ayant fait l'objet d'une profonde révision en 1990 (dernières révisions en 2016). Le BND, quant à lui, est fondé par décision gouvernementale, étant un service sans compétences exécutives sur le sol allemand. En 1990, c'est dans le contexte d'une vaste législation sur le droit à l'information, donc éloignée des préoccupations d'espionnage, qu'est votée une loi portant sur le BND et le MAD. Il ne s'agit donc pas d'une loi de portée générale mais d'une loi qui règle des questions informatiques, surtout concernant les données relatives à l'individu. Seule exception : l'article 2, qui permet au BND d'assurer son propre contre-espionnage (à la différence de la CIA par exemple). Par la suite, dans l'après 11-Septembre, une législation très spécifique modifie l'accès à l'information personnelle des individus et l'échange d'information entre les autorités publiques. Sont visées les personnes soupçonnées d'activités terroristes, islamistes et criminelles organisées dans le cadre de recherches préventives.

Cette législation a suscité de vifs débats et des craintes multiples dans l'opinion allemande, surtout concernant le stockage gigantesque des données et l'exploitation de l'Internet (messageries, réseaux sociaux, etc.). Pour rassurer le public, le contrôle parlementaire a été renforcé sur tous les services, et en particulier sur le BND. La première législation visant à un contrôle généralisé du BND avait été votée en 1978, à la suite d'un scandale d'écoutes téléphoniques. Elle instaurait une commission spéciale pour surveiller les activités du BND. En 2009, pour élargir le contrôle parlementaire (après l'adoption de la législation post-11-Septembre qui avait élargi les compétences du renseignement), une nouvelle loi règle les détails de compétence et de procédure de la commission de contrôle parlementaire du Bundestag (Parlamentarisches Kontrollgremium). En 2016, une nouvelle législation ajoute un chef d'équipe de recherche auprès de la commission. Cette dernière a accès à tous les dossiers et peut demander une audition de tous les employés et fonctionnaires des trois services fédéraux. Elle jouit également d'un droit d'accès à tous les bureaux et toutes les installations. Les services doivent lui fournir toutes leurs données (électroniques) mais n'ont pas l'obligation de lui permettre un accès direct à ces données (ordinateurs, bases des données). Sont également exclues toute information transmise par des services étrangers ainsi que toute information personnelle concernant les sources humaines. De même, le gouvernement n'est pas obligé de lui donner ses documents délibératifs, donc concernant des projets ou décisions éventuels (« domaine réservé de l'exécutif »). Mais la Cour constitutionnelle a très étroitement limité cette prérogative de l'exécutif (lors d'une plainte concernant une mission secrète du BND en Irak en 2003). D'après la loi de 2009, la Cour peut être saisie directement par la commission en cas de conflit sur l'application de cette loi (3).

Pour aller plus loin

Wolfgang Krieger, « The German Intelligence Community », *in* Bob de Graaff et James M. Nyce (dir.), *The Handbook of European Intelligence Cultures,* Lanham (MD, États-Unis), Rowman&Littlefield, 2016.

Parmi d'autres institutions de contrôle, il faut mentionner le comité secret de la Commission du budget fédérale, qui a le droit d'examiner en détail le budget des services secrets, le comité de la surveillance qui autorise les écoutes (G-10 Kommission), et un tout nouveau comité indépendant, installé par une nouvelle loi pour le BND (2016), pour autoriser la surveillance des communications en dehors du territoire allemand. Ce dernier comprend plusieurs procureurs et juges fédéraux qui décident en toute liberté. Ainsi, on élargit la protection de l'individu sous la constitution allemande de manière planétaire. Autrement dit, si un taliban en Afghanistan ou un guerrier de Daech en Irak parlent au téléphone, ils ne peuvent plus être écoutés par le BND sans l'accord de la haute justice allemande. Cela suppose une longue procédure préalable car les agents allemands sont obligés de vérifier l'identité précise de leurs cibles.

Le message politique est assez clair. On veut une « judiciarisation» du renseignement extérieur. Est-ce un droit-de-l'hommisme (Hubert Védrine) un peu particulier ? On ne sait pas pour l'instant si cette nouvelle législation de novembre 2016 jouera en faveur du renseignement anti-islamiste ou pas. Et, si Berlin commence (en 2016 seulement) à parler d'un cyberdispositif qui ne soit plus exclusivement défensif, et de drones armés (4), c'est plus la Bundeswehr qui en profitera que les services de renseignement. Quoi qu'il en soit, les deux domaines sont encore très loin d'une réelle capacité de riposte.

Wolfgang Krieger

Notes

(1) Selon mes propres estimations, ils dépassent les 15 000 personnes.

(2) Voir : Wolfgang Krieger, « De la difficulté de combiner renseignements extérieurs et militaires : le Bundesnachrichtendienst (BND) allemand », *Cahiers de la sécurité*, nº 13 (juillet-septembre 2010).

(3) Aucune autre commission parlementaire ne dispose d'un accès comparable à la plus haute instance judiciaire.

(4) Voir : Wolfgang Krieger, « The German Approach to Drone Warfare », *Intelligence and National Security*, vol. 32-3, 2017.

Photo ci-dessus : Nouveau siège du BND à Berlin, dont le cout total de la construction est estimé à 1,5 milliard d'euros. Alors que l'Allemagne fait face à une menace terroriste particulièrement importante, les budgets des services de renseignement ont été fortement augmentés en 2016 : +18 % pour le BfV, + 12 % pour le BND, auxquels s'ajoutent 150 millions d'euros pour déchiffrer les messageries en ligne cryptées. (© Fridolin Freudenfett)


NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
UNITED STATES OF AMERICA

Techniques

Photo ci-contre : Le 9 août 2010, le secrétaire à la Défense Robert Gates arrive à Springfield, au siège de la NGA (National Geospatial Intelligence Agency), l'agence du département de la Défense des États-Unis en charge de la collecte, de l'analyse et de la diffusion du renseignement géospatial. La NGA possède des bureaux inaugurés en 2011 pour un coût de 1,4 milliard de dollars, constituant le troisième bâtiment le plus important de Washington. Épargnée par les scandales qui ont pu toucher la CIA ou la NSA, la NGA est aux images ce que la NSA est à la voix, et dispose des caméras les plus performantes au monde : l'ARGUS-IS, invisible depuis le sol à une altitude de 6000 mètres, bénéficie d'une résolution de 1,8 milliard de pixels, peut surveiller entre 25 et 40 km² en une seule fois et stocker jusqu'à 1 million de téraoctets de données par jour. (© DoD/Cherrie Cullen)

analyse

Par **Alain Charret**, rédacteur en chef de *Renseignor*, chercheur associé au CF2R, ancien cadre des centres d'écoutes de l'armée de l'air.

Photo ci-dessus :
Station d'interception du Réseau Échelon à Menwith Hill, au Royaume-Uni. Le réseau Échelon est le nom de code utilisé pour désigner le système mondial d'interception des communications privées et publiques mis en place en 1946 par les pays signataires du traité secret UKUSA (États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande) et géré par les services de renseignement des États membres.
(© Matt Crypto)

Les enjeux du renseignement d'origine électromagnétique

Depuis la fin de la Seconde Guerre mondiale, le renseignement issu d'éléments d'informations émis par du matériel électronique, notamment appels téléphoniques et emails, représente une source essentielle pour les agences de renseignement. Au-delà des révélations sur les systèmes d'écoute à grande échelle, il est essentiel de bien comprendre le fonctionnement du ROEM et ses utilisations pour mieux en appréhender les enjeux.

Les interceptions des communications électroniques pour obtenir du renseignement d'origine électromagnétique (ROEM) sont souvent vivement dénoncées par des défenseurs des libertés individuelles protestant contre les écoutes de masse pratiquées par les organismes gouvernementaux. Mais avant de verser dans la paranoïa, il est intéressant de comparer quelques chiffres.

Durant l'année 2003, l'Union internationale des télécommunications (UIT) a estimé que le nombre de communications vocales avait dépassé les 180 milliards de minutes. Ce qui équivaut à 340 années de temps ! Treize ans plus tard, devant l'accroissement considérable des moyens de communications, on peut raisonnablement penser que ce nombre a augmenté de manière exponentielle. Même les supercalculateurs de la NSA ne sont pas en mesure d'intercepter et encore moins d'exploiter une telle masse de données. Les chiffres qui circulent entre initiés indiquent que 10 % à 20 % de l'ensemble des communications tomberaient ainsi dans les filets de l'agence américaine, dont une partie seulement, difficile à évaluer sans y avoir accès, serait véritablement exploitée... Comment ? Pour quoi ?

Comprendre le fonctionnement des écoutes

L'acquisition du renseignement fait appel à des sources diverses. Parmi celles-ci figurent deux grands groupes : le renseignement d'origine humaine (ROHUM), également appelé HUMINT pour *Human Intelligence*, et le renseignement technique. Ce dernier relève essentiellement de deux domaines : le ROIM (IMINT, pour *Imagery Intelligence*), autrement dit l'imagerie, et le renseignement d'origine électromagnétique (ROEM), également appelé SIGINT pour *Signal Intelligence*, qui nous intéresse ici.

Le ROEM lui-même comprend le COMINT – pour *Communication Intelligence*, qui consiste à exploiter le contenu des transmissions – et l'ELINT pour *Electronic Intelligence*, qui consiste en l'étude du support de la transmission. Les moyens permettant le recueil de ce type de renseignement peuvent être de natures diverses. Ainsi, il peut s'agir de centres d'écoutes fixes, d'unités mobiles, sur terre et mer comme dans les airs, ou encore de satellites.

Principes techniques

Un certain nombre de connaissances techniques (voir encadré ci-dessous) permettent à l'opérateur d'écoutes d'orienter ses recherches et de sélectionner ainsi le spectre de fréquences qu'il devra explorer. Par ailleurs, il est intéressant de noter que, de la même façon qu'il existe des prévisions météorologiques, on peut faire des prévisions de propagation. Ainsi, l'opérateur qui aurait pour objectif de rechercher et d'intercepter une communication émanant de Syrie à destination de la Somalie saurait, en les consultant, dans quelle gamme axer sa surveillance. D'autres éléments permettent d'affiner la recherche en associant connaissances techniques et renseignement ouvert. Ainsi, la simple observation d'un bulletin d'information télévisé montrant des djihadistes communiquant avec des radios portables apporte de précieux indices. Une radio portable de type talkie-walkie comporte généralement une antenne dont la longueur est équivalente à un quart de la longueur d'onde. Il suffit d'estimer la longueur de cette antenne et de la multiplier par quatre pour avoir la longueur d'onde utilisée. Ensuite, une formule très simple permet d'en calculer la fréquence. De quoi sérieusement faciliter le travail de recherche de l'opérateur d'écoutes au sein de la structure pour laquelle il travaille...

Écouter quoi ?

Dans le domaine militaire, il s'agira principalement d'écouter les transmissions des forces armées d'ennemis potentiels, afin d'être en mesure de connaître au mieux la doctrine d'emploi de ses matériels et autres armements, ainsi que les tactiques employées lors des exercices. Ceci afin de mieux préparer des contre-mesures et une riposte éventuelle.

