Sécurité globale

N° 8, nouvelle série [N° 34 de la série originale]

Sécurité globale

Editions ESKA
12, rue du Quatre-Septembre - 75002 Paris
Tél. : 01 42 86 55 65 - Fax : 01 42 60 45 35
Site : www.eska.fr

RECOMMANDATIONS AUX AUTEURS

Le comité de rédaction de la revue est ouvert à toute proposition d'article.

Les auteurs sont priés de respecter les lignes directrices suivantes quand ils préparent leurs tapuscrits :

- ✔ Les articles ne doivent pas dépasser 40 000 signes (notes et espaces comprises).
- ✔ Les articles doivent êtres inédits. Si justifié par un intérêt éditorial précis, la rédaction accepte néanmoins les versions longues et étayées d'articles préalablement parus.
- ✔ Deux résumés, l'un en français, d'une dizaine de lignes maximum et un autre, en anglais, de la même importance, doivent être fournis avec le manuscrit, accompagnés de la qualité et la liste des dernières publications de l'auteur.
- ✔ Une bibliographie sommaire peut éventuellement être jointe aux articles.
- ✔ Les auteurs feront parvenir leur article par Internet à l'adresse suivante : agpaedit@wanadoo.fr en format MS Word (.doc ou .rtf) ; Times New Roman 11 justifié, interlignes simples.
- ✔ Les auteurs doivent joindre dans un fichier séparé portant mention de l'ensemble de leurs contacts : courriel, adresse postale et le cas échéant numéro de téléphone.
- ✔ L'article doit être présenté de la manière suivante : titre en Times 14, suivi, à chaque fois à la ligne, du prénom et du nom de l'auteur, de sa qualité (notice biographique), du résumé français/anglais et du corps du texte.
- ✔ Les auteurs sont invités à structurer leurs analyses par intertitres afin de faciliter la lecture.
- ✔ Lors de la remise de l'article à la rédaction les fichiers Word doivent être titrés de la façon suivante : NOM (de l'auteur en majuscules) – titre (de l'article en minuscules)
- ✔ Tous les tableaux, graphiques, diagrammes et cartes doivent porter un titre et être numérotés en conséquence et sourcés s'ils ne constituent une œuvre originale. Toutes les figures doivent être transmises séparément en fichiers jpeg ou pdf d'une résolution suffisante (idéal 300 dpi) et leurs emplacements doivent être clairement indiqués dans le texte.
- ✔ Réduire au minimum le nombre de notes, et les placer en notes de fin selon le système de référencement Word.
- ✔ Tous les textes qui ne correspondraient pas aux critères linguistiques standards et aux exigences de rigueur critique seront renvoyés aux auteurs pour adaptation.
- ✔ Une attention particulière devra être portée à la ponctuation : guillemets français, majuscules accentuées (État, À partir de, Égypte, etc.) et à un usage modéré des majuscules conformément aux règles typographiques.

Référence : Collectif, *Lexique des règles typographiques en usage à l'imprimerie nationale*, Imprimerie Nationale, Paris, 2002.

Les articles signés expriment la seule opinion de l'auteur et ne sauraient engager la responsabilité de la revue.

Sécurité Globale | N°8, nouvelle série | N°34, série originale
Revue trimestrielle | © Editions ESKA

ISSN : 1959-6782 • ISBN : 978-2-7472-2664-6 • CPPAP : 0916 K 90246

Imprimé en France

Sommaire

N°8, Nouvelle série 2016

Dossier
Cyber-chaos et sécurité numérique

Géopolitique

Rubriques et chroniques

Bulletin d'abonnement ou de réabonnement, page 160

Introduction

De la cyber-jungle au cybermonde

Xavier RAUFER

Quatre thèses fondatrices de la cyber criminologie[1]

- *Diagnostic 1* - Dans l'ensemble «cyber-crime», crime domine. Scruter le monde cyber-criminel révèle qu'il n'a rien inventé d'original. Dans leur milieu et jusqu'à présent, les cybercriminels se bornent à reproduire les variantes de la criminalité physique.

