

Bruno Lassalle
Chercheur associé
Fondation pour la recherche stratégique

Le renseignement, phénix du 11 septembre

L'attaque terroriste du 11 septembre 2001 a mis en défaut l'organisation du renseignement des Etats-Unis. En effet, les différents systèmes en service, dont le fameux Echelon, furent impuissants à capter des informations décisives et les analystes n'ont pas su exploiter les indices révélateurs pourtant décelés avant l'attentat puis mis en évidence lors des enquêtes ultérieures. Ainsi, « *[e]ntre 1998 et 2001, rien n'est venu perturber les préparatifs des attentats par Al Qaida* »¹, alors même que les services de renseignement disposaient d'informations fiables sur l'éventualité d'attentats contre des intérêts américains. De ce fait, l'adversaire, déployé clandestinement sur le territoire des Etats-Unis et utilisant des moyens dévoyés de leur usage habituel, bénéficia de la liberté d'action et de l'effet de surprise pour prononcer son attaque tout aussi odieuse que spectaculaire.

Cet événement a démontré la capacité d'action et de destruction des réseaux terroristes et la nécessité de réorganiser les organismes de renseignement en les adaptant pour affronter ces menaces inédites. Après la sidération, le temps de la réflexion et des analyses sans concessions est venu, ouvrant des voies qui s'avèreront bénéfiques pour l'avenir du renseignement, lui permettant de s'adapter aux nouveaux périls asymétriques non étatiques et, d'une certaine manière, de renaître des sinistres cendres du 11 septembre.

Aux Etats-Unis comme au sein des autres Etats conscients du changement de donne et soucieux d'adapter leur renseignement avec volontarisme, un consensus s'est rapidement dégagé sur les voies à suivre. Parmi les pistes d'amélioration relevées, on peut citer, sans

¹ Conclusion du rapport de la commission d'enquête du Congrès sur les attentats du 11 septembre 2001.

prétendre à l'exhaustivité, quelques axes majeurs. D'abord favoriser les échanges d'informations en palliant les défauts des structures verticales, coordonner les différentes bases de données pour mieux exploiter leurs complémentarités. Ensuite extraire l'information utile même lorsqu'elle est noyée dans des volumes considérables de données interceptées, en trouvant un juste équilibre entre renseignement humain et renseignement technique. Enfin, cultiver des relations de confiance entre les décideurs et leurs services de renseignement.

Ces réformes et aménagements ont conduit à la mise en réseau de certaines entités, étatiques ou non, visant à dépasser les pesanteurs bureaucratiques et à élargir la veille à tous les domaines. En bref, et de manière un peu caricaturale car les menaces traditionnelles ne disparaissent pas pour autant, créer des réseaux pour lutter contre des réseaux dans une lutte réseau-centrée en exploitant toute la puissance des systèmes d'information pour détecter l'adversaire dans le « bruit de fond ». Ces tendances impactèrent à des degrés divers tous les organismes de renseignement, dont le renseignement français.

Neuf ans avant l'attentat, le renseignement national fut réformé conformément aux enseignements de la première guerre du Golfe de 1991, qui soulignaient que le renseignement militaire, marqué par l'héritage de la Guerre froide, était trop dépendant des renseignements alliés et centré à l'excès sur la connaissance des systèmes de combat et les ordres de bataille. Il était recommandé d'élargir la quête des informations opérationnelles à la connaissance de l'environnement en développant la production et l'exploitation du renseignement d'intérêt militaire (RIM). Rappelons que le RIM, en complément du renseignement strictement militaire, s'intéresse à la connaissance de l'environnement humain, physique, économique... C'est sur ces bases que fut créée la DRM, tête de chaîne du renseignement militaire, mieux adaptée à la nouvelle donne géopolitique pour apporter aux armées et aux décideurs des plus hauts niveaux une capacité d'anticipation et une autonomie d'appréciation de situation.

Par ailleurs, cette organisation permettait de mettre en œuvre en toute complémentarité, dans une logique de mutualisation, des capacités de renseignement d'origine humaine (ROHUM), d'origine électromagnétique (ROEM) et d'origine image optique et radar (ROIM) et d'en tirer la meilleure synergie. La culture du RIM facilite, en outre, l'extraction des signaux faibles trahissant des changements d'habitudes ou des curiosités.

A la veille du 11 septembre, la DRM constituait bien un outil modernisé. Il faut toutefois noter que sa création, comme toute innovation, bouleversa l'ordre ancien. Les effectifs de la DRM furent prélevés par transfert depuis d'autres entités, ce qui ne manqua pas de susciter des regrets au sein des armées, qui durent se passer de leurs bureaux renseignements (B2) et des effectifs correspondants. De la même manière, le domaine d'action de la DRM fut élaboré en réaménageant ceux des Armées et de la DGSE. Quelques rugosités ont pu parfois troubler les relations entre organismes, lors des arbitrages financiers liés aux programmes ou pour le recrutement des cadres de la DRM.

De manière salubre, l'effet 11 septembre et les axes de réformes adoptés ensuite par les Etats-Unis firent ressortir le bien-fondé des réformes du renseignement français et confèrent un surplus de légitimité à l'organisation de la DRM en tant que tête de chaîne du renseignement militaire, éteignant les critiques et conduisant à une appréciable normalisation des relations. Ultérieurement, la montée en puissance de la coopération en bonne intelligence avec les armées, la DGSE et plus largement les autres organismes de renseignement nationaux et étrangers se poursuivit en toute efficacité.

L'élargissement de la surveillance implique, pour la DRM, la multiplication des écoutes et un accroissement du besoin en systèmes de guerre électronique pour de nouvelles stations d'interception terrestres, maritimes, aériennes et spatiales. Toutefois, la réalisation de ces besoins est d'abord liée à la capacité de convaincre les décideurs. Dans son livre intitulé *La guerre électronique, maître des ondes, maître du monde...*², le général Jean-Paul Siffre notait que « *convaincre de l'importance de la guerre électronique a vraiment été durant 20 ans un exercice laborieux* ». La complexité inhérente aux lois de l'électromagnétisme n'a jamais facilité l'expression d'arguments décisifs pour promouvoir un programme de guerre électronique en concurrence avec, par exemple, un programme de capteur plus traditionnel, comme un imageur optique, pour lequel les concepts sont plus intuitifs. Ce fut un autre effet indirect du 11 septembre que de démontrer l'importance de ces capteurs, de démystifier l'emploi de la guerre électronique, tout en favorisant les processus d'acquisition des systèmes.

A titre d'illustration, il est intéressant d'évoquer la réalisation du besoin d'un système satellitaire permettant depuis l'espace la détection et la localisation d'émetteurs de télécommunication ou radars situés au sol. Un tel projet, également adapté à la détection de déploiements terroristes, est soutenu depuis près de vingt ans avec opiniâtreté par la DRM. Elle s'attacha à convaincre et réussit à obtenir l'utilisation opérationnelle des démonstrateurs Essaim, lancé en 2004, puis Elisa, lancé en 2011, composés chacun de quatre microsatellites, avec une durée opérationnelle de trois ans. Cet emploi opérationnel apporta expérience et soutien effectif au profit des opérations. Clin d'œil de l'histoire, dans quelques jours³, les trois satellites du système satellitaire opérationnel CERES (pour Capacité d'Ecoute et de Renseignement Electromagnétique Spatial) seront placés sur orbite par un lanceur Vega.

² Lavauzelle, 2003.

³ Lancement prévu par le CNES au mois de septembre 2021.

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643

© FRS—TOUS DROITS RÉSERVÉS