13 septembre 2019
Nouvelles technologies

Terrorisme nouvelle génération : les services de renseignement ont-ils perdu l'efficacité qu'ils avaient retrouvée après le 11 septembre ?

Après avoir échoué à détecter les attentats du 11 septembre 2001, les centrales américaines du renseignement ont été sommées de se réinventer pour lutter plus efficacement contre le terrorisme. Les réformes ne sont pas closes.

Avec Franck DeCloquement

Atlantico.fr : Les nouvelles menaces sécuritaires concomitantes à l'évolution des technologies numériques, créent-elles une nouvelle inadaptation des services de renseignements américains, similaire à celle qui engendra la non-détection des intentions terroristes ayant mené aux attentats du 11 septembre 2001?

Franck DeCloquement : Pour beaucoup, le fait que les attaques élaborées par les terroristes du 11 septembre n'aient pas été détectée à temps restera pour toujours l'un des pires échecs de la communauté du renseignement américain. Cette faillite collective, ainsi que le coût humain effroyable lié à l'inadaptation des agences de renseignement aux menaces émergentes d'alors,sont encore très présents dans tous les esprits 18 ans après les faits. Et la détermination à anticiper et prévenir de futures attaques est aujourd'hui très forte.

Pendant la décennie qui a suivi l'effondrement du bloc soviétique, la CIA et le FBI ont été embourbés dans les structures, les priorités, les processus et la culture du contre-espionnage issue de la guerre froide. Et ceci, alors même que le danger du terrorisme islamique grandissait. Des recherches universitaires comme celles de l'Américaine Amy Zegart relatées dans son livre « Spying Blind: La CIA, le FBI et les origines du 11 septembre », ont depuis montré que si de nombreux services de renseignement extérieurs américains avaient vu la menace terroriste arriver, et ont insisté de ce fait pour que les choses changent bien des années auparavant, ils n'ont pourtant pas réussi à obtenir les réformes nécessaires à temps. Le choc du 11 septembre a finalement contraint le Pentagone à un calcul simple qui a conduit– in fine–à une série de succès dans la lutte contre le terrorisme. Allant de complots déjoués contre les intérêts américains à l'usage des drones armés dans les exécutions ciblées de profils criminels à haute valeur ajoutée, à l'opération secrète qui a permis de trouver et de tuer le fondateur d'Al-Qaïda, Oussama Ben Laden,à Abbottābad au nord du Pakistan. Mais aujourd'hui, près de deux décennies plus tard, les 17 agences de renseignement américaines doivent à nouveau se réinventer. Et cette fois en réponse au nombre sans précédent de technologies de pointe qui transforment radicalement les sociétés occidentales, les Etats-nations, la politique internationale, les enjeux du commerce mondial et la nature même des conflits internationaux. Anticiper l'insécurité globale et les ruptures stratégiques à venir est devenu le maître mot pour la sécurité nationale.

Observe-t-on aussi ce même décalage aujourd'hui en dans le contexte français?Quels exemples

d’initiatives ou d'utilisation prospective de ces nouvelles technologies vous semble les plus marquants en la matière?

Maintenant, comme dans la période qui a précédé les attentats du 11 septembre 2001, les premiers indicateurs du monde qui s’annonce sont préoccupants. Et l’impératif de la réforme des activités de renseignement est clair. Le premier effondrement de cette nouvelle ère a déjà eu lieu côté américain: l'incapacité de la communauté du renseignement de comprendre rapidement et complètement l'instrumentalisation des médias sociaux par la Russie, lors de l'élection présidentielle américaine de 2016. Avant les élections, les agences de renseignement ne comprenaient pas clairement ce qui se passait… Depuis les élections, les révélations faites grâce aux enquêtes menées par le Comité du renseignement du Sénat bipartite et l'avocat spécial Robert Mueller, ont montré que les tentatives d'influence sur les médias sociaux par la Russie ont débuté courant 2014, voire bien plus tôt.