En revanche, dans le domaine civil, le champ d'action est beaucoup plus vaste. L'écoute des réseaux de téléphonie mobile et satellitaire y occupe une place importante. Les centres d'interception – sur le territoire national, dans des pays alliés ou encore dans certaines ambassades – recueillent les transmissions diplomatiques de pays étrangers. Si les codes utilisés sont parfois difficiles à casser, l'analyse du volume du trafic est déjà, en soi, un renseignement. Par exemple, l'augmentation soudaine des échanges de messages entre une capitale et une de ses ambassades est, généralement, le signe d'une activité particulière qui peut ensuite être confirmée par une ou plusieurs autres sources.

En France, l'autorité gouvernementale ou militaire établit ses besoins dans un Plan particulier de renseignement (PPR) qu'elle adresse à ses services spécialisés. Les priorités y sont clairement indiquées. Le service de renseignement ainsi sollicité réalise un Plan particulier de recherche afin d'orienter ses moyens de recueil. Il émet également des OIH, Ordres d'interception hertzienne. Les centres d'interception (voir encadré page 87) recueillent les données indiquées, en font une pré-analyse et les adressent aux organismes chargés de l'exploitation. Là, les données sont exploitées, corrélées avec d'autres sources et une synthèse est adressée à l'autorité ayant exprimé son besoin. On peut imaginer que ce schéma est plus ou moins le même dans la plupart des pays.

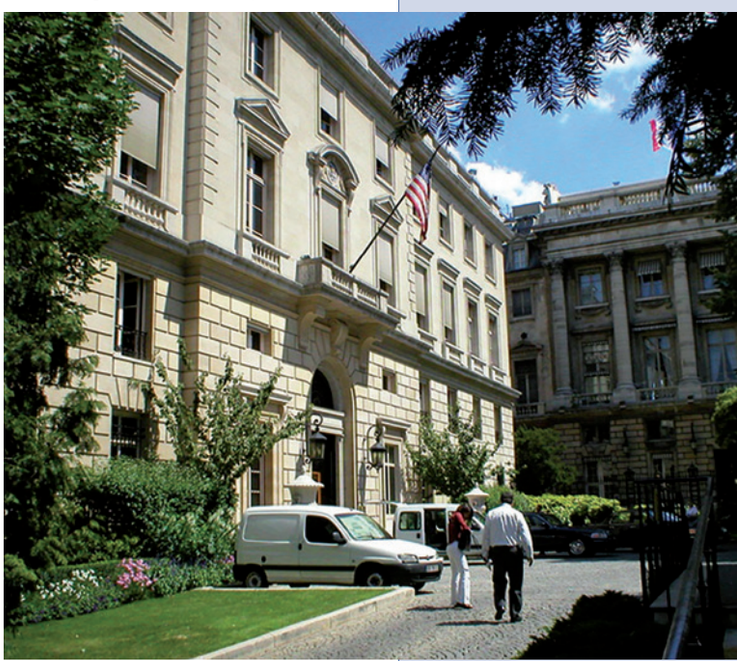


Photo ci-dessus :
Ambassade des États-Unis à Paris, suspectée d'accueillir un centre d'écoutes installé au dernier étage du bâtiment et permettant notamment d'écouter les communications de l'Élysée, situé à proximité. Quatre-vingt sites de ce type auraient déjà été construits dans le monde par les services américains. (© usembassy.gov)

La physique, au cœur du fonctionnement des centres d'écoutes

D'une manière générale, lorsque l'on parle de renseignement d'origine électromagnétique (ROEM), il s'agit des informations véhiculant ou véhiculées par des ondes hertziennes appelées également ondes radioélectriques. Elles ont la propriété de se propager dans l'espace. Mais cette propagation varie en fonction de différents critères dont, notamment, la fréquence et le type de milieu dans lequel elles évoluent. Ainsi, d'une manière générale, ces ondes se propagent très bien dans l'air, alors qu'elles sont arrêtées ou tout du moins sérieusement affectées par des matières conduisant l'électricité, par exemple le cuivre.

Par ailleurs, la fréquence et, dans une moindre mesure, la puissance d'émission, affectent le mode de propagation. Ainsi, certaines ondes vont se refléter sur des couches de l'ionosphère et ainsi pouvoir, par rebonds successifs, faire le tour de la Terre. D'autres, non affectées par les couches de l'ionosphère, vont se propager à vue et elles seront arrêtées par tout obstacle un tant soit peu conducteur. C'est pourquoi les transmissions à destination et en provenance de submersibles posent certaines difficultés. L'eau étant un conducteur, seule une catégorie de ces ondes est à même de traverser le milieu aquatique. Il s'agit des très grandes ondes, appelées également VLF (*Very Low Frequency*). À l'opposé, pour communiquer avec des satellites, on utilisera des ondes ultra-courtes qui traverseront les différentes couches de l'ionosphère sans en être affectées. Aussi, on note que la longueur d'onde qui s'exprime en mètres est inversement proportionnelle à la fréquence qui, elle, s'exprime en hertz.

Du même auteur

Al-Shabaab, au cœur du terrorisme somalien, Paris, Les éditions de l'absence, 2016, 243 p.

Écoutes radioélectriques et renseignement, Paris, L'Harmattan, 2006, 240 p.

Photo ci-dessous :
Le 14 février 2005, un attentat à la bombe vient de causer la mort du Premier ministre libanais, Rafic Hariri. Si les services de renseignement syriens sont rapidement montrés du doigt, l'analyse des communications mobiles au moment de l'attentat va conduire à l'arrestation de quatre suspects : Moustapha Hamdane (chef de la garde présidentielle), Jamil Sayyed (ancien chef de la sûreté générale), Ibrahim El-Haj (ex-directeur des forces de sécurité intérieures) et Raymond Azar (chef des services de renseignement de l'armée). (© AFP/Joseph Barrak)

Différentes utilisations du ROEM à travers trois exemples

L'exploitation des données de téléphone mobile : un atout stratégique

L'analyse des communications mobiles quelque temps avant ou pendant une opération particulière – telle qu'un attentat ou un enlèvement – peut fournir des informations cruciales. Ce fut notamment le cas après que, le 14 février 2005, le Premier ministre libanais Rafic Hariri fut tué dans un attentat à la voiture piégée. Devant les difficultés liées au contexte trouble de la région et afin de tenter d'obtenir des conclusions objectives à des investigations complexes, une enquête internationale sous l'égide de l'ONU a été demandée par la France. Un des éléments principaux des investigations repose sur l'exploitation des téléphones portables actifs dans la zone au moment des faits. Ainsi, ce sont huit numéros d'abonnés et dix téléphones mobiles dont les données furent analysées. Les lignes ont été activées le 4 janvier 2005 dans le Nord du Liban, entre Terbol et Menyeh. Ensuite, ces terminaux ont été repérés dans le secteur de Beyrouth en corrélation avec les déplacements de Rafic Hariri. Le 14 février, six des téléphones ont été repérés entre le Parlement et l'hôtel Saint George ainsi que sur l'axe Zqaq El-Blat et Al-Bachoura. Les appels ont eu lieu à 11 heures. Le téléphone localisé à proximité du Parlement émit quatre appels à destination des autres appareils à 12h53, l'heure à laquelle le véhicule du Premier ministre quitta Nejmeh Square. Ensuite, les téléphones restèrent silencieux jusqu'à 12h56, heure de l'explosion.

En octobre 2008, un mémo confidentiel portant sur la faiblesse de l'alibi d'une personne de l'entourage direct de Rafic Hariri fut adressé à Gary Loeppky, un ancien cadre de la gendarmerie canadienne qui avait repris le poste d'enquêteur en chef de l'ONU quelques mois auparavant. Dans ce cas, l'exploitation des données du téléphone portable de l'intéressé fut essentielle. Alors qu'il avait indiqué dans son témoignage qu'il avait été appelé la veille au soir pour se présenter à un examen universitaire, les données téléphoniques indiquaient qu'il était à l'origine de l'appel. En effet, à 21h57 il appela l'examinateur. Ce dernier le rappela à 22h06. Plus troublant encore, les appels eurent lieu plus de 30 minutes après que le suspect eut, selon ses dires, demandé sa journée à Rafic Hariri, afin justement de se présenter à l'examen. Sinon, il se serait trouvé au côté du Premier ministre au moment de l'attentat. Le téléphone portable du mis en cause indique qu'il se trouvait dans la zone de son domicile le 14 février de 8h35 à 12h06. Au cours des trois heures et demie durant lesquelles il était censé étudier à domicile, il reçut 24 appels d'une durée variant de 5 à 226 secondes, ce qui fait une moyenne d'un appel toutes les 9 minutes. Difficile de se concentrer dans de telles conditions. Ce cas démontre une nouvelle fois l'importance que revêt l'exploitation des données de téléphonie mobile dans la plupart des investigations.

> *« L'analyse des communications mobiles quelque temps avant ou pendant une opération particulière – telle qu'un attentat ou un enlèvement – peut fournir des informations cruciales. »*

Le renseignement technique qui causa la perte d'Oussama ben Laden

Ce n'était un secret pour personne, Oussama ben Laden avait quant à lui totalement proscrit les moyens modernes de communication tels que téléphones mobiles ou satellitaires, internet et autres systèmes radioélectriques afin de déjouer le système d'écoute planétaire opéré par les États-Unis et leurs alliés. D'ailleurs, ce fut un des indices qui ne fit que renforcer les interrogations des services de renseignement américains lorsqu'ils découvrirent que le complexe d'Abbottabad ne disposait d'aucune ligne téléphonique, pas plus que de connexion internet. Et pourtant, selon des sources proches des services de renseignement s'exprimant sous couvert d'anonymat dans la presse d'outre-Atlantique, c'est une communication téléphonique qui serait à l'origine de la perte de Ben Laden.

Selon certaines informations, en 2010, un appel téléphonique destiné à Abou Ahmed al-Kuwaiti, connu des services de renseignement comme étant un des messagers de confiance employés par le chef d'Al-Qaïda, a mené les Américains à s'intéresser à la résidence d'Abbottabad. En fait, cette communication ne comportait pas d'informations véritablement confidentielles. Cependant, l'attention des analystes fut attirée. L'ami d'Al-Kuwaiti demanda à celui-ci où il se trouvait maintenant. Al-Kuwaiti répondit qu'il était retourné « *auprès des gens avec qui il était auparavant* ». Cette phrase fut suivie d'un silence estimé plus long que la normale. Connaissant la proximité d'Al-Kuwaiti avec Ben Laden, les services américains estimèrent qu'il pouvait se trouver avec le chef d'Al-Qaïda lui-même. À partir de ce moment, tous les moyens humains et techniques

de surveillance furent employés afin de suivre le moindre geste d'Al-Kuwaiti. C'est ainsi que fut découverte la résidence d'Abbottabad.
Parmi les indices relevés lors de cette longue surveillance, il fut établi que pour utiliser leurs téléphones portables, les habitants de la résidence s'éloignaient au minimum à 90 minutes de route d'Abbottabad. Ceci afin de déjouer toute tentative de localisation des services d'interception. Après de longs mois de surveillance intensive et d'analyses, les autorités américaines furent convaincues que le chef d'Al-Qaïda se cachait à Abbottabad. Barack Obama donna l'ordre d'intervenir. C'est donc bien encore une fois un renseignement technique qui est à l'origine de cette opération...

> *« Non contents de figurer parmi les meilleurs sur le plan des techniques d'interception, les spécialistes israéliens ont rapidement compris qu'ils pouvaient s'en servir comme d'une véritable arme, au sens propre du terme. »*

Les écoutes téléphoniques, une arme létale au service de l'État ?