- *Diagnostic 2* - La cybercriminalité ne baissera pas par plus encore de haute technologie, mais par *décision* politique. Dans ce domaine, une fuite en avant type blindage-et-canon provoquerait un désastre analogue à celui de l'inepte guerre *high-tech* d'Irak.

- *Traitement, 1* - Il faut au cybermonde un code de la route comme, en son temps, la société de l'automobile suscita le sien. Un code conçu et imposé par une coalition de nations puissantes, dans l'espoir raisonnable qu'il s'imposera mondialement. Autre image pour l'indispensable superstructure normative : celle de la tour de contrôle.

- *Traitement, 2* - Le code de la route vaut pour tout véhicule, luxueux ou modeste : de même, seul un code du cybermonde sanctionnera-t-il vraiment les prédateurs, financiers maraudeurs, géants du net, etc., qui, aujourd'hui, le pillent impunément ou exploitent ses usagers.

CRIME et monde numérique - le problème aussi mondial qu'énorme - d'abord, par la taille de ses acteurs de premier plan :

- Facebook a 1,7 milliard d'utilisateurs qui en moyenne, passent quelque 50 minutes par jour sur ses sites et applications ;
- Autre titan de l'Internet, Apple a vu en 2015 son chiffre d'affaires atteindre 234 milliards de dollars.

Ainsi, tout ce qui circule, invente, construit, vend, paie, etc., sur la planète s'inscrit désormais dans un cybermonde qui, en matière de sécurité et sans doute pour longtemps encore, ressemble fâcheusement à la Banque de France - moins les coffres forts.

Cour des miracles et Piste Ho-Chi-Minh à la fois, le cybermonde est presque sans défense ; trop souvent, bandits, pirates, espions, saboteurs, etc., s'y ébattent, volent et pillent à leur aise. Or comme il est toujours aussi ardu d'attribuer précisément une attaque dans le monde numérique, les cybermalfaiteurs se rient d'une répression semblable à l'Arlésienne d'Alphonse Daudet, qu'on attend toujours - mais ne vient jamais. Cela bien sûr, ces malfaiteurs adorent.

Or trop souvent, les Etats et grands groupes font comme si la menace était secondaire ou anodine. Ils assurent le minimum syndical, une rustine ici, un sparadrap là, espérant que le méga-piratage, ou le super-sabotage, attendra la prochaine élection ou le prochain bilan. Quand au commerce de la cyber-sécurité, il tend à s'enfermer dans une logique d'ingénieurs, considérant - idée Ô combien fausse - qu'un souci technique se corrige par plus de technique encore. Ce dans le mépris de tout ce qui n'est pas codeur. Pour ces preux chevaliers du cybermonde en effet, l'usager moyen de l'informatique et de l'Internet n'est qu'une sorte de simplet, défini en langue *Geek* par la formule PICNIC (*Problem In Chair, Not In Computer*).

Cependant, les signes avant-coureurs d'un cyber-chaos aggravé se multiplient ces derniers mois. En voici quelques uns de préoccupants pour des domaines stratégiques : défense, monde des entreprises, finance, crime organisé, etc.

■ **DÉFENSE** : en août 2016, on apprend que la célèbre et effrayante NSA (*National Security Agency*) s'est fait voler d'ultrasecrets outils de piratage, conçus par l'unité d'élite de l'agence, le TAO (*Tailored Access Operations*, opérations d'accès sur-mesure). Un groupe de hackers nommé *Shadow Brokers* (en référence aux personnages d'un jeu vidéo) organise sur le site *Pastebin* une ironique et humiliante vente aux enchères ; qui veut acheter les jouets du service secret le plus secret au monde ? Dans la communauté américaine du renseignement en effet, ses rivaux prétendent que NSA signifie «No Such Agency»...

Les mois suivants, la réalité éclate : vieux en fait de 16 ans ce piratage de la NSA est (à l'instant...) le vol de documents secrets le plus massif de l'histoire ; immensément plus que le vol d'Edward Snowden en 2013.