En France, alors que le monde se réarme et que les militaires sont quotidiennement bousculés par le développement des technologies civiles dans le spatial, les télécommunications ou l’IA,les choses bougent. Pour preuve, entre autres exemples, la création du cluster « Data Intelligence » par le GICAT présidé par Emmanuel Tonnelier qui regroupe une vingtaine de sociétés françaises – Grands groupes, PME/ETI, Start-Up – disposant de technologies et de solutions innovantes permettant de répondre aux enjeux du renseignement et du traitement massif des données. Mais aussi de la toute nouvelle Agence de l'innovation de défense(AID)dirigée par Emmanuel Chiva rattachée au délégué général de l’armement (DGA). Cette dernière pilote désormais un budget annuel d’un milliard d’euros, et s’appuie sur une équipe rapprochée d’une centaine de personnes – dont une quinzaine de scientifiques – installées dans l’Hexagone de Balard. Outre Def'Invest, le fond d'investissement du ministère des armées dédié aux PME stratégiques, ces deux nouvelles entités ont pour mission d’ouvrir le monde militaire et celui du renseignement aux innovations civiles et aux mutations imposées par la technologie, mais aussi d'éclairer l’innovation de défense par des idées nouvelles issues de la sphère privée.

Preuve encore : la constitution également au sein de l’AID d’une « Red Team », sorte de cellule prospective et d’anticipation de 4 à 5 personnes chargée de proposer des scénarios de disruption, composée d'auteurs de science-fiction et de futurologues pour imaginer l’au-delà, mais aussi la physionomie de l’ennemi probable et de ses possibles actions futures. Pour pouvoir se projeter sans avoir de préjugés ni de barrières mentales à l’entrée, il faut avoir un certain « état d’esprit ». C’est celui entre autres des auteurs et des dessinateurs de science-fiction.

A l’image de la DARPA américaine, et bien que plus modeste, « l’intelligence campus »est une initiative pertinente qui est portée par les militaires,également au cœur des enjeux stratégiques des armées françaises en matière d’anticipation et d’innovation. Dirigé par l’ingénieur général de l’armement Caroline Gervais, il s’agit d’une structure intégrée au dispositif innovation de la défense centrée sur les objectifs de la DRM (Direction du Renseignement Militaire),pleinement investie dans les nouveaux espaces cybers et le spatial. Ce dispositif ambitieux contribue à la supériorité opérationnelle de la France à l’horizon 2030. Car comprendre, anticiper et s’adapter en permanence permet de prévenir les menaces futures et de garantir dès aujourd’hui les succès opérationnels de demain.L’énorme enjeu de la massification de la donnée est un réel challenge pour les services de renseignement Français. Si la DRM dispose de multiples capteurs de données, la source ouverte reste un moyen nécessaire. Il existe cependant le risque d’obtenir des informations biaisées, à l’exemple des Fake ou Deep News. La DRM via « l’Intelligence Campus »assume de se tourner vers le monde civil, là où se situe l’innovation. Car le secteur privé porte aussi l’innovation de l’armée. L’Intelligence Campus répond à d’autres attentes et expressions de besoins que portent les divers clusters cités précédemment, comme « GENERATE » du GICAT. Celui-ci ne conduit pas de projet à vocation commerciale, mais recueil les besoins et les applications possibles. Le but étant de diffuser l’innovation au sein du renseignement militaire et à l’ensemble de la communauté du renseignement, si cela peut améliorer la performance globale des services.

Une meilleure coordination nationale entre services de renseignement est-elle primordiale pour surmonter leur décalage stratégique souvent observé dans le cas des Etats-Unis ou celui de la France, et éviter ainsi les possibles errements au regard d’un contexte international particulièrement durci,imprévisible et sensible ?