Les experts s'accordent à dire qu'Israël a souvent été un précurseur en matière de guerre électronique. Non contents de figurer parmi les meilleurs sur le plan des techniques d'interception, les spécialistes israéliens ont rapidement compris qu'ils pouvaient s'en servir comme d'une véritable arme, au sens propre du terme. La première opération connue d'élimination d'un terroriste présumé grâce à l'interception se déroula le 5 janvier 1996. La cible n'était autre que Yahia Ayache, un artificier du Hamas. L'opération était assez complexe puisqu'il avait fallu tout d'abord subtiliser le téléphone cellulaire du Palestinien afin d'y placer une charge explosive actionnable à distance. Le jour dit, un système d'interception se trouvait à bord d'un hélicoptère qui survolait discrètement la zone du domicile de Yahia Ayache. Il a suffi d'attendre qu'un appel arrive. Une fois la voix de Yahia Ayache formellement identifiée, la bombe fut déclenchée à distance et l'explosion tua le Palestinien.

Le 21 avril de la même année, les services russes utilisèrent un procédé semblable. La cible n'était autre que le président indépendantiste tchétchène Djokhar Doudaïev. Les services techniques de Moscou avaient placé son téléphone satellitaire sous surveillance. Parallèlement, des avions de combat étaient placés en alerte. Dès qu'une communication fut établie et la voix du général tchétchène identifiée, le terminal fut localisé et la position transmise à l'aviation. Quelques minutes plus tard, deux missiles air-sol étaient tirés sur sa position. Djokhar Doudaïev trouva la mort dans ce raid.
Les États-Unis ont, eux aussi, recours à cette pratique. Ainsi, le 1er mars 2008, les services américains, après avoir identifié le téléphone satellitaire de Raul Reyes, lors d'une communication, ont localisé l'appareil à la frontière équatorienne et fourni sa position aux Colombiens, qui ont déclenché un raid dans lequel le numéro deux des FARC a perdu la vie.
L'usage croissant de la technologie sans fil – donc utilisant les ondes radioélectriques – renforce le rôle joué par le ROEM. Il est désormais un atout majeur dans la lutte contre le terrorisme et notamment dans la localisation de cibles potentielles. Ce type d'actions, bien que restant discrètes pour des raisons évidentes de sécurité, est donc encore appelé à se développer.

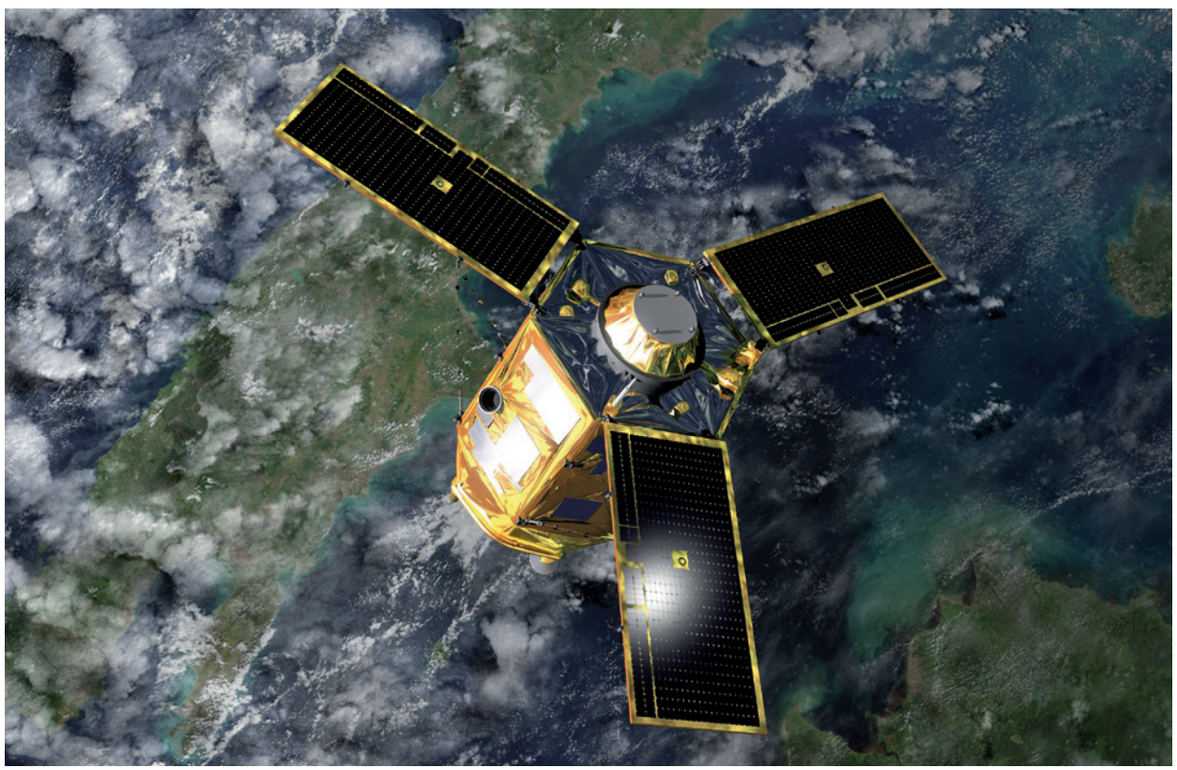
Alain Charret

Photo ci-dessus :
Site d'écoute de la DGSE sur le plateau d'Albion. Il constituerait l'une des stations d'écoute du renseignement électronique stratégique français – que certains ont baptisé « Frenchelon » – réparti entre la métropole et les territoires d'outre-mer. En France, la loi sur le renseignement différencie les interceptions effectuées sur le territoire national de celles réalisées à l'étranger. D'une manière générale, la surveillance des communications internationales fait l'objet de moins de contrôles. (© Véronique Pagnier)

Photo ci-dessus :
Artificier du Hamas et considéré comme le responsable d'un certain nombre d'attentats, Yahia Ayache fut assassiné en janvier 1996 par le contre-espionnage israélien – le Shin Bet – grâce à une mini-bombe placée dans son téléphone portable. (DR)

Composition d'un centre d'écoutes COMINT type

Si le vocabulaire employé diffère quelque peu entre les organismes militaires ou civils, la structure du centre d'écoutes type reste, globalement, la même.
Ce dernier est dirigé par un chef de centre secondé par un chef des opérations. Le premier est chargé de veiller au bon fonctionnement du centre dans son ensemble ; le second est plus particulièrement chargé de faire appliquer l'OIH (Ordre d'interception hertzienne).
Le personnel opérationnel est constitué d'opérateurs maîtrisant la langue du pays cible et d'analystes. Leur nombre varie en fonction des missions attribuées au centre et de ses priorités. Souvent, des décodeurs viennent compléter l'équipe. Ils sont chargés de « casser » les codes éventuellement utilisés lors de transmissions sensibles. Les postes de travail de chaque opérateur, appelés également tables d'écoute, sont généralement constitués de plusieurs récepteurs reliés à des systèmes d'enregistrement et d'un terminal permettant de rédiger les procès-verbaux d'écoutes ainsi que d'accéder à la documentation opérationnelle. Les missions confiées à chaque opérateur le sont sous la responsabilité d'un chef de quart.
Dans chaque centre se trouve une table dédiée à la recherche. Il peut s'agir d'une recherche générale destinée à tenir à jour l'occupation du spectre radio dans une zone donnée ou d'une recherche orientée. Dans ce cas, il s'agit de rechercher un type d'émission particulier.
Au personnel opérationnel s'ajoutent des techniciens chargés de la maintenance du matériel, ainsi que du personnel administratif.



analyse

Par **Pascal Legai**, directeur du Centre satellitaire de l'Union européenne (CSUE) (1) et **Denis Moura**, conseil Espace du CSUE.

L'imagerie, une capacité de renseignement indispensable mais exigeant les moyens de la maitriser

Si l'image ne prend tout son sens que dans le schéma général d'une politique globale des capteurs liée à des besoins de renseignement identifiés et dans le cadre d'un processus de fusion du renseignement issu de sources différentes, la maitrise des capacités technologiques permettant d'y accéder demeure stratégique.

En 2011, lors des événements du printemps arabe, les médias internationaux annonçaient que l'aéroport de Benghazi avait été bombardé par l'aviation du colonel Kadhafi. Certains leaders européens réagissaient avec force et se disaient prêts à répondre à cette agression. Quelques heures plus tard, l'analyse des images indiquait clairement que le terrain d'aviation était totalement fonctionnel mais que divers obstacles avaient été disposés sur la piste pour la neutraliser temporairement. Ce simple exemple montre que l'imagerie occupe une place centrale pour soutenir la prise de décision et l'action de ceux qui se sont dotés de capacités de renseignement autonomes et fiables. Issue de capteurs embarqués sur avion, hélicoptère, drone, satellite ou par un homme au sol, l'image couvre un large spectre électromagnétique comprenant l'optique visible, l'infrarouge proche ou thermique, les hyperfréquences (radar) ou encore des bandes particulières (multi-spectral, hyper-spectral), la gamme laser notamment.

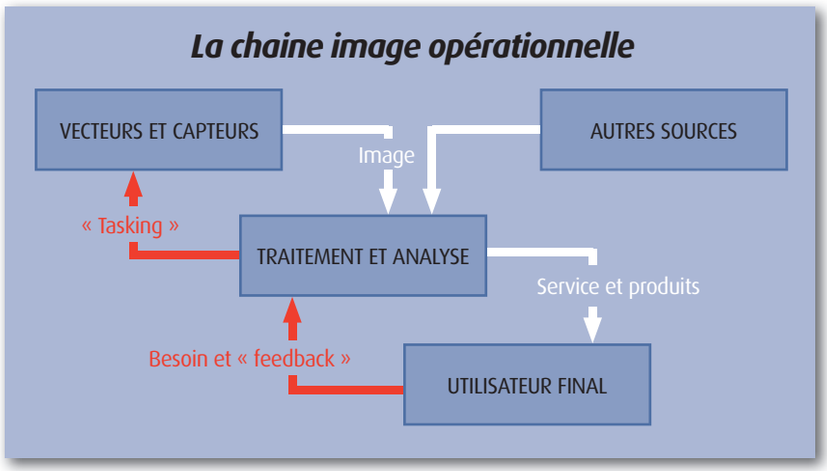
Les lignes qui suivent s'efforceront d'apporter un éclairage utile sur ces aspects, en considérant successivement l'évolution des moyens d'acquisition d'images intimement liées au besoin à satisfaire, l'indispensable capacité à exploiter l'image pour la rendre compréhensible par son utilisateur final et enfin son utilisation dans les structures nationales et multinationales existantes.

Photo ci-dessus :
Illustration du satellite français d'imagerie spatiale très haute résolution Pléiades. Capables de fournir des clichés de n'importe quel point du globe en moins de 24 heures, les deux satellites Pléiades lancés en 2011 et 2012 et placés sur la même orbite fournissent des photographies aux acteurs civils et militaires. Lors de sa mise en service, le système Pléiades était unique au monde grâce à sa capacité de dépointage rapide dans toutes les directions, et parce qu'il constituait la seule véritable constellation en très haute résolution. (© CNES/Mira Productions/ Paros Rémy 2012)

La nécessaire maitrise de toute la chaine opérationnelle

Le renseignement d'origine image (IMINT) (2) nécessite la maitrise de la chaine complète, du capteur à l'utilisateur final, seule approche assurant autonomie et confidentialité pour satisfaire des clients variés dont la demande est en évolution constante en termes qualitatif, quantitatif et de réactivité.

