Centre Français de Recherche sur le Renseignement

« SIGNATURE REDUCTION » : LE PROGRAMME DE PROTECTION DES UNITÉS CLANDESTINES DU PENTAGONE

BULLETIN DE DOCUMENTATION N°25 / JANVIER 2022

ÉRIC DENÉCÉ ET ALAIN-PIERRE LACLOTTE

Au printemps dernier, un article de l'hebdomadaire américain *Newsweek* [1] a révélé au public l'important dispositif militaire clandestin mis en place par le Pentagone pour lutter contre le terrorisme et ceux que Washington, qualifie « d'États voyous ».

Cette armée secrète regroupe 60 000 militaires, soit vingt fois plus que le Service Action de la CIA. Ses membres – dont la moitié sont issus des forces spéciales – travaillent pour la plupart sous de fausses identités, se dissimulant souvent derrière la façade de nombreuses entreprises privées qui administrent et soutiennent ce dispositif.

Cette force clandestine de renseignement et d'action traque et élimine les terroristes islamistes partout dans le monde. Ses hommes opèrent également dans de nombreux points chauds, notamment en Corée du Nord, en Iran, sur les frontières de la Russie (Donbass) et de la Chine. Officiers-traitants, commandos de reconnaissance, saboteurs et combattants de l'ombre y agissent quotidiennement, sans que la trace de leurs actions soit toujours

identifiable.

Leur identité et leurs activités doivent être protégées tout autant que celles des cyberwarriors qui effectuent leur travail quotidien depuis les Etats-Unis sous de faux noms, conduisant le type d'actions agressives que Washington dénonce lorsque ce sont les Russes ou les Chinois qui le font.

L'ABSOLUE NÉCESSITÉ DE LA SÉCURITÉ OPÉRATIONNELLE

Les Etats-Unis font tout pour garder secrète l'action de ces unités, changeant régulièrement leur dénomination, dissimulant leurs budgets, cachant parfois même leur existence aux parlementaires comme à l'opinion, et faisant en sorte que leurs adversaires ignorent leurs déploiements.

La sécurité opérationnelle (OPSEC) est indispensable tant pour la sécurité des opérations que celle des personnels et de leur famille, notamment en raison des nouvelles vulnérabilités liées à la digitalisation de nos sociétés et aux réseaux sociaux.

L'une des principales tâches afin de rendre indétectables les unités et les activités clandestines militaires consiste à garder secrètes l'existence des organisations et l'identité des personnels participant aux opérations, mais aussi les moyens qu'elles utilisent (automobiles, avions, hélicoptères, etc.). L'abondance d'informations en ligne sur les individus ainsi que certains piratages étrangers spectaculaires ont permis aux services de renseignement adverses de mieux démasquer les fausses identités des espions américains. La « réduction de la signature » est donc non seulement indispensable dans le cadre de la lutte contre le terrorisme, mais aussi dans celui des rivalités géopolitiques de plus en plus tendues avec la Russie et la Chine. Il est également essentiel de protéger les familles des membres de cette armée secrète dont certaines ont été ciblées par l'Etat islamique. Un énorme travail de dissimulation et de couverture est donc indispensable. Il va du nettoyage des signes révélateurs des véritables identités des opérateurs sur internet à l'implantation de fausses informations pour protéger les missions et les personnes.

Les unités militaires clandestines américaines sont ainsi protégées par un programme spécial appelé *« Signature Reduction »* qui dissimule leurs activités derrière des dizaines d'organisations gouvernementales inconnues du public et des entreprises privées, réelles ou fictives. Il est géré par la *Defense Intelligence Agency* (DIA) via le *Defense Cover Office*.

Leurs budgets – qui pourraient permettre de connaitre leur implantation, leurs effectifs et leurs moyens – sont également extrêmement protégés sous des programmes anodins. Le *Joint Special Operations Command* (JSOC) camoufle par exemple son organisation et ses activités sous plus de cinquante *Special Access Programs (SAP)*, chacun correspondant à une opération ou une capacité particulière. Ces programmes reçoivent des noms de code qui sont eux-mêmes classifiés De nombreux SAP de « réduction de la signature », portant des noms tels que *Hurricane Fan, Island Hopper* et *Peanut Chocolate*, sont administrés par un monde obscur d'organisations secrètes au service de l'armée clandestine – la *Defense Programs Support Activity,* le *Joint Field Support Center,* le *Army Field Support Center, le Personnel Resources Development Office,* l'*Office of Military Support,* le *Project Cardinals et* le *Special Program Office.* De plus, les unités du JSOC changent si souvent de nom que même les autres militaires ne savent jamais véritablement qui elles sont, ni ce qu'elles font.