Depuis la fin de la guerre froide, l’anatomie de « l’ennemi probable » ainsi que la nature de la menace ont radicalement changé. Les progrès de l'intelligence artificielle (IA), de l'information de source ouvert, des sciences cognitives et du cyber, des biotechnologies, de la miniaturisation des satellites et de nombreux autres domaines technologiques ayant trait au traitement des mégas données,offrent paradoxalement aux adversaires des Etats-Unis et à la France,de nouvelles formes capacitaires en matière de « techno-guérillas »et d’actions belliqueuses« law-cost ». Le paysage et la cartographie des menaces et des acteurs d'aujourd'hui est beaucoup plus complexe qu'il ne l'était en 2001. Les actions terroristes font partie des nombreuses préoccupations en tête de liste, bien entendu. Avec notamment l'intensification de la concurrence et des conflits avec la Russie et la Chine, les risques nucléaires croissants en Corée du Nord, en Iran, en Inde et au Pakistan. Mais aussi l'instabilité croissante au Moyen-Orient,de même que la recrudescence des régimes autoritaires en forte progression sur la scène internationale. De surcroît, les nouvelles technologies numérique accélèrent encore la diffusion de l’information biaisée à une très grande échelle, et rendent les enjeux du renseignement encore plus importants et plus complexes qu’auparavant.

L’érosion du fil conducteur classique de la quête éperdue du renseignement efficient dans un monde complexe,impose encore plus aux agences de séparer la vérité de la supercherie à l’ère des fake news, de la post-vérité et des Deepfake. Mais la communauté du renseignement américaine,par exemple, ne réagit pas assez rapidement aux yeux de certains militaires de haut rang,à ces changements technologiques déstabilisateurs et aux défis qu’ils lancent à l’Amérique. C’est ce qu’indique en substance l’universitaire Amy Zegart dans The Atlantic, membre senior de la Hoover Institution et du Freeman Spogli Institute de l'Université de Stanford. Alors que le 11 septembre était une surprise stratégique, il n'aurait pas dû l'être. Au cours de la décennie précédente, une douzaine de

commissions de haut vol, d'études de groupes de réflexion et de rapports gouvernementaux avaient sonné l'alarme. Mettant ouvertement en garde contre la nouvelle menace terroriste et recommandant des réformes du renseignement américain urgentes et de grande envergure pour y faire face. Ces études ont abouti à un total de 340 recommandations qui portaient toutes sur des lacunes cruciales en matière de renseignement, telles que les problèmes de coordination, les faiblesses en matière de renseignement humain ou de source ouverte (OSINT), et le manque général d'informations et de partage au sein et entre les agences. Ce sont exactement ces mêmes faiblesses que la Commission du 11/9 a finalement identifié par la suite.

Cependant, avant ces attaques funestes, « presque aucune de ces recommandations spécifiques n'avait été pleinement mise en œuvre. La très grande majorité d'entre elles, 268 pour être exact, n'a produit aucune action… Pas même un appel téléphonique, un mémo ou une réunion de concertation… Neuf mois avant les attentats, la commission bipartite « Hart-Rudman », qui avait procédé à l'évaluation la plus complète des problèmes de sécurité nationale des États-Unis depuis la fin de la Guerre froide, avait prédit à juste titre que les défaillances institutionnelles des États-Unis rendaient le pays exceptionnellement vulnérable à une attaque terroriste d'ampleur. Mais ces appels, ainsi que d'autres appels externes à la réforme ont été vains, et n'ont finalement abouti à rien ».