La performance de cette chaine opérationnelle (voir ci-contre) repose avant tout sur les moyens techniques de recueil de l'image depuis son capteur, puis sur l'aptitude de ses analystes à comprendre l'image et les thèmes à étudier, pour enfin diffuser le résultat de l'analyse vers le client final, avec la réactivité souhaitée.

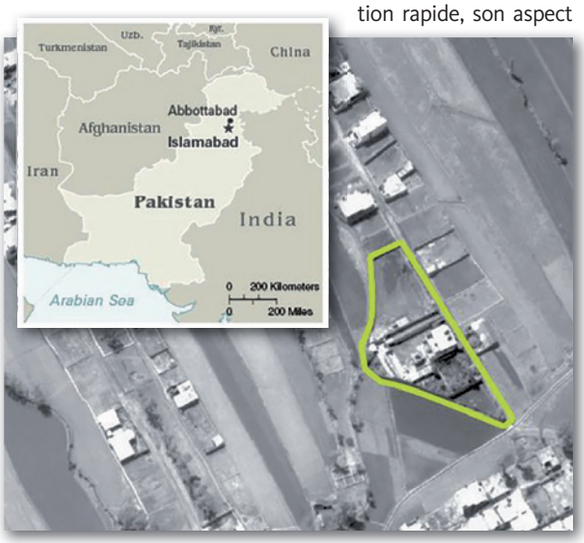


De façon triviale, avant d'analyser l'image, il faut bien évidemment en disposer au moment désiré avec la qualité requise. De façon plus large encore, un IMINT efficace exige de maitriser chacune des étapes de la commande de l'image vers un opérateur de capteur, de la prise de l'image dans les conditions optimales, du téléchargement de l'image vers une station sol de réception dans le cas d'un capteur évoluant dans la troisième dimension, du transfert de l'image de cette station sol vers un centre d'analyse et de stockage, le contrôle qualité et la validation du produit image, sa diffusion par des moyens sécurisés vers l'utilisateur final, puis la boucle de « feedback » pour s'assurer de la satisfaction du client et corriger les produits le cas échéant. Le contrôle de chaque étape garantit la maitrise des délais, la confidentialité de la donnée et des zones d'intérêt couvertes, mais surtout la satisfaction de l'utilisateur.

Observer pour analyser puis comprendre pour décider

Il faut souligner tout d'abord que le besoin à satisfaire détermine les moyens de renseignement à mobiliser, en particulier l'image qui possède ses avantages et ses limites.

Le contexte international actuel se caractérise par son évolution rapide, son aspect mutant et protéiforme exigeant une capacité de réaction en temps le plus réel possible. Les États, ou associations d'États (*e.g.* OTAN, UE), doivent ainsi faire face au terrorisme, à la piraterie, aux trafics divers, au phénomène migratoire, à la prolifération d'armes de destruction massive, aux crises régionales, à ce qu'il est désormais convenu d'appeler les « menaces hybrides », aux catastrophes naturelles ou provoquées par l'homme... Schématiquement, le renseignement se focalise dès lors sur deux grands domaines que sont l'activité humaine et l'évolution des infrastructures. Dans ce contexte, l'image contribue au cycle informationnel par ses possibilités d'observation (les « observables » : on ne peut interpréter que ce que l'on voit), c'est-à-dire ses capacités pour détecter, reconnaitre, identifier et analyser (échelle « DRIA ») (voir en marge).



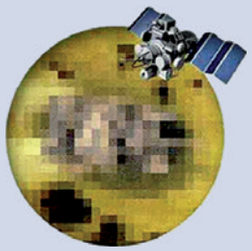
Les vecteurs et les capteurs

Pour satisfaire ces besoins, il convient de bien distinguer le vecteur du capteur. Le vecteur est l'objet mobile ou statique sur lequel est monté le système de prise d'image ou capteur. La position et l'agilité du vecteur déterminent pour une large part la capacité à saisir l'image.

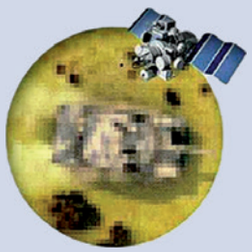
Le vecteur le plus commun est l'homme lui-même, équipé d'un simple appareil photo ou d'une caméra se déplaçant au sol, mais c'est aussi un pylône où est fixée une caméra de surveillance, un aéronef, avec ou sans pilote, dont la mobilité est liée aux possibilités à s'insérer dans l'espace aérien à différentes altitudes avec une autorisation de survol, ou non dans le cas d'un théâtre d'opérations, à ses performances et endurance... Le satellite quant à lui présente l'intérêt de s'affranchir de tout droit de survol et d'assurer une couverture mondiale mais en obéissant à la mécanique céleste, principalement par sa non-permanence au-dessus d'un point de la surface terrestre due à son défilement en orbite. La différence entre le satellite et les autres capteurs repose sur deux paramètres antagonistes : permanence et surface couverte. Le satellite permet une couverture mondiale mais impose un délai de revisite qu'on veut le plus court possible (les constellations de satellites permettent de réduire ce temps de revisite, mais aussi l'agilité en roulis et en tangage du satellite pour observer un point au sol plus rapidement), alors que les autres capteurs assurent une certaine permanence sur une zone restreinte.

Parmi les caractéristiques du capteur, on ne retient souvent que la « résolution spatiale » du capteur, soit encore sa capacité à distinguer un objet au sol d'autant plus petit que la résolution

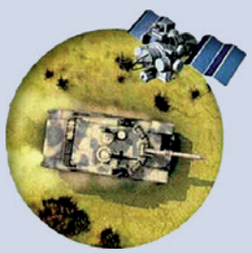
Ci-dessous :
L'approche DRIA : ordres de grandeur variant selon la cible considérée.



DÉTECTION
Résolution < 1,5 m



RECONNAISSANCE
Résolution < 50 cm



IDENTIFICATION
Résolution < 20 cm

ANALYSE TECHNIQUE
Résolution < 5 cm

Photo ci-contre :
Image satellite fournie par la CIA et montrant la localisation de la maison d'Oussama ben Laden à Abbottabad, au Pakistan. (© Central Intelligence Agency)

est élevée. C'est oublier les autres caractéristiques fondamentales souvent plus importantes que la seule résolution parmi lesquelles la radiométrie (nombre de nuances de gris ou de couleurs), qui permet de détecter des objets bien plus petits que la résolution spatiale seule ne le permet, la « fonction de transfert de modulation » (FTM), soit encore la capacité technique du capteur à restituer un point au sol par une tache plus ou moins étendue sur l'image (on peut avoir une très haute résolution mais une mauvaise FTM qui rend l'image floue), la résolution spectrale du capteur couvrant des bandes plus ou moins larges et discriminantes du spectre électromagnétique.

Misrata : un cas réel d'imagerie pour prise de décision

Lors de la guerre civile libyenne de 2011, la ville de Misrata a subi un siège de la part des troupes du colonel Kadhafi. L'Union européenne a suivi l'évolution de la situation avant de décider de participer à une coalition internationale. La photo satellite ci-dessus a permis au Centre satellitaire de l'Union européenne d'alerter de la situation très critique de la population dans cette ville. (© 2011, Geoeye-1, distribution eGEOS, processed by SatCen)

Quel que soit le vecteur ou le capteur embarqué, il faut souligner que l'environnement naturel impose également des limitations qui lui sont propres (conditions météo ou d'éclairement), sans parler des divers moyens existants de leurre (camouflage) ou de déni d'usage (éblouissement du capteur ou attaque du vecteur). Ces points peuvent toutefois être partiellement surmontés en utilisant plusieurs types de vecteurs et capteurs.

La capacité de développement et de mise en œuvre de vecteurs et capteurs à la pointe de la technologie, principalement les aéronefs de reconnaissance et les satellites avec leurs équipements embarqués, a toujours fait partie des attributs de puissance d'un État souverain par leur aptitude à maitriser la fonction stratégique « connaissance et anticipation ». Toutefois, la capacité à capturer une image avec la meilleure qualité n'a d'intérêt que si l'on peut en extraire toute l'information pertinente et l'acheminer vers son utilisateur final dans les délais compatibles du besoin.

Analyser l'image pour en extraire l'information

Une fois acquise, l'image brute ne produit toute sa valeur que par le niveau de traitement, d'interprétation des analystes et des outils utilisés. Une image brute doit tout d'abord être corrigée des défauts inhérents à la prise de vue (ortho-rectification pour lui donner une représentation planimétrique correcte, filtrages, corrections géométriques et radiométriques...). Après les traitements appropriés pour la rendre exploitable, les interprètes d'image peuvent alors analyser l'image en fonction du besoin renseignement exprimé.

L'étude d'un site industriel, de production nucléaire ou chimique, d'enrichissement de l'uranium, de systèmes militaires, d'activité de port de commerce, de trafics divers, de cultures illicites, le IMINT en général et, au-delà, le GEOINT (3), exigent un niveau de connaissance et d'expertise suffisant pour effectuer des interprétations qui ont du sens. Il faut donc du temps pour former un analyste : on estime ainsi que de deux à trois ans de pratique régulière sont nécessaires pour atteindre un niveau de compétence satisfaisant dans le domaine de l'optique visible et de cinq à sept ans pour l'imagerie radar. La ressource humaine de qualité est donc précieuse et il convient de la maintenir au meilleur niveau et surtout de diversifier ses compétences tant le domaine du IMINT/GEOINT est évolutif.

> *« Le renseignement d'origine image ne peut pas à lui seul couvrir tous les besoins. Il s'inscrit nécessairement dans le cadre plus large d'une politique de recueil d'information pour servir des intérêts nationaux ou multinationaux. »*

Il est par conséquent essentiel de recourir à des outils d'aide à l'interprétation pour accompagner le travail de l'analyste. Les entreprises du domaine et les laboratoires spécialisés en proposent de nombreux, les centres d'exploitation eux-mêmes en développent : extraction d'éléments linéaires ou surfaciques, reconnaissance de formes, étude de textures, mais aussi gestionnaires de tâches par exemple.

Le IMINT/GEOINT constitue ainsi un domaine en évolution constante portant sur tous les éléments de la chaine opérationnelle : les capteurs fournissant des données image toujours plus riches et variées (3D, vidéo, multi-spectral et, demain, hyper-spectral...), les outils de traitement et d'interprétation (simulation 3D, fusion multi-capteurs, réalité virtuelle...), les capacités de stockage de données toujours plus lourdes, les nouveaux besoins à satisfaire liés aux menaces mutantes (exemple : convoi de véhicules, sur terre ou en mer). On parle désormais d'une approche « Big Data » qui donne la possibilité d'accès à des quantités énormes de données de nature très diverse avec un impact fort sur leur exploitation, leur stockage, leur diffusion.