En fait, le JSOC ne veut pas que la plupart des dirigeants élus sachent quoi que ce soit, en particulier au cas où les choses tourneraient mal. Et la plupart des politiques préfèrent ne pas savoir non plus, pour la même raison.

UNE IMPRESSIONNANTE INFRASTRUCTURE DÉDIÉE

Aux Etats-Unis, peu de gens ont entendu parler du programme *« Signature Reduction »* et encore moins sont conscients de son ampleur. Environ 130 sociétés privées participent à ce programme et soutiennent cet « empire clandestin ». Au total, elles engrangent plus de 900

millions de dollars par an pour servir les forces clandestines, qu'il s'agisse de créer de faux documents, de payer les factures et les impôts de personnels opérant sous des noms d'emprunt, de fabriquer des déguisements et autres dispositifs pour déjouer la détection et l'identification afin de faciliter les déplacements clandestins, ou de construire des appareils spéciaux pour photographier et écouter les activités dans les zones les plus reculées du Moyen-Orient ou de l'Afrique.

Alors que les documents d'identité infalsifiables et la biométrie sont devenus des normes mondiales, les spécialistes du programme *Signature Reduction* ont dû mettre au point des moyens afin de déjouer les systèmes de sécurité aux frontières, notamment les empreintes digitales et la reconnaissance faciale. Avant Internet, le risque qu'un policier ou un garde-frontière étranger ne soit connecté à des bases de données mises à jour en temps réel était minime. Tout ce dont un agent opérant sous couverture avait besoin était une pièce d'identité « authentique ». De nos jours, cependant, pour ceux qui opèrent sous couverture, la « légende » derrière une identité fictive doit être beaucoup plus élaborée : il faut créer toutes les preuves – physiques comme électroniques – d'une existence réelle. De faux lieux de naissance et de fausses adresses de domicile doivent être soigneusement recherchés, de fausses vies électroniques et de faux comptes de médias sociaux doivent être créés, etc. Et les individus fictifs doivent avoir des « amis » correspondants à leur vie inventée.

Pour ce faire, les spécialistes du programme *Signature Reduction* appliquent six principes : crédibilité, compatibilité, réalisme, soutenabilité, véracité et conformité. Cette approche est essentielle car dans le monde ultra sécuritaire post 11 septembre, les points de contrôle se sont multipliés et les activités douteuses sont examinées de plus près. Faire opérer quelqu'un sous couverture nécessite un travail de longue haleine qui ne doit pas seulement concerner son identité opérationnelle, mais qui implique aussi de prendre en charge la gestion de sa vie réelle aux Etats-Unis, dont les célibataires notamment, ne peuvent plus s'occuper.

Il faut d'une part assurer le paiement de factures de l'individu fictif, ce qui entraine une collaboration avec les banques et les services de sécurité des cartes de crédit pour éviter qu'elles ne révèlent le « pot aux roses » lorsqu'ils enquêtent sur une fraude d'identité ou luttent contre le blanchiment d'argent. De plus, les spécialistes *Signature Reduction* doivent s'assurer que les véritables impôts et paiements de sécurité sociale des opérateurs sont effectués – afin que les personnes puissent retourner à leur vie lorsque leurs missions prennent fin.

C'est l'*Operational Planning and Travel Intelligence Center* (OPTIC) qui est chargé de superviser une grande partie de ces activités. Il gère le plus grand bureau financier militaire du Pentagone. Ses personnels – souvent de militaires à la retraite – se consacrent à plein temps à cette tâche exigeante. Rien n'est laissé au hasard. Certains sont chargés d'effectuer quotidiennement la tournée d'une quarantaine de bureaux de poste et de boîtes aux lettres. Ils y collectent des dizaines de lettres et de paquets et en envoient un nombre similaire depuis des adresses rurales. De retour au bureau, ils procèdent au tri entre les courriers fictifs, servant à faire vivre les couvertures, et les courriers réels, puis remettent les factures aux responsables des finances. D'autres ont pour mission d'obtenir passeports et permis de conduire, factures, documents fiscaux, cartes de membre d'organisations…. pour des personnes qui n'existent pas. Ces documents constituent la base des fausses identités.