On parle de «plusieurs terabytes de données» volées. Pour les Béotiens, un terabyte équivaut au contenu en volume d'environ un million de livres.

Là resurgit le bon vieux facteur humain - celui qui affecte nos cyber-ingénieurs eux-mêmes... Car le pillard présumé (qui travaillait pour TAO) est un *geek* parmi d'autres, un peu poivrot, se prenant pour James Bond, perdu dans le grand jeu numérique et voulant sauver le monde du cyber-diable. Des «montagnes de documents» sont retrouvés par le FBI dans le foutoir de sa vie personnelle, entre sa voiture, un logis en grand désordre et une baraque à outils...

■ **GAFA & co. : victimes eux aussi.** GAFA, ce sont les quatre titans de l'Internet : Google, Apple, Facebook et Amazon. Libertaires d'idées et de pratiques, ces géants sont à leur tour victimes des pirates. Le 21 octobre 2016 : *Amazon, eBay, Spotify, Airbnb, Netflix, Paypal, Twitter* ; les jeux en ligne de *Playstation* et de *XBox* ; rayon médias, *CNN*, le *New York Times*, le *Boston Globe*, le *Financial Times*, le *Guardian*, sont inaccessibles des heures durant ; mondialement, des millions (minimum) d'usagers sont privés d'accès à ces serveurs majeurs.

L'attaque informatique géante qui les frappe tous cible en fait DYN, société prestataire dans le domaine des DNS (*Domain Name System*). L'attaque a été menée par un «Bot» exploitant les failles de sécurité des objets connectés (caméras de surveillance, téléviseurs, etc.). Relais possibles d'attaques majeures, ces objets connectés sont désormais des millions (voitures autonomes... domaine de la santé... maisons «intelligentes», etc.) et à ce jour, nul antivirus ne les sécurise vraiment.

Qui sont les pirates ? Comme d'usage les «experts», officiels ou privés, pataugent et n'en savent en réalité rien. Ils pressentent cependant que la généralisation du *Cloud* et des *Smartphones* n'arrangera pas les choses... Déjà, *Yahoo*, *MySpace*, *LinkedIn* ont subi de massifs pillages : environ 1,5 milliard de comptes «braqués» par des pirates de l'été 2015 à l'été 2016. (*Yahoo* : ± 500 millions de comptes piratés ; *MySpace*, 427 millions ; *LinkedIn*, 117 millions).

Que cherchent les pirates dans ces pillages ? Des comptes «pépites», où figurent : identifiants, adresses de courriels, mots de passe, adresses postales ; mieux, des dates d'anniversaires et références bancaires. Ce luxe de données autorise des arnaques sur mesure, personnalisées, pouvant viser des particuliers, des entreprises ou des institutions.

Pour les grands groupes, notamment dans le domaine de l'énergie, la sécurité numérique tourne au cauchemar stratégique. En 2018, les seules sociétés pétrolières investiront 1, 87 milliard de dollars pour se protéger.

■ **FINANCE, classique ou Bitcoin** : fonctionnant depuis 1977, la plateforme financière SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) est

le réseau sanguin de la finance mondiale. Or en février 2016, la Banque d'Etat du Bangladesh a subi un braquage de 81 millions de dollars - la banque étant ciblée plus que la plateforme Swift elle-même, mais à travers celle-ci. De par le monde, d'autres structures financières ont subi des pertes lors d'attaques analogues ; d'abord en Asie (Japon, Philippines, Vietnam), mais aussi aux Amériques (Nord, Latine), en Europe et en Australie.

A l'automne 2016, la City de Londres s'alarme de la forte augmentation des attaques visant les institutions financières britanniques : on en comptait 5 pour toute l'année 2014 ; il y en a eu 75 de janvier à septembre 2016. Toutes cibles confondues et pour l'année 2015, le Royaume-Uni a subi environ 2,5 millions de *cybercrimes*, dont 250 000 seulement ont fait l'objet de plaintes auprès de la police.