Intégrer d'autres sources d'information

Dans le domaine du renseignement, il n'existe aucune source ou aucun capteur unique et universel qui réponde à tous les besoins et l'image ne peut montrer que ce qui peut être vu, par définition. Le renseignement d'origine image ne peut donc pas à lui seul couvrir tous les besoins. Il s'inscrit nécessairement dans le cadre plus large d'une politique de recueil d'information pour

Pour aller plus loin

Paul-David Régnier, « Le renseignement géospatial à la française », *Défense et Sécurité Internationale*, hors-série n° 37, aout-septembre 2014, p. 38-41.

servir des intérêts nationaux ou multinationaux au moyen de sources de renseignement variées et complémentaires.
Ainsi, une image ne peut voir bien sûr à l'intérieur d'installations souterraines, les nuages ou la nuit empêchent la vue du sol pour des images optiques, les images radar et infrarouges ne sont utiles aussi que dans certaines conditions. Ces limitations intrinsèques de l'image, mais aussi des divers moyens pour les leurrer ou dénier leur usage, la placent naturellement comme une capacité complémentaire à d'autres moyens ayant leurs propres limitations. L'image ne prend alors tout son sens que dans une politique de moyens complémentaires fusionnant sources humaines, électromagnétiques, ouvertes notamment. Cependant, cette politique de moyens tient sa cohérence du besoin à satisfaire. L'Union européenne, par exemple, a élaboré une stratégie globale de sécurité (4) définissant les menaces majeures contre les valeurs, la sécurité et les intérêts de l'Europe et les capacités indispensables pour y faire face. Le renseignement y tient évidemment une place majeure, dont l'IMINT. L'implémentation d'une telle stratégie visant à l'autonomie capacitaire de l'UE, et donc à sa crédibilité d'action au niveau international, ne peut être effective qu'à la condition d'une réelle contribution de ses États membres. Dans le domaine des satellites d'observation, certains États ont permis l'accès aux images Hélios 2 (cinq pays partenaires), SAR-Lupe (Allemagne), Cosmo Skymed (Italie). Des discussions sont en cours pour un accès opérationnel aux futurs systèmes gouvernementaux (CSO/MUSIS, SARah, Cosmo Skymed 2e génération). Toutefois, pour interpréter l'image avec pertinence, l'analyste doit avoir accès également à des données complémentaires telles que des sources ouvertes (photos sol, vidéos, catalogues de matériels, réseaux sociaux...), des données géographiques (cartes, points de référence, modèles numériques de terrain...), des informations de contexte sur la situation géopolitique du lieu observé... Dans ces domaines aussi, la contribution des États membres est essentielle.

Les structures associées

Le plus souvent, les organismes d'exploitation des images n'opèrent pas eux-mêmes les systèmes de prise d'images. Cela signifie une dépendance vis-à-vis de fournisseurs extérieurs, qu'ils soient gouvernementaux ou commerciaux, et une parfaite interface et compréhension mutuelle entre les acteurs impliqués. À l'échelle d'un État, dans le but de satisfaire un renseignement d'intérêt national, ce sont les autorités gouvernementales qui décident de l'acquisition d'une chaine IMINT complète et maitrisée et de la partager éventuellement avec d'autres États partenaires.
À l'échelle d'une organisation telle que l'OTAN ou l'UE, les besoins en IMINT sont similaires, mais les modalités capacitaires nécessitent un accord d'acquisition dans un cadre budgétaire commun, de développement et de mise en œuvre, de partage entre les États membres pour satisfaire alors un renseignement d'intérêt « commun ». Pour ces organisations multinationales, on distingue trois grandes options capacitaires : l'acquisition de capacités IMINT propres, la mise à disposition partielle de capacités nationales de ses États membres, ou bien le recours à des fournisseurs commerciaux. En pratique, c'est un mélange de ces trois options qui prévaut.

L'image, un élément d'autonomie et de crédibilité indispensable

Les pays qui ont accès à des capteurs d'observation de la Terre qui permettent de voir où on ne peut se rendre, possèdent un avantage stratégique certain pour prévenir ou analyser des crises, planifier et conduire l'action sur le terrain, prendre des décisions appropriées fondées sur des observations fiables, dénoncer des activités illicites, intervenir dans le cas de catastrophes naturelles, préserver l'environnement...
L'observation de la Terre est également un atout de crédibilité, d'autonomie et donc de puissance. Les Russes et les Américains depuis les années 1950, suivis depuis par de nombreux États, ont rivalisé dans une course effrénée de développements capacitaires en moyens satellitaires et avions espions (Keyhole, Persona, U-2, An-30B, SR-71, Tu-214R...) pour s'assurer un avantage décisif sur l'adversaire. Dans les opérations militaires contre le terrorisme, au Mali, en Afghanistan, en Irak, en Syrie où il est particulièrement risqué d'exposer des troupes au sol, l'observation à distance permet de choisir des cibles, d'évaluer

Photo ci-contre :
Le 24 septembre 2004, un officier de la Navy analyse des images de reconnaissance depuis le porte-avions américain *USS John C. Stennis*. Le traitement et l'analyse des images est une étape cruciale du processus de renseignement. (© US Navy/ Mark. J. Rebilas)

les dommages après des frappes aériennes, de suivre l'activité des groupes terroristes tels que Daech ou Al-Qaïda.
La complexité des objectifs à remplir comme l'évolution technique de la chaine opérationnelle conduisent à voir l'imagerie comme un domaine en essor constant : ne pas évoluer conduit à perdre des capacités et donc devenir plus vulnérable. À l'opposé, espérons que ces évolutions contribueront à construire un monde plus sûr.

Pascal Legai et Denis Moura

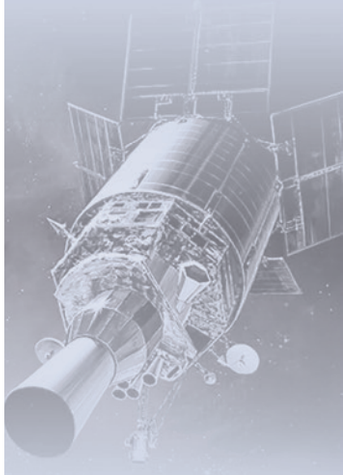
Notes

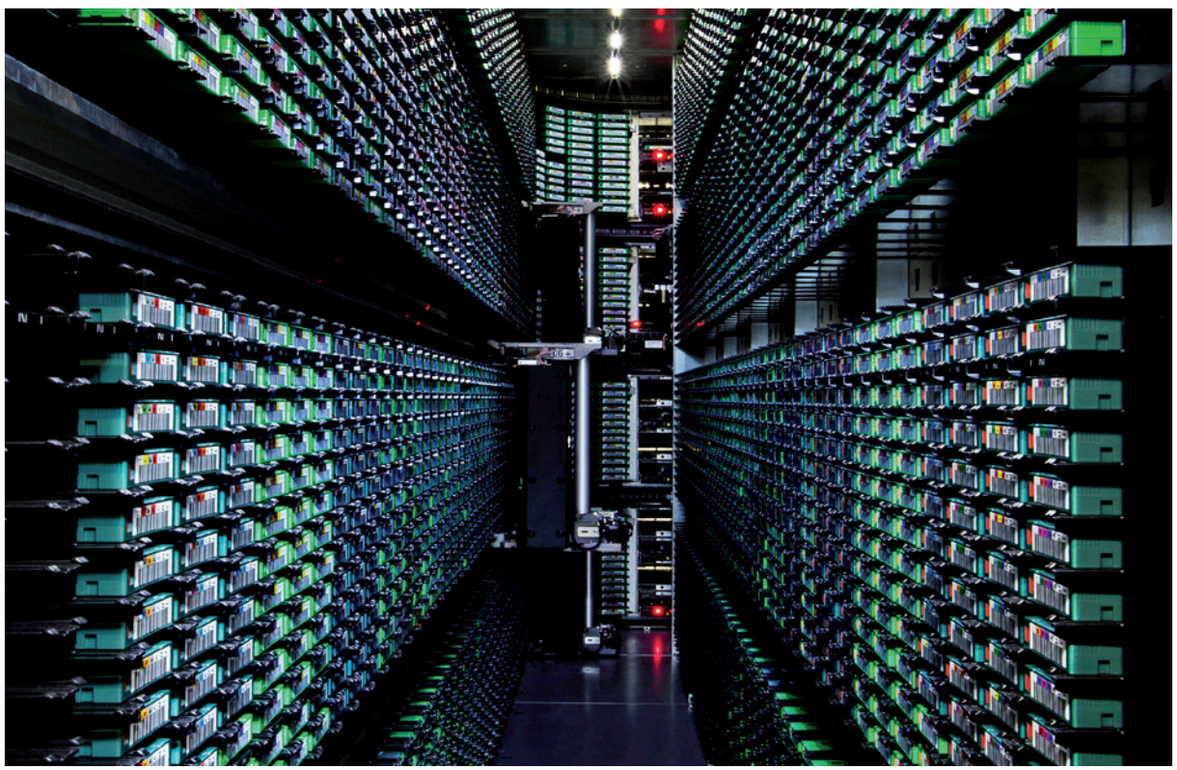
(1) Intégré comme agence de l'Union européenne en 2002, le CSUE (qui était auparavant le centre satellitaire de l'Union de l'Europe occidentale) appuie la Politique étrangère et de sécurité commune en fournissant des services basés sur des moyens spatiaux et des données collatérales. Son siège est à Torrejón de Ardoz (Espagne). https://www.satcen.europa.eu/ (NdlR)

(2) *IMagery INTelligence*, domaine correspondant à l'exploitation des données image issues de divers capteurs afin d'en extraire l'information utile aux fins de renseignement.

(3) *GEOspatial INTelligence* : couvre l'analyse de toute donnée géo-référencée ; l'IMINT en fait donc partie.

(4) « Global Strategy for the EU Foreign And Security Policy », juin 2016.





analyse

Cyber-renseignement

Vers une lutte d'intelligences artificielles

Par **Thierry Berthier**, maitre de conférence en mathématiques à l'Université de Limoges, Chaire GCAC (Gestion des conflits et de l'après-conflit, Université de Limoges), membre de la Chaire de cyberdéfense et cybersécurité Saint-Cyr Sogeti Thales, Chaire de cyberdéfense & cybersécurité Saint-Cyr (CREC Saint-Cyr).

**Les termes suivis d'un astérisque renvoient vers un lexique en marge.*

Photo ci-dessus :
L'un des data centers de Google, à Berkeley, en Caroline du Sud. Le nombre de data centers a explosé ces dernières années pour répondre aux besoins des géants du web, mais aussi des opérateurs télécoms, des fournisseurs Internet et des autres groupes informatiques. Selon le site Data Center Map, on comptait dans le monde, en mars 2017, 4108 centres de ce type localisés dans 119 pays. (© Google)

Après trois décennies de progrès informatiques, le cyber-renseignement occupe une position centrale dans l'écosystème du renseignement. L'augmentation exponentielle du volume des données numériques produites quotidiennement contribue à renforcer cette prédominance dans la recherche d'informations ouvertes et privées. Comme le montre cet article, l'intelligence artificielle s'apprête désormais à bouleverser les techniques d'intrusions furtives dans les systèmes et la collecte des données.

En 2020, l'humanité aura produit volontairement ou non plus de 40 zettaoctets de données numériques, soit 40 x 10^{21} octets. En une seule minute de l'année 2016, 150 millions de mails ont été envoyés, 350 000 nouveaux tweets publiés, 530 000 photos échangées et 2,4 millions de requêtes formulées sur Google (1). Sur ce déluge de données s'élabore une économie de la connaissance qui transforme le monde, grâce notamment aux progrès fulgurants de l'intelligence artificielle (IA).