Pour mener à bien cette tâche exigeante, les membres de l'OPTIC se connectent à deux bases de données de la communauté du renseignement : la première est celle des faux documents de voyage et d'identité, qui contient 300 000 passeports et visas étrangers contrefaits et modifiés ; la seconde est le registre ultra-secret des fausses identités où sont consignées les couverturesutilisées par les opérateurs clandestins et la liste des pièces qui leur donnent corps. En complément, les spécialistes de l'OPTIC travaillent avec les bureaux du *Department of Homeland Security* et du département d'État, ainsi qu'avec la quasi-totalité des 50 États américains, afin de pouvoir créer « d'authentiques » individus fictifs et modifier les bases de données de l'immigration et des douanes afin de s'assurer que les opérateurs clandestins puissent revenir aux États-Unis sans être inquiétés au titre de leurs activités illicites conduites à l'étranger sous leur identité fictive.

DES SECRETS BIEN GARDÉS

Des sources proches du Pentagone estiment que 80% des missions du JSOC effectuées avant 2000 restent classifiées. Elles rapportent que des opérateurs de la Delta Force, du Seal Team 6 et des éléments de la CIA auraient été infiltrés en Chine pour y cartographier les installations de transmission par satellite dans l'éventualité d'une action de neutralisation. Elles évoquent aussi diverses actions sur le sol iranien. Après le 11 septembre, le JSOC aurait infiltré au moins deux agents dans le pays. Suite à l'invasion de l'Irak, la Mission Support Activity (MSA) et la Delta Force auraient effectué des actions le long de la frontière iranienne, en particulier au Kurdistan. Des agents kurdes recrutés localement auraient conduit à une ou deux sources sur le programme nucléaire iranien, livrant des renseignements capitaux. En 2004, la MSA, avec l'appui de la CIA, a introduit un couple en Iran sous couverture commerciale. En 2007, les généraux Stanley McChrystal et Michael Flynn ont créé un groupe de travail pour contrer l'influence de Téhéran et de son allié, le Hezbollah libanais, dans le monde – notamment afin de mettre en lumière les liens de ce dernier avec les cartels de la drogue d'Amérique du Sud. Enfin, le JSOC a envisagé l'idée de provoquer des troubles en Iran afin de pousser les membres du Corps des gardiens de la révolution islamique (pasdaran) à se livrer des représailles, afin de les identifier et de les éliminer un à un.

Les dirigeants du Pentagone continuent cependant d'affirmer *« L'armée ne mène pas d'opérations secrètes, et le personnel militaire ne combat pas sous couverture »* sauf quand ils le font… parce que des militaires sont affectés à la CIA pour certaines missions, ou parce qu'un organisme comme le JSOC opère clandestinement !

LES « MISTERS Q » DU PENTAGONE

Fausses pierres dissimulant un dispositif de surveillance ou de communication caché, tissus chauffants rendant les soldats invisibles à la détection thermique, motos électriques capables d'opérer silencieusement sur les terrains les plus accidentés, *shalwar kameez* (vêtements

afghans) portés par les commandos tissés de dizaines de mètres de fils spéciaux les transformant en récepteurs ambulants capables d'intercepter les radios de faible puissance et les signaux des téléphones portables… les créations des laboratoires spéciaux du Pentagone au service des opérations clandestines dépassent largement la fiction.

LES MOYENS D'INFLITRATION CLANDESTINS

Dans un monde où tout est électronique, où tout est filmé, il est impossible d'entrer dans un parking sans que la plaque d'immatriculation du véhicule soit enregistrée. De même, il n'est pas possible de réserver un vol ou un hôtel sans une pièce d'identité ni d'utiliser une carte de crédit sans que le lieu et l'heure de la transaction ne soient enregistrés. Dès lors, comment passer inaperçu et ne pas laisser de traces ? Comment déjouer la biométrie, les caméras de surveillance et les lecteurs d'empreintes digitales ?

Pour les membres des unités militaires clandestines du Pentagone, ces difficultés sont facilement contournées. La plupart d'entre eux s'infiltrent clandestinement dans les pays hostiles pour y réaliser leurs missions, par voie aérienne, maritime ou terrestre. Les autres voyagent sous leur vrai nom ; ils n'adoptent une fausse identité et n'emploient de faux moyens de paiement qu'une fois dans le pays où ils opèrent.

Afin de passer sans risque le contrôle des passeports sous de fausses identités, les « moyens spéciaux » américains ont mis au point deux types de systèmes pour déjouer les dispositifs de sécurité biométriques : des programmes informatiques pour modifier les bases de données adverses ; et des masques et des techniques de maquillage inédites pour transformer de manière indétectable l'aspect physique des opérateurs.

L'un de ces programmes informatiques, *ExpressLane*, a été conçu afin de pénétrer dans les systèmes étrangers de biométrie afin d'en voler ou d'en corrompre les données. Ainsi, les cyberespions américains peuvent en modifier le contenu lorsqu'un agent passe le contrôle des passeports avec une fausse identité, puis effacer toute trace de cette action.