Côté Cybermonnaies, on note l'inquiétant enthousiasme du WEF-Davos, notoire agent d'influence de la DGSI (Davos-Goldman-Sachs-Idéologie), pour la technologie *Blockchain*, issue de l'architecture *Bitcoin*. Inquiétude car par le passé, la DGSI, le WEF Davos et consorts ont toujours dédaigné toute stratégie sérieuse visant à protéger la planète des prédations financières.

Ce, alors que les monnaies, ou devises, virtuelles sont toujours aussi fragiles. Début août 2016, on apprend le piratage de *BitFinex*, l'une des grandes plateformes mondiales d'échanges de Bitcoins : 60 millions de Bitcoins «braqués» par des auteurs (comme d'usage...) inconnus et introuvables. Autre pillage en juin 2016 : la plateforme DAO (*Decentralized Autonomous Organization*) se fait voler environ 50 millions de dollars d'une autre monnaie digitale nommée «Ether». Rappelons que déjà en 2014, l'importante plateforme *Mt.Gox*, de Tokyo, avait vu «disparaître» 119 756 Bitcoins (valeur lors du vol, 72 millions de dollars).

■ CRIME ORGANISÉ : celui-ci pille et pirate la finance numérique, surtout en usant de deux armes/techniques/méthodes. Le «siphonage» des DAB (Distributeurs automatiques de billets) et le *Ransomware*, qui voit un pirate verrouiller l'accès à un ordinateur ou à des données personnelles puis les libérer contre rançon (d'usage payée en *Bitcoins* sur un compte exotique.

En mai 2016 dans 17 préfectures du Japon, Tokyo inclus, d'importants clans yakuza (Yamaguchi Gumi, Kobe Yamaguchi Gumi, Dojin-Kai, Inagawa-Kai, Sumiyoshi Kai et Godda-Ikka), associé à des pirates-experts, multiplient les retraits de 100 000 yen (maximum autorisé) sur des cartes de paiement trafiquées, à l'origine émises par la *Standard Bank of South Africa*. Butin total : 1,8 milliard de yens (1, 75 million de dollars).

Côté *Ransomware*, spécialité du monde russe, des entreprises cybercriminelles comme «Petya» et «Misha» se spécialisent dans ces formes de «kidnapping numérique»,

devenues un véritable *business* parallèle, avec son marketing, la création de «franchises» et la vente d'outils criminels spécifiques (avec modes d'emploi vidéo, etc.).

■ **DEMAIN, l'avenir proche** : Les cyberguerres ne sont plus une lointaine fiction. Dans la constamment excellente *New York Review of Books* ((29/09/2016) Un expert observe : «Les cyber-armes sont furtives. Ni explosions ni boules de feu : comme tout en informatique, elles se composent de 0 et de 1 ; on s'en sert pour infiltrer en douce des machines individuelles, ou des réseaux entiers. Frappant précisément, elles peuvent paralyser d'immenses infrastructures, brouiller les signaux de l'ennemi, interrompre des communications ; aussi, riposter à des attaques, et les neutraliser, avant même qu'elles ne débutent». Selon Edward Snowden, les Etats-Unis ont mené dès 2011 213 de ces cyber-attaques - qui sont bien d'ordre militaire : «chaque fois que *Stuxnet* était déclenché (virus censé paralyser les centrifugeuses iraniennes produisant de l'uranium de qualité militaire) un officier de la CIA se tenait derrière l'opérateur de l'ordinateur et lui donnait l'ordre d'attaquer».

Enfin, les capacités criminelles de l'intelligence artificielle («*machine learning*»), domaine de recherche majeur de l'informatique de demain. Bientôt, vous risquez d'entendre au téléphone une voix familière : proche, collègue... La «voix» sera aux mains de pirates voulant vous piller, vous manipuler, vous induire à faire ceci, vous pousser à interrompre cela. Le logiciel existe déjà : c'est donc pour bientôt.

Ainsi - comme les criminologues l'observent de longue date - logiciels et algorithmes ne sont qu'une moderne version de la langue d'Esope, meilleure et pire des choses à la fois. Mais si la sagesse grecque des origines l'enseignait déjà voici vingt-cinq siècles, des ingénieurs un peu perdus dans le champ du seul calculable l'entrevoient à peine...