Et Amy Zegart de conclure dans The Atlantic : « dans la période qui a précédé les attaques, la CIA et le FBI ont eu 23 occasions de pénétrer et éventuellement d'arrêter le complot du 11 septembre. Ils ont manqué les 23, pour une raison primordiale: les deux agences fonctionnaient comme elles l'avaient toujours fait auparavant, à l'époque révolue de la guerre froide qui accordait une faible priorité au terrorisme et gardait les informations bloquées dans différentes parties de la bureaucratie. »Les services de renseignement n'ont pas réussi à se réorganiser en conséquence du changement de dimension de la menace, pour mieux mettre un terme aux actions terroristes d'alors, bien avant qu'elles ne se produisent. Une étude interne réalisée en 2002 par le FBI a révélé que les deux tiers des analystes du bureau - les personnes qui étaient supposées «faire le lien» entre les causes et les cas - n'étaient pas qualifiés pour faire leur travail. Et juste quelques semaines avant les attaques du 11 septembre selon Amy Zegart, un examen interne hautement classifié des capacités antiterroristes du FBI a attribué une note d'échec à chacun des 56 bureaux extérieurs du bureau aux Etats-Unis. Pendant ce temps, le directeur de la CIA, George Tenet, travaillait d'arrache-pied pour amener plus d'une douzaine d'agences de renseignement américaines à mieux se coordonner. Peine perdue : il a fait face à une très forte résistance. Tenet n'a même pas réussi à amener les agences à utiliser les mêmes badges sécurisés pour permettre un accès plus aisé des différents personnels aux bâtiments,des uns et des autres. Les efforts de lutte contre le terrorisme sont restés dispersés dans 46 organisations différentes sans stratégie budgétaire ou de coordination centrale.

L'avenir s'annonce donc plus que jamais incertain?

Grâce aux divers progrès de l'intelligence artificielle, les photographies, les vidéos et les deepfake « audios » deviennent très réalistes, difficiles à authentifier, largement disponibles et très faciles à utiliser. Le potentiel de tromperies profondes dans l'espace politique mondiale devient très problématique. Imaginez une vidéo d'apparence réaliste montrant une invasion, un programme nucléaire clandestin ou des responsables politiques en train de discuter de la manière de truquer une élection. Bientôt, « même voir » ne sera pas « croire ». Les opérations de« déception » ont toujours fait partie dans le passé de méthode de l'espionnage et de la guerre subversive, mais pas à ce niveau d'intensité.Entre temps, les anciennes méthodes de collecte du renseignement sont en passe de se démocratiser à très grande vitesse. L'espionnage était coûteux et très exclusif. Lorsque les satellites qui interceptaient des signaux ennemis et des images de l'espace coutaient des milliards de dollars, et requérait un savoir-faire considérable, les États pouvaient se permettre de conserver un avantage technologique évident. Désormais, l'espace est en train de se démocratiser à grands pas, avec la commercialisation de satellites très bon marché. Dan Coats, ancien directeur du renseignement national, a récemment déclaré au Congrès Américain : «À partir de 2019, les innovations qui favorisent la compétitivité militaire et économique proviendront de plus en plus des États-Unis, alors que le leadership des États-Unis dans le domaine de la science et de la technologie (S & T) diminue; l'écart de capacité entre les technologies commerciales et militaires s'évapore; et les acteurs étrangers redoublent d'efforts pour acquérir les meilleurs talents possible, mais aussi les entreprises, les données et la propriété intellectuelle par des moyens licites et illicites. »

Dès lors, manque une ré-imagination globale de « l'intelligence »à l'usage d'une nouvelle ère technologique. À l'avenir, les services de renseignement s'appuieront de plus en plus sur des informations de sources ouvertes collectées par tous, sur du code avancé et des plates-formes accessibles en ligne à moindre coût, ou gratuite, ainsi que sur des algorithmes capables de traiter d'énormes quantités de données plus rapidement et bien mieux que les humains. C'est un tout nouveau monde qui s'annonce. Selon Amy Zegart, la communauté du renseignement occidental a l'impérieuse nécessité de produire un effort stratégique sérieux et soutenu pour identifier la manière dont leurs différentes agences doivent désormais s'organiser pour obtenir et maintenir un avantage concurrentiel consistant, tout en préservant les libertés civiles dans un paysage technologique qui s'annonce radicalement différent. La tâche s'annonce rude.