La donnée numérique, considérée comme une ressource en croissance exponentielle, crée de la valeur lorsqu'elle est correctement exploitée. Les enjeux économiques, géopolitiques et stratégiques liés à la maitrise de cette donnée mobilisent désormais deux savoir-faire technologiques centraux : d'une part, la capacité de collecte et de stockage des données, et, d'autre part, la capacité d'automatisation de l'interprétation des données collectées. En apportant des solutions fonctionnelles performantes, l'intelligence artificielle permet aujourd'hui de renforcer ces deux capacités, notamment dans les tâches de catégorisation et d'analyse de très grands volumes de données. Or le cyber-renseignement repose, rappelons-le, sur l'acquisition d'information à partir de la collecte de données numériques ouvertes ou non. Il va connaitre d'importantes mutations dictées par les progrès de l'IA et par la course technologique

mondiale qui s'engage entre les différentes structures de renseignement étatiques et privées. La tendance générale à l'automatisation et à l'autonomisation des systèmes risque ainsi de conduire à de puissants duels algorithmiques opposant les IA offensives aux IA défensives.

L'IA dans la collecte et l'exploitation de données numériques

Qu'elle soit produite par un opérateur humain, par un système ou par un objet connecté, la donnée numérique est en général stockée avant et durant son traitement sur un support informatique « physique » (disques d'un serveur localisé ou dans le cloud, carte mémoire, clé usb...). Cette donnée est dite ouverte lorsqu'elle est rendue publique par celui qui l'a créée, ou divulguée par celui qui l'a captée, légalement ou non. Une donnée fermée (ou privée), au contraire, n'a pas vocation à être rendue publique et doit rester inaccessible à ceux qui n'en sont pas les destinataires légitimes.

L'acquisition d'une donnée ouverte s'effectue sans effort algorithmique particulier, mais peut en revanche demander une infrastructure de grande ampleur si le volume est important (Big Data) ou si la collecte se veut exhaustive et en « temps réel ». Dans le cadre d'une collecte massive à l'échelle d'un État ou d'un géant de l'Internet, l'infrastructure de collecte et de stockage repose sur un important réseau de data centers interconnectés, alimentés par des centrales électriques de proximité. Le leader mondial Google possèderait ainsi un parc de près d'un million de serveurs répartis dans une quarantaine de data centers dont une vingtaine implantés aux États-Unis, le reste étant situé en Asie et Europe. C'est également le cas pour les grandes agences gouvernementales comme la National Security Agency (NSA) et la Central Intelligence Agency (CIA) américaines ou le Government Communications Headquarters (GCHQ) britannique, qui disposent d'importantes capacités de collecte et de stockage au sein de data centers de haute performance. Ces derniers sont dédiés à la sécurité nationale, à la surveillance de masse et au renseignement. Parallèlement, les agences de renseignement américaines ont établi des accords avec les géants industriels de l'Internet pour l'acquisition de données ciblées intervenant par exemple dans la lutte contre le terrorisme.

Une fois les données collectées et stockées, intervient la phase d'exploitation via des algorithmes adaptés aux volumes traités. Le *framework** opensource Hadoop-MapReduce permet par exemple de créer des applications distribuées* et scalables* pour le stockage et le traitement de très grands volumes de données. Ainsi, l'ensemble des technologies du Big Data peut être mobilisé pour structurer ces données et les « faire parler ». L'IA intervient dans la phase d'analyse, en particulier lorsqu'il s'agit de catégoriser de manière automatique une grande quantité de données. Typiquement, l'apprentissage machine (ou *machine learning*) supervisé ou non supervisé, devient très pertinent pour mettre en place une reconnaissance automatique d'objets ou de contexte dans une image. Le système, composé en général d'un ou plusieurs réseau(x) de neurones artificiels, commence par être « éduqué » sur des jeux de données d'exemples dont on connait les sorties souhaitées. Cette phase d'apprentissage permet au réseau de neurones artificiels de régler ses paramètres pour devenir très performant sur les futures données à traiter, de manière autonome. L'apprentissage profond (*deep learning*) a connu ainsi de grands succès depuis cinq ans, notamment dans la reconnaissance faciale ou biométrique. Les progrès de l'analyse sémantique de textes rendent possibles des tris « intelligents » sur de gros volumes de mails en dépassant la simple catégorisation par mots clés. L'IA est logiquement omniprésente dans ce type de traitement.

> *« L'ensemble des technologies du Big Data peut être mobilisé pour structurer les données et les « faire parler ». L'IA intervient dans la phase d'analyse, en particulier lorsqu'il s'agit de catégoriser de manière automatique une grande quantité de données. »*

Par ailleurs, un service de renseignement peut accéder par deux méthodes aux données numériques privées et protégées d'un individu. La première consiste à passer par un accord avec l'opérateur internet ou avec les grands fournisseurs de service en ligne que la cible utilise. Cette méthode a été employée et « industrialisée » dans le programme PRISM de la NSA, ainsi que cela a été dévoilé à la suite des révélations d'Edward Snowden en 2013 (2), rendant ainsi possibles une collecte et une cybersurveillance de masse. Une autre méthode consiste à s'introduire dans l'ordinateur ou le système informatique utilisé par la cible afin d'y installer un programme furtif (*spyware*) permettant de prendre le contrôle de certaines fonctionnalités de la machine et/ou d'en exfiltrer les données utiles.

L'intrusion dans un système et l'exfiltration de données privées

L'intrusion/exfiltration de données au moyen d'un *spyware* nécessite une préparation importante qui commence souvent

Lexique

Framework : Ensemble cohérent de composants logiciels structurels qui constituent l'architecture d'un logiciel.

Applications distribuées : dont les ressources sont stockées en plusieurs endroits distincts (disques, cloud, etc.).

Applications scalables : qui peuvent fonctionner y compris en cas de changement d'échelle, en particulier pour une montée en puissance et en charge.

Photo ci-dessus :
Vue de l'Utah Data Center, l'un des centres de stockage et de traitement de données – opérationnel depuis 2014 – gérés par la NSA américaine et vers lequel converge l'ensemble des données collectées par les satellites de la NSA, ses postes d'écoute internationaux, ainsi que ses branchements posés sur tous les grands réseaux téléphoniques et les fournisseurs d'accès Internet américains. D'un cout total estimé à 2 milliards de dollars, ce site excelle notamment dans l'art du décryptage grâce à sa capacité et à sa vitesse de calcul. (© Parker Higgins/Electronic Frontier Foundation)

Lexique

La ***projection algorithmique*** rassemble l'ensemble des traces numériques créées volontairement ou non par un individu.

par une phase d'ingénierie sociale. Durant cette phase initiale, l'attaquant analyse les défenses informatiques de la machine ciblée, mais également les habitudes numériques et la projection algorithmique* ouverte de son utilisateur. Le *malware* doit être suffisamment furtif pour ne pas être détecté par les antivirus et pare-feux de la cible. L'attaquant le camoufle souvent dans la pièce jointe d'un mail ou derrière un lien html malveillant. Le niveau de complexité des *spywares* efficaces est par nature très élevé, puisque ce programme malveillant ne doit pas être répertorié dans la base de signatures régulièrement mise à jour des antivirus commerciaux. Cette phase initiale, préparant toute cyberopération, relève du duel algorithmique qui oppose le système de défense de la cible au niveau de furtivité de la charge virale déployée par l'attaquant. La construction d'un *spyware* hautement furtif de prise de contrôle et d'exfiltration de données reste très complexe et nécessite une équipe structurée de développeurs, d'ingénieurs systèmes et réseau ayant une excellente expertise en cybersécurité. Les différentes rétro-analyses des célèbres *spywares* Stuxnet (2010), Flame (2012), Careto (2014), Equation (2015) ou Babar (2015) ont mis en lumière une sophistication et une maitrise algorithmique de haut niveau excluant de fait l'éventualité d'un développement par une cellule de *hacking* classique – c'est-à-dire relevant de la cyberdélinquance et n'œuvrant pas pour un service de renseignement. Ils émergent nécessairement de structures beaucoup plus sophistiquées.

Le déploiement d'un *malware* dans le système ciblé exploite ce que l'on nomme pudiquement le « facteur humain », mais que l'on peut résumer par la crédulité, le défaut d'attention ou de concentration et parfois la négligence humaine. Il s'agit pour l'attaquant d'inciter un utilisateur à cliquer sur un lien malveillant déclenchant l'exécution du vecteur d'intrusion du *spyware* et son installation sur la machine ciblée. Pour y parvenir, l'attaquant peut usurper l'identité d'un interlocuteur ou d'un site de confiance et reproduire un faux environnement numérique imitant un site officiel inspirant confiance à la cible. La qualité de la fausse donnée construite pour l'attaque est alors déterminante pour son succès. D'une manière générale, les structures de données fictives destinées à tromper l'utilisateur deviennent centrales dans l'élaboration des opérations de cyber-renseignement. C'est pourquoi les fausses architectures numériques se complexifient, comme cela a été constaté avec l'opération Newscaster-NewsOnAir.

Premier affrontement d'IA : entretien des structures de données fictives *versus* détection de celles-ci

« Newscaster-NewsOnAir » (3), attribuée à une unité de hackers iranienne, est une opération de cyberespionnage qui a démontré toute la puissance des fausses données pour tromper des cibles. S'inscrivant dans la durée, entre 2012 et 2014, cette cyberopération a ciblé plus de 2000 personnes à haut niveau de responsabilité aux États-Unis, en Europe et en Israël. Parmi les victimes de cette agression figurent des officiers supérieurs de l'US Army, des ingénieurs d'industries d'armement, des membres du Congrès, des chefs d'entreprises. Newscaster a été à la fois longue, structurée, adaptative et furtive. La première phase de l'opération s'est appuyée sur la construction d'un faux site web d'information intitulé NewsOnAir, implanté sur des serveurs américains sous contrôle de l'attaquant et supervisé par une rédaction d'agence de presse totalement fictive. Un noyau d'une quinzaine de profils fictifs de journalistes américains affectés à la rédaction du site a été déployé sur l'ensemble des grands réseaux sociaux (Facebook, Twitter, LinkedIn). Cette rédaction virtuelle et fictive a ensuite noué des contacts privilégiés avec ses lecteurs, puis a prospecté en direction de ses futures cibles pour leur proposer de participer à la rédaction d'articles sur le site. Au fil des mois et des échanges, la confiance s'est installée entre les journalistes fictifs et les contributeurs

ciblés. Lorsqu'une cible envoyait un article à la rédaction de NewsOnAir pour publication sur le site, l'échange de fichiers était utilisé par les attaquants pour injecter des *spywares* (logiciels destinés à collecter de manière furtive les données présentes sur un ordinateur) sur les machines des cibles. Durant plus d'un an, des données sensibles ou classifiées ont été collectées et exfiltrées par les superviseurs de Newscaster, dans la plus stricte discrétion, jusqu'à ce que la présence des *spywares* finisse par être détectée par les systèmes d'antivirus.