Annexe : La criminalité de l'Internet aux Etats-Unis en 2015, selon le FBI

(Il y a quelque 270 millions d'usagers de l'Internet aux Etats-Unis début 2016, sur une population de ± 323 millions d'habitants)

Statistiques générales

Niveau fédéral (national), Etats-Unis : environ 1,08 milliard de dollars de préjudices constatés pour l'année de référence ; 288 012 plaintes reçues, dont 127 145, suite à une perte financière (perte moyenne : $ 8 421).

Infractions-Internet signalées

- par le biais de réseaux sociaux : 19 967
- par usage des monnaies virtuelles : 1 920

Type d'infractions signalées *(10 000 victimes ou plus)*

- Défaut de paiement ou de livraison : 67 375 *infractions signalées*
- Surfacturation (419, *nigérianes*) : 30 885
- Vol d'identité : 21 949

- Enchères truquées/fraudes : 21 510
- Vol de données personnelles : 19 632
- Fraudes à l'emploi : 18 758
- Extorsion : 17 804
- Fraudes à la carte de paiement : 17 172
- Phishing & analogue : 16 594
- Fraudes à l'avance sur paiement : 16 445
- Intimidation et violence : 14 812
- Escroquerie sentimentale ou à la confiance : 12 509
- Escroquerie à la qualité : 11 832
- Escroquerie dans l'immobilier : 11 532

Plus de cent millions de dollars US de préjudice

- Usage frauduleux d'emails dans les affaires (escroquerie «au président» ou à l'israélienne : 264,3 millions de dollars de préjudice
- Arnaque à la confiance ou aux sentiments : 203,4m.$
- Arnaque au paiement ou à la livraison : 121, 4m.$
- Arnaque à l'investissement : 119,2m.$

Sources

Xavier Raufer «Cyber criminologie» - CNRS Editions, 2015

US Department of Justice - BBI 2015 Internet Crime Report

New York Review of Books - 27/10/2016 «They've got you, whenever you are»

New York Times International - 25/10/2016 «As artificial intelligence evolves, so does its criminal potential»

Le Parisien - 23/10/2016 «Piratage massif de sites Internet : quand les objets connectés attaquent»

Le Parisien - 22/10/2016 «Ce qui se cache derrière la cyberattaque massive qui a touché Internet»

New York Times International - 20/10/2016 «Trove of stolen data is said to include top secret US hacking tools»

Le Figaro - 18/10/2016 «Cybersécurité : pourquoi les entreprises sont de plus en plus vulnérables»

Reuters - 14/10/2016 «Banks are hiding their cyber-attacks»

GNT (Site) - 13/10/2016 «Cyber menace : le crime organisé s'empare du ransomware»

Yomiuri Shimbun - 4/10/2016 «6 yakuza crime groups implicated in Y. 1.8 Billion ATM scam»

Le Point - 2/10/2016 «Réseau interbancaire : les attaques de pirates informatiques continuent»

New York Review of Books - 29/09/2016 «US cyber weapons our demon pinball»

Libération - 18/08/2016 «La NSA dans le viseur de Shadow Brokers»

New York Times International - 15/08/2016 «Bitcoin technology seen going global»

New York Times International - 4/08/2016 «Hacking at Bitcoin exchange»

Note

[1] «Cyber criminologie», Xavier Raufer, CNRS-Editions, 2015.

Dossier | Cyber-chaos et sécurité numérique

Dossier conçu avec l'aide précieuse d'Alain Establier, éditeur de la lettre «*Securité Defense Business Review*»

Alain Establier est le rédacteur en chef de «SECURITY DEFENSE Business Review» (SDBR*), lettre d'information bimensuelle en français, couvrant les sujets du **continuum Défense et Sécurité**. Alain Establier est universitaire (Droit + IAE) et l'auteur de nombreux articles sur le contrôle interne, la sûreté aérienne, la gestion des risques, d'un ouvrage "Et si nous parlions de la performance dans votre Entreprise ?" Eyrolles 1988, et le co-auteur de « Sûreté - Mode d'emploi » Ellipses 2011.