Une autre méthode des Misters Q américains consiste à transformer les personnes pour leurs missions clandestines grâce à un appareil facial en silicone sculpté pour modifier parfaitement l'apparence. Ils peuvent vieillir un individu, augmenter sa masse corporelle et même le faire passer pour quelqu'un d'un autre sexe. Il leur est également possible de modifier les empreintes digitales à l'aide d'un manchon en silicone qui s'adapte si bien à une vraie main qu'il ne peut être détecté ; de plus, il intègre des empreintes digitales modifiées, imprégnées d'huiles simulant les fluides secrétés par la peau humaine. Ces dispositifs, dignes de la série *Mission Impossible*, seraient particulièrement performants…

LES COMMUNICATIONS CLANDESTINES

L'autre enjeu majeur pour les opérateurs clandestins est celui des communications secrètes ou COVCOMM, comme les appellent les initiés.

Depuis deux décennies, les cafés Internet et les portes dérobées en ligne sont devenus les moyens privilégiés des communications secrètes, remplaçant largement les ondes courtes. Mais peu à peu, en raison de la diffusion des technologies de pointe, les pays totalitaires ont rattrapé leur retard et leurs services de renseignement ont acquis la capacité de détecter et d'intercepter les activités clandestines sur Internet, mais aussi d'intercepter une frappe sur un clavier distant. Aussi, il est essentiel d'innover en permanence et d'inventer de nouveaux moyens de communication indétectables.

En mai 2013, la Russie a expulsé à Ryan C. Fogle, troisième secrétaire de l'ambassade américaine à Moscou, après avoir publié sur le site de *Russia Today* des photos de lui portant une perruque blonde mal ajustée et d'une étrange collection d'accessoires saisis lors de son arrestation par le Service fédéral de sécurité (FSB) : quatre paires de lunettes de soleil, une carte routière, une boussole, une lampe de poche, un couteau suisse et un vieux téléphone Nokia. Derrière ces accessoires que l'on pourrait considérer d'un autre âge se cachaient en réalité des gadgets d'espionnage beaucoup plus sophistiqués que leur apparence ne le laisse penser. Le Nokia de dissimulait en effet un dispositif de communication secret, dernier cri. Le « diplomate » américain était également équipé d'un bouclier RFID, une pochette de blocage de l'identification par radiofréquence destinée à empêcher de le suivre électroniquement.

Aujourd'hui, les opérateurs clandestins utilisent des appareils de communication cryptés très spéciaux, mais aussi de dizaines d'émetteurs et de récepteurs différents, transmettant en « mode rafale », dissimulés dans des objets courants. Un dispositif de communication secret peut être par exemple un faux rocher ou une fausse brique implantée dans un mur ; il peut être doté d'un dispositif de transmission, d'écoute ou d'observation fonctionnant sur batterie, comme cela a été pratiqué lors de missions de reconnaissance et de surveillance en Afghanistan. Ces dispositifs sont implantés secrètement par les membres des unités de soutien des opérations spéciales. Pour activer les communications, il suffit à un opérateur de passer devant le récepteur cible et les messages clandestins sont aussitôt cryptés et renvoyés vers des centres de réception.

Mais ces méthodes d'espionnage peuvent aussi être utilisées par les ennemis des Etats-Unis. Le développement rapide de technologies de l'information pose également des défis en matière de sécurité opérationnelle comme pour la protection des forces. En 2015, État islamique a publié les noms, photos et adresses de plus de 1 300 militaires américains, donnant pour instruction à ses partisans de les éliminer. Selon le FBI, chargé de l'enquête sur ces vols de données confidentielles, cette liste aurait été exploitée par des pirates informatiques russes se faisant passer pour des membres de Daech qui ont menacé les familles de militaires par le biais de Facebook. En 2016, l'organisation djihadiste poursuivit son action en publiant plus de 8 300 noms de cibles, puis 8 700 en 2017. En 2018, des militaires américains ayant partagé leurs informations sur l'applications de jogging Strava ont révélé leurs lieux d'opérations.

En conséquence, les responsables de la sécurité et du contre-espionnage du Pentagone ont entrepris une sensibilisation à grande échelle pour avertir les personnels militaires et leurs familles de mieux protéger leurs informations personnelles sur les médias sociaux [2] .

[1] William M. Arkin, « Exclusive : Inside the Military's Secret Undercover Army », *Newsweek* , 17 mai 2021 (https://www.newsweek.com/exclusive-inside-militarys-secret-undercover-army-1591881)

[2] Cet article a également fait l'objet d'une publication dans le magazine *RAIDS* , Hors série n°81, janvier/février/mars 2022.