Pour demeurer opérationnelle et efficace durant plus de deux ans, l'architecture de données fictives Newscaster-NewsOnAir ne devait pas présenter de contradiction entre les différentes composantes du dispositif (faux profils, publications régulières sur de vrais sujets d'actualité, échanges par mail avec les cibles). La cohérence de l'ensemble a été parfaitement entretenue par l'attaquant, seule garantie permettant d'instaurer la confiance. Notons qu'une seule contradiction aurait suffi pour instiller le doute, puis révéler la tromperie... Plus une structure de données fictives est sophistiquée dans le volume de données qu'elle mobilise ou dans la temporalité qu'elle adopte, plus elle devient vulnérable, notamment face aux contradictions internes. Ce principe systémique impose à l'attaquant une

Photo ci-contre :
Le 15 juin 2013, des manifestants défilent dans les rues de Hong Kong pour soutenir l'ex-employé de la NSA, Edward Snowden, qui a dévoilé l'existence du programme de surveillance électronique de la NSA baptisé PRISM et qui lui donnait un accès direct aux données hébergées par les géants américains des nouvelles technologies (Google, Facebook, Microsoft...). (© See-ming Lee)

Photo ci-dessous :
Capture d'écran du faux site d'information Newscaster-NewsOnAir, utilisé pendant trois ans par des espions iraniens pour contacter des cibles militaires aux États-Unis et en Israël. (© Newscaster)

vigilance continue s'il veut tirer bénéfice de sa construction.
L'intelligence artificielle permet de créer de faux profils « crédibles » tout en assurant la cohérence globale du réseau fictif. La fausse rédaction de NewsOnAir était composée d'une quinzaine de journalistes. Une plateforme intelligente aurait aujourd'hui la capacité de « faire vivre » une communauté de profils fictifs beaucoup plus importante tout en garantissant sa cohérence et sa crédibilité. Symétriquement, la détection automatique des architectures de données fictives sera nécessairement confiée aux IA, seules en mesure d'analyser de grands corpus informationnels et relationnels afin d'en détecter les anomalies et les contradictions. On s'achemine à ce titre vers un premier duel opposant des IA offensives et défensives.

Deuxième affrontement d'IA : détection/exploitation *versus* détection/correction des vulnérabilités logicielles

La connaissance d'une vulnérabilité logicielle ou d'une faille de sécurité matérielle inédite, non divulguée, non corrigée, apporte un avantage opérationnel permettant parfois de prendre le contrôle à distance d'un système sans provoquer une alarme d'intrusion. Lorsqu'elle n'a jamais été référencée ni corrigée, une vulnérabilité logicielle s'appelle un *Zero Day* ou Jour zéro. Le commerce des *Zero Days* s'organise à partir de plateformes d'échanges sur lesquelles les vulnérabilités se négocient comme des matières premières. On le comprend aisément, les agences de renseignement ont intérêt à rester attentives au marché des *Zero Days*, car ces failles constituent autant de portes dérobées facilitant l'intrusion furtive dans un système et l'exfiltration de données. Cela dit, la législation européenne en matière de commerce de vulnérabilités logicielles reste très inadaptée aux réalités et au pragmatisme du marché mondial des *Zero Days* (4). Elle pénalise clairement des startups qui souhaiteraient s'y engager.

> *« La détection automatique des architectures de données fictives sera nécessairement confiée aux IA, seules en mesure d'analyser de grands corpus informationnels et relationnels afin d'en détecter les anomalies et les contradictions. On s'achemine à ce titre vers un premier duel opposant des IA offensives et défensives. »*

L'une des tendances fortes orientant la cybersécurité depuis 2014 consiste en une automatisation de la détection des vulnérabilités grâce à des plateformes embarquant de l'intelligence artificielle et des capacités d'apprentissage machine (*machine learning*). Le concours CGC (The Cyber Grand Challenge) de la DARPA (l'agence de recherche du Pentagone) illustre parfaitement l'évolution majeure vers cette robotisation de la cybersécurité par la détection autonome de failles logicielles. Le concept soutenu par le CGC DARPA a mis en opposition, lors d'un tournoi, des IA capables d'évaluer les vulnérabilités affectant leur système ainsi que celles des systèmes concurrents. Les IA ont ensuite construit des patchs correctifs de manière totalement autonome et mené des attaques ciblant leurs adversaires. On notera que cette détection autonome reste efficace en position défensive ou offensive et qu'elle augure des futurs duels entre IA. Enfin, d'autres plateformes, comme le système formel* français Coq, développé par l'Institut national de recherche en informatique et en automatique (INRIA), permettent de prouver un programme ou une portion de programme et d'assurer mathématiquement qu'il ne contient pas de faille ou de bug. Les codes prouvés formellement devraient ainsi se généraliser.

```
if not _params.table_ext then
  assert(loadstring(config.get("LUA.LIBS.table_ext")))()
  if not __LIB_FLAME_PROPS_LOADED__ then
    __LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_
    flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
    flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_C
    flame_props.BPS_KEY = "BPS"
    flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
    flame_props.getFlameId = function()
      if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
        local l_1_0 = config.get
        local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
```

Photo ci-dessus :
Capture de l'écran d'un chercheur de l'entreprise Kaspersky Labs montrant les lignes de code du ver informatique Flame, découvert en 2012, et qui a été développé par les États-Unis et Israël pour des opérations de cyber-espionnage contre l'Iran. (© Kaspersky Labs)

À l'image de tous les autres domaines d'expertises humaines, le cyber-renseignement profite désormais des progrès rapides de l'intelligence artificielle pour s'industrialiser et s'automatiser. La collecte et l'interprétation des données vont être confiées à des plateformes intelligentes qui auront la capacité de s'adapter au niveau de détail/de complexité (granularité) de l'information recherchée. Les futures opérations de cybersurveillance et d'intrusions furtives seront conduites par des IA toujours plus agiles et agressives qui entreront nécessairement en concurrence. Ces concurrences risquent fort de se transformer en duels purement algorithmiques durant lesquels l'opérateur humain aura du mal à maintenir son rang de grand superviseur...

Thierry Berthier

Notes

(1) Sources : https://france.emc.com/leadership/digital-universe/index.htm ; http://www.excelacom.com/resources/blog/2016-update-what-happens-in-one-internet-minute.

(2) La collecte s'appliquait en effet non seulement aux données ouvertes du citoyen, mais également aux données privées, confiées par l'utilisateur à Microsoft, Skype, Google, Facebook ou Twitter en échange de services en ligne gratuits.

(3) Isight Partners (spécialiste de la cyberintelligence), « Newscaster: An Iranian Threat inside Social Media », Dallas, 28 mai 2014, accessible sur le site Cyber-peace.org (http://bit.ly/2lgeI9K). Voir également : Thierry Berthier, « Projections algorithmiques et cyberespace », *Revue internationale d'intelligence économique*, Lavoisier, vol. 5, n° 2, juillet-décembre 2013, p. 179-195.

(4) Le commerce et l'exploitation des vulnérabilités informatiques ont été intégrés à l'Arrangement Wassenaar, relatif aux ventes d'armes et aux outils à usage dual (civil et militaire), qui réglemente fortement l'exportation des *Zero Days*. L'UE a par ailleurs voté plusieurs résolutions limitant leur exportation et leur commerce.

Lexique

Un ***système formel*** est une modélisation mathématique d'un langage spécialisé.

En librairie…

NSA, National Security Agency : l'histoire de la plus secrète des agences de renseignement

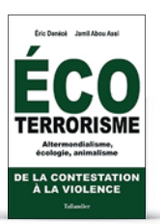
Claude Delesse, Paris, Tallandier, 2016, 509 p.

L'histoire de la NSA plonge le lecteur dans l'univers fascinant mais inquiétant du renseignement d'origine électromagnétique (*SigInt*) qui évolua avec la guerre froide mais est depuis longtemps confronté aux phénomènes terroristes et à la criminalité organisée. Instrument de souveraineté, l'Agence nationale de sécurité américaine a connu, dès son émergence, maintes crises et supporté divers conflits. Elle apporte un soutien aux décisions politiques et militaires des États-Unis tout en étant clandestinement très active sur le plan de la sécurité économique et de la sécurité intérieure. Espionne et cryptologue hors pair, en perpétuelle quête de domination technologique et de maîtrise de l'information, elle opère en étroite collusion avec les complexes militaro-industriel et *high-tech*. Les contre-pouvoirs – congrès, justice, médias, lanceurs d'alerte, hacktivistes – n'entravent guère sa détermination face aux guerres cyber et d'autres natures qui se profilent. Le texte très documenté est accompagné d'annexes éclairantes sur la communauté du renseignement. Cet ouvrage a reçu le prix « Géopolitique et entreprise » du Festival de géopolitique de Grenoble.

Histoire secrète des RG

Brigitte Henri, Paris, Flammarion, 2017, 555 p.

En 2008, les Renseignements généraux disparaissent pour laisser place à la DCRI. Neuf ans plus tard, cette incarnation de la modernité est un échec. Même si tout n'a pas toujours été irréprochable au sein des RG, ils participèrent à protéger la France d'actions terroristes soudaines et violentes qu'elle a connues depuis 2012. Pourtant, ce service mal connu a endossé un habit politique dont il a eu du mal à se défaire. Plusieurs scandales ont terni son image. Affaire des écoutes du PS, disparition du pasteur protestant et militant homosexuel Joseph Doucé, affaire Clearstream… Affaires, efficacité du service, rôle des politiques… Brigitte Henri, une ancienne de la maison, raconte et sonde, documents à l'appui, l'histoire, les hommes, les réussites et les carences des RG, pour en dessiner un portrait loin des passions.



Ecoterrorisme : altermondialisme, écologie, animalisme, de la contestation à la violence

Éric Denécé et Jamil Abou Assi, Paris, Tallandier, avril 2016, 368 p.

Des mouvements contestataires agissant au nom de l'éthique (altermondialisme, écologie, défense des droits des animaux) donnant naissance à des groupes radicaux partisans d'attaques violentes et à des actions « armées ». Ce phénomène porte un nom : écoterrorisme. Black Blocs, Front de libération des animaux ou Front de la libération de la terre multiplient sabotages, attentats, voire meurtres, contre le « pouvoir de l'argent ». Ils figurent aujourd'hui, aux États-Unis et en Grande-Bretagne, sur la liste noire des organisations terroristes au même titre que Daech et Al-Qaïda. La France est encore peu touchée, mais déjà des signes annonciateurs de telles campagnes violentes sont notables après les événements de Sivens, Roybon et Notre-Dame-des-Landes. Premier ouvrage du genre en France, il présente les causes et idéologies contestataires, décrit les groupes violents, leurs modes d'organisation, leurs cibles et leurs opérations.

Renseignement et avant-guerre de 1914 en Grande Région

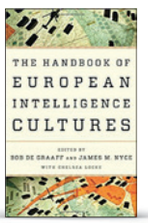
Gérald Arboit (dir.), Paris, CNRS Éditions, novembre 2016, 168 p.

Préfacé par Olivier Forcade, ce livre étudie l'avant-guerre en Lorraine française, allemande, belge et Luxembourg. Une étude consacrée au premier service de renseignement serbe ouvre cet ouvrage collectif pour mieux démontrer l'incongruité de l'étincelle bosniaque. L'espace grand-régional correspond mieux à l'affrontement en préparation entre la France et l'Allemagne. Les services de renseignement de ces deux pays y développent, depuis le début du XX^{e} siècle, les conditions de l'affrontement de leurs deux pays. Planifié pour n'être qu'un nouvel affrontement régional, à l'image de la guerre de 1870, les voisins luxembourgeois et belges observent et constatent une augmentation de l'espionnage sur leurs territoires respectifs. La guerre secrète qui se joue dans l'avant-guerre est plus clandestine, dans ses pratiques, et humaines, dans ses conséquences, que ce que l'on pense usuellement. Ce livre a obtenu le label « Centenaire » de la Mission centenaire 1914-1918.

Les réseaux du fer : information, renseignement économique et sidérurgie luxembourgeoise entre France, Belgique et Allemagne, 1911-1940

Gérald Arboit, Berne, Peter Lang éditeur, coll. « Études luxembourgeoises », novembre 2015, 411 p.