«SECURITY DEFENSE Business Review» (SDBR) : Depuis le 01/09/2009, cette lettre d'information électronique-confidentielle en français couvre le **continuum Défense-Sécurité,** notamment la cybersécurité et la cyberdéfense. Bimensuelle, elle publie 22 numéros par an. Elle s'adresse aux dirigeants et aux responsables opérationnels des entreprises privées ou publiques, aux élus, et aux décideurs des administrations et établissements mixtes. SDBR s'intéresse aux moyens de sûreté, à la vie des industries de Défense et de Sécurité, à la géopolitique-géostratégie, à la lutte contre les terrorismes, à l'intelligence économique, à la cybersécurité, à la recherche dans le champ du C4i, à la protection des moyens de transport, au Crime organisé et au narcotrafic, etc.
Le site www.securitydefensebusinessreview.com donne les modalités d'abonnement.

Entretiens réalisés par Alain Establier (par ordre de présentation dans cette étude) :

commissaire divisionnaire Jean Marc Souvira ; colonel Nicolas Duvinage ; général Michel Masson ; général Christophe Gomart ; professeur Kavé Salamatian ; MM. Philippe Courtot, Franck Greverie, Laurent Hesnault, Alain Bouillé, experts de haut niveau ès-cyber sécurité, général Marc Watin-Augouard ; vice-amiral Arnaud Coustillière ; ICA Frédéric Valette ; M. Guillaume Poupard, DG de l'ANSSI, M. Alain Juillet et le CCED Constant Hardy.

La sécurité numérique par ceux qui la conçoivent et la pratiquent

Alain ESTABLIER

Introduction

Dans le numéro 5 (NS) de *Sécurité Globale*, nous avons pu lire un excellent article de Tewfik Hamel intitulé « la lutte contre le terrorisme et la criminalité : un changement de paradigme ? » dans lequel l'auteur analysait la relation entre terrorisme et criminalité au regard de la situation vécue en Algérie. L'auteur y soulignait l'impact du terrorisme sur les populations civiles et l'apport des nouvelles technologies (internet, cyber, réseaux sociaux, etc.) aux guérillas armées et aux entités criminelles de toutes sortes pour leur permettre de proliférer. L'auteur soulignait aussi dans son article le déplacement des situations de conflits vers l'espace urbain : « les conflits futurs adviendront dans les rues, les gratte-ciel, les égouts, les immeubles, les parcs industriels des villes urbanisées » prophétisant ainsi avec Paul Virilio (The city of Panic, Berg publications, Oxford 2005) que « la guerre moderne sera une guerre de civils qui, à l'aide de communications instantanées, débouchera sur une guerre civile mondiale (l'équivalent mondial des émeutes de Los Angeles en 1992) ».

"SECURITY DEFENSE Business Review" (SDBR) suit depuis 2009 l'évolution de la Menace et les implications technologiques en matière de Défense et de Sécurité, publiant dans ses colonnes, au fil des mois, des responsables et experts du « continuum défense et sécurité ». Alain Establier, son rédacteur en chef, a sélectionné pour *Sécurité Globale* diverses interviews récentes (toutes réalisées par lui-même) pour illustrer les thèmes suivants :

1. La criminalité organisée, menace pour la société
2. Le Renseignement, outil essentiel de la lutte contre la menace
3. Cyber : la menace au quotidien
4. Le monde cyber : menaces, parades, le rôle de l'Etat
5. Les interceptions de communication

1. La criminalité organisée, vraie menace pour la société

Le 26 mai 2015, SDBR a publié dans son numéro 128 une large interview du commissaire divisionnaire Jean-Marc Souvira qui était alors Chef de l'Office Central pour la Répression de la Grande Délinquance Financière, dépendant du ministère de l'intérieur français. En voici des extraits qui sont révélateurs de l'existence de la menace criminelle et des implications pour la société.

SDBR : Qu'observez-vous dans le comportement des organisations criminelles ?

Jean-Marc Souvira : Les groupes criminels se sont très vite adaptés aux nouvelles lois sur les saisies d'avoirs criminels, en organisant leur insolvabilité et en plaçant rapidement leur argent ailleurs, marchant en cela sur les traces des mafieux italiens qui le font depuis longtemps. Quelque soit le délinquant, du plus petit au plus grand, la saisie des avoirs criminels est considérée comme la peine principale, l'emprisonnement devenant pour lui la peine accessoire. Pour comprendre cela, il faut simplement rappeler que le vol est rarement commis pour le bien en soi mais pour l'argent que le voleur peut retirer du bien volé. Le voleur peut voler un téléphone portable pour son usage, mais s'il vole plusieurs cartons de téléphones c'est bien leur valeur d'échange qui l'intéressera. La plupart du temps, les délinquants n'ont qu'un objectif: l'argent. La saisie de leurs profits étant toujours douloureusement vécue par les délinquants, le législateur a progressivement élargi l'assiette des saisies à la confiscation en valeur. Exemple: si une infraction commise par un délinquant a rapporté 500.000 euros, qu'il ne les possède plus, en revanche s'il possède un bien immobilier d'une valeur au moins équivalente dont nous ne connaissons pas la provenance, la PIA (plateforme d'identification des avoirs criminels) peut saisir ce bien. La loi sur les saisies a aussi été élargie au bénéficiaire économique, pour lutter contre l'insolvabilité économique : par exemple, si le délinquant achète avec le produit de ses trafics des biens mobiliers et immobiliers à ses proches, ces biens pourront être saisis puisque les proches sont des bénéficiaires économiques (qui en tirent profit).

Et ça marche ?

Tous les services de police et de gendarmerie ont intrinsèquement cette culture de la saisie, ce qui fait que les chiffres progressent régulièrement depuis l'instauration de la loi: en 2006, 71M€ ont été saisis et, en 2014, il y a eu 458M€ saisis soit 6,5 fois plus ! Nous travaillons avec l'AGRASC, l'agence de gestion et de recouvrement des avoirs saisis et confisqués créée en 2010, qui administre les biens saisis.

Quel est le volume d'affaires traité par l'OCRGDF *?

*Nous sommes constamment sollicités par les JIRS**, peut-être à cause des succès ren-*

contrés sur certaines affaires, ce qui nous amène à traiter en permanence plus de 300 dossiers; c'est un portefeuille d'activité très lourd à gérer. En moyenne, le traitement d'un dossier dure deux ans. Il peut arriver que certains dossiers puissent être bouclés en six mois, mais c'est assez exceptionnel. C'est un travail de spécialistes de la police judiciaire et ces officiers ont reçu, en outre, une formation à l'enquête financière dans la lutte contre toutes les formes de criminalité organisée : trafic de stupéfiants, réseaux de proxénétisme, d'extorsion de fonds, braquage de fret, vols d'œuvres d'arts, etc. Tous les dossiers que nous traitons ont toujours un pied hors de nos frontières, car tout système de blanchiment d'argent s'entend en dehors de nos frontières. Les délinquants n'évacuent pas l'argent de Paris à Marseille, mais le feront circuler, via la Belgique, en direction de Dubaï, des EAU, du sud-est asiatique, d'Israël ou de la Chine, par exemple. Les systèmes de blanchiment sont industriels, car le fonctionnement économique de ces groupes criminels est comparable à celui des grandes entreprises: avec des produits à vendre (stupéfiants par exemple), des logisticiens, des recherches de canaux d'évacuation de l'argent, etc. Nous observons des conjonctions d'intérêts entre structures criminelles, selon la spécialisation de chacune: fabrication du produit, transport, vente, etc. Ensuite ces structures s'adossent à d'autres, de nationalités différentes, pour gérer l'argent: exemple, un groupe franco-marocain traitant la résine de cannabis adossé à un groupe indo-pakistanais pour évacuer l'argent.

Les politiques ont-ils conscience de ces ramifications internationales ?

Nous avons eu des difficultés à une certaine époque, avec mes collègues des stups, de la criminalité organisée et certains magistrats spécialisés, pour faire entendre que la criminalité organisée était une réalité en France. Quel est le fonctionnement d'une mafia (mafia s'entendant dans un sens générique) ? C'est un groupe criminel qui accapare un territoire par la violence et le maintient par une dépendance financière. Derrière ce premier niveau d'existence sur un territoire, vous trouverez la corruption, la captation de marchés publics, la prise illégale d'intérêts, etc. Et bien, il y a des mafias en France! Une des plus importantes criminalités organisées en France est celle des Corso-Marseillais. Aujourd'hui, la sphère politique et judiciaire a intégré que nous faisions face aussi à des groupes autres, tels des Georgiens ou des Arméniens qui sillonnent la France pour se livrer à des vols en masse, comme par exemple des moteurs de bateaux ou des pots catalytiques très recherchés par des fondeurs pour récupérer les métaux rares. Ces vols, pris de manière isolée, sont qualifiés de basse intensité mais, reliés les uns aux autres, donnent une autre physionomie de groupes qui agissent comme des prédateurs...Un marché de 450 millions d'habitants, c'est bien pour le commerce ou les études, mais c'est aussi formidablement bien pour la criminalité organisée qui profite du système: ainsi l'Euro leur permet de sillonner l'Europe avec la même monnaie, sans se livrer à des changes de monnaie, une fois les infractions commises. Les délinquants ont 3 milliards d'eu-

ros par an à blanchir sur le trafic de stupéfiants en France, ils travaillent donc aussi sur les parités de change: euro/dollar, euro/or, euro/métaux rares, etc. Tous les services de PJ travaillent avec leurs homologues étrangers, européens ou autres. Les groupes sur lesquels nous travaillons ne se rencontrent pas sur le Dark Web. Ils sont toujours mis en relation par une tierce personne de confiance, car nous sommes en présence d'une économie-bis qui fonctionne comme l'économie réelle. Par exemple, il existe en France un système de banques parallèles, tenues pour partie par la communauté asiatique, qui fait circuler des centaines de millions d'euros en dehors du système bancaire. Ce sont des points de croissance qui quittent régulièrement la France, car l'argent quitte toujours le territoire national pour s'investir, par exemple en immobilier, au sud-est asiatique, au Maghreb, en Israël ou en Chine. Sur les 3 milliards d'euros du trafic de stups 2,5 environ quittent le territoire national chaque année. C'est considérable. L'ensemble des fraudes annuelles en France (fraude à la TVA comprise) est de l'ordre de 80 milliards. La PIAC saisit environ 450 millions par an, ce qui ne représente que 5% du total...

Travaillez-vous sur les fraudes aux entreprises ?

Oui, nous travaillons sur ces fraudes majeures qui permettent à des escrocs d'obtenir des informations sur leurs cibles, qui sont les entreprises françaises: internet, carte de paiement prépayée, plate-forme dématérialisée, tout ce qui permet d'anonymiser leur démarche. La dérégulation du système bancaire et les nouveaux moyens de paiements, mis en place pour favoriser les échanges et le commerce, sont utilisés par les escrocs. Les entreprises sont des proies faciles du fait de leur vulnérabilité financière. En quatre ans, 350 millions d'euros ont été dérobés aux entreprises françaises (par des attaques du type fraude au Président, virement SEPA, changement de RIB, etc.) et 100% de ces attaques sont parties d'Israël. Ce sont des escroqueries très intelligemment montées, avec des sociétés fictives réparties dans différents pays européens, qui montrent une grande et longue expérience des escrocs: on retrouve trace de gens impliqués dans les affaires du Sentier de Paris dans les années 1990, ou de la fraude à la taxe carbone plus récemment. On note d'ailleurs que les groupes franco-israéliens ont des conjonctions d'intérêts avec les groupes asiatiques pour activer des systèmes de compensation. Il est anormal que ce soient les escrocs qui révèlent les failles de sécurité d'une entreprise. On sent souvent les responsables démunis face à ce genre de problématique, à mille lieues de