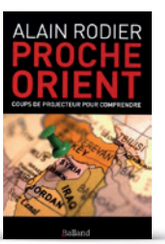
Quel est le rôle de l'information dans l'activité économique ? Question fondamentale à la base de l'intelligence économique, elle est trop souvent négligée par les opérateurs. Elle guida les choix d'Emile Mayrisch à chaque étape de l'histoire de l'Arbed. Depuis la création de cette entreprise sidérurgique (1911) jusqu'à son avènement comme une industrie mondiale, dans l'entre-deux-guerres, ces choix stratégiques fondés sur l'information ont également eu des conséquences sur la structure économique luxembourgeoise. Ces mutations attirèrent l'attention de la Belgique et de la France, vainqueurs (1918) d'une Allemagne qui ne comprit jamais le Luxembourg. Si la dynamique de Mayrisch ne s'émoussa pas après sa disparition, ses successeurs furent moins habiles à manier l'information.



The Handbook of European Intelligence Cultures

Bob de Graaff, James M. Nyce (dir.), Lanham, Rowman & Littlefield, juillet 2016, 450 p.

Les cultures nationales du renseignement résultent de l'histoire et de l'environnement de leur pays. Prenant en compte 32 pays européens, ce livre collectif met en perspective plusieurs agences de renseignement (Albanie, Belgique, Croatie, Lettonie, Luxembourg, Monténégro, Norvège…) rarement retenues dans les études comparatives, le plus souvent faute d'accès facile à de l'information. Dans leurs chapitres, les contributeurs, qui sont tous experts des services de leur pays, ont mis en évidence leur communauté du renseignement, plutôt qu'une énième étude centrée sur une agence seule. Ils examinent l'environnement dans lequel chaque service opère, ses acteurs, et le climat culturel et idéologique. Ils couvrent les facteurs externes et internes qui influencent la communauté du renseignement d'une nation. Le résultat n'est pas une étude exhaustive, mais une étude unique des communautés européennes du renseignement présentées.



Proche-Orient : coups de projecteur pour comprendre

Alain Rodier, Paris, Balland, février 2017, 357 p.

Cette série de chroniques sur le Proche-Orient est un éclairage précieux sur une situation très complexe et difficile à appréhender dans sa globalité. À savoir que les guerres civiles syrienne, irakienne et yéménite ne sont que la partie émergée des luttes d'influence qui opposent Riyad à Téhéran. La solution est d'abord doctrinale, mais elle concerne avant tout les musulmans, car les actes terroristes qui ont lieu en Occident ne sont que des répliques du séisme qui bouleverse le monde musulman. Il confronte les populations chiites aux sunnites et, à l'intérieur de ces dernières, les partisans du salafisme radical qui prônent le renversement de tous les pouvoirs en place car considérés comme « corrompus » ou « apostats ». Des problèmes plus globaux viennent se superposer : Kurdes, Turcs, migrants, armes chimiques… et Moscou qui tente de reprendre de l'influence dans la région en assurant sa défense avancée contre l'islam radical.

La Fabrique du djihad

Stéphane Berthomet, Québec, Edito, septembre 2015, 160 p.

En octobre 2014, pour la première fois de son histoire, le Canada est atteint en plein cœur par un attentat perpétré par un citoyen canadien. De l'évolution du terrorisme d'Al-Qaïda à celui de l'État islamique en passant par l'émergence d'un terrorisme isolé et quasi individuel au Canada comme dans la plupart des pays occidentaux, cet ouvrage dresse un portrait éclairant de cette menace en dévoilant au grand public les méthodes de radicalisation et de recrutement des futurs terroristes.

Centre Français de Recherche sur le Renseignement

VOCATION /

Fondé en 2000, le CENTRE FRANÇAIS DE RECHERCHE SUR LE RENSEIGNEMENT (CF2R) est un Think Tank indépendant, régi par la loi de 1901, spécialisé sur l'étude du renseignement et de la sécurité internationale.

Il a pour objectifs :

- *le développement de la recherche académique et des publications consacrées au renseignement et à la sécurité internationale,*
- *l'apport d'expertise au profit des parties prenantes aux politiques publiques (décideurs, administration, parlementaires, médias, etc.),*
- *la démystification du renseignement et l'explication de son rôle auprès du grand public.*

ORGANISATION /

Le CF2R est organisé en trois pôles spécialisés, regroupant une vingtaine de chercheurs.

- **HISTOIRE DU RENSEIGNEMENT qui étudie les activités de renseignement à travers l'histoire :**
  - Renseignement et contre-espionnage,
  - Actions clandestines et opérations spéciales,
  - Interceptions et décryptements,
  - Guerre psychologique,
  - Tromperie et stratagèmes.

- **POLITIQUES DU RENSEIGNEMENT qui analyse le fonctionnement du renseignement moderne :**
  - Organisation et coordination des services,
  - Budget et effectifs,
  - Analyses d'opérations,
  - Technologies du renseignement,
  - Gouvernance et éthique du renseignement,
  - Intelligence économique et privatisation du renseignement,
  - Contrôle parlementaire.

- **NOUVELLES MENACES ET NOUVEAUX RISQUES qui a pour objet l'identification et le suivi des sujets d'intérêt des services de renseignement et de sécurité :**
  - Terrorisme,
  - Conflits en cours ou en devenir,
  - Espionnage économique,
  - Criminalité internationale,
  - Cybermenaces,
  - Extrémisme politique et religieux, subversion violente.

ACTIVITÉS /

- **RECHERCHE ACADÉMIQUE ET ENCADREMENT DE THÈSES**

- **ORGANISATION DE COLLOQUES, CONFÉRENCES ET DINERS-DÉBAT** consacrés aux questions de renseignement.

- **SOUTIEN À LA RECHERCHE**
  Chaque année, le **CF2R** décerne deux prix universitaires qui récompensent les meilleurs travaux académiques francophones consacrés au renseignement :
  - le « *Prix Jeune chercheur* » prime un mémoire de mastère,
  - le « *Prix universitaire* » récompense une thèse de doctorat.

- **PARTICIPATION À DES RÉUNIONS SCIENTIFIQUES ET COLLOQUES EN FRANCE ET À L'ÉTRANGER**

- **ACTIONS DE SENSIBILISATION**
  à l'intention des parlementaires et des décideurs politiques et économiques.

- **FORMATIONS SPÉCIALISÉES**
  Notamment une session internationale « ***Management des agences de renseignement et de sécurité (MARS)*** ».
  Unique formation de ce type dans le monde francophone, elle a pour finalité d'apporter à des participants provenant des secteurs public et privé une connaissance approfondie de la finalité et du fonctionnement des services.

- **ASSISTANCE AUX MÉDIAS**
  Le **CF2R** met son expertise à la disposition des journalistes, scénaristes, romanciers, éditeurs et traducteurs pour les aider dans leur approche du renseignement (conception de dossiers spéciaux et de documentaires, conseil pour scénarios).

- **MISSIONS D'EXPERTISE DE TERRAIN ET D'ÉVALUATION DES CONFLITS INTERNATIONAUX**

- **MISSIONS DE CONSEIL, D'ÉTUDE ET DE FORMATION**
  au profit d'entreprises, de clients gouvernementaux, d'institutions internationales ou d'organisations non gouvernementales.

Centre Français de Recherche sur le Renseignement (CF2R)
21 boulevard Haussmann
75 009 Paris - FRANCE
Courriel : info@cf2r.org
Tel. 33 (1) 53 43 92 44
Fax 33 (1) 53 43 92 00

www.cf2r.org

OFFRE SPÉCIALE D'ABONNEMENT

Chaque mois, découvrez dans nos magazines
DIPLOMATIE *(6 n°/an)* & **LES GRANDS DOSSIERS DE DIPLOMATIE** *(6 n°/an)*
le meilleur de la géopolitique et des affaires internationales

OUI, JE M'ABONNE OU J'ABONNE UN(E) AMI(E) :

OFFRE N°1
ABONNEMENT À DIPLOMATIE

1 AN D'ABONNEMENT • 6 NUMÉROS
❑ France métrop. **40**€ ❑ DOM/TOM/Europe **55**€ ❑ Reste du monde **70**€

2 ANS D'ABONNEMENT • 12 NUMÉROS
❑ France métrop. **70**€ ❑ DOM/TOM/Europe **100**€ ❑ Reste du monde **130**€

OFFRE N°2
ABONNEMENT AUX GRANDS DOSSIERS DE DIPLOMATIE

1 AN D'ABONNEMENT • 6 NUMÉROS
❑ France métrop. **45**€ ❑ DOM/TOM/Europe **60**€ ❑ Reste du monde **75**€

2 ANS D'ABONNEMENT • 12 NUMÉROS
❑ France métrop. **80**€ ❑ DOM/TOM/Europe **110**€ ❑ Reste du monde **140**€

OFFRE N°3
ABONNEMENT À DIPLOMATIE + LES GRANDS DOSSIERS DE DIPLOMATIE

1 AN D'ABONNEMENT • 12 NUMÉROS
❑ France métrop. **75**€ ❑ DOM/TOM/Europe **105**€ ❑ Reste du monde **135**€

2 ANS D'ABONNEMENT • 24 NUMÉROS
❑ France métrop. **140**€ ❑ DOM/TOM/Europe **200**€ ❑ Reste du monde **260**€

Offres valables jusqu'au 30/06/2017 dans la limite des stocks disponibles

MES COORDONNÉES

❑ M. ❑ Mme ❑ Melle Nom.....
Prénom.....
Adresse.....
.....
.....
Code postal..... Ville.....
Pays.....
Téléphone.....
E-mail.....

JE RÈGLE MON (MES) ABONNEMENT(S) PAR :

❑ chèque bancaire ou postal, libellé en euros (à l'ordre d'AREION)
❑ par carte bancaire (VISA/ Mastercard)

N° de carte ____/____/____/____
Date d'expiration __/__
Cryptogramme ___
(3 derniers chiffres au dos de la CB)

Date et signature (obligatoires)

Conformément à la loi Informatique et Libertés du 6.01.1978, vous disposez d'un droit d'accès et de rectification des données vous concernant. Les renseignements demandés sont réservés au traitement de votre commande. Par notre intermédiaire, vous n'êtes pas amené à recevoir de propositions émanant d'autres sociétés.

Passez votre commande sur notre boutique sécurisée
areion24.news

À renvoyer par courrier à :
MAGAZINE DIPLOMATIE – SERVICE ABONNEMENT
c/o BACK-OFFICE PRESS –12350 PRIVEZAC
Vous pouvez également vous abonner sur Internet : **www.areion24.news**

ILERI

L'ECOLE
DES RELATIONS
INTERNATIONALES
A PARIS DEPUIS 1948

LE MONDE PREND
UNE AUTRE DIMENSION

DEUX PARCOURS D'EXCELLENCE BAC+3 & BAC+5

- **Bachelor en Relations internationales** (Bac+3)
  - Droit, sciences politiques, géopolitique, économie et langues
- **Deuxième Cycle en Relations Internationales** (Bac+5)

  Trois spécialisations :
  - Sécurité internationale et défense - **Grade de Master**
  - Intelligence économique - **Grade de Master**
  - Action humanitaire - **Titre RNCP Niveau I**

TÉLÉCHARGEZ
L'APPLI ILERI

DISPONIBLE SUR Google Play

Télécharger dans l'App Store

SOIRÉE PORTES OUVERTES
VENDREDI 12 MAI

CONCOURS D'ENTRÉE
JEUDI 1ER JUIN

ECOLE D'ÉTÉ
JUILLET 2017

01 40 53 00 44 - 7, Avenue des Chasseurs 75017 Paris *ileri.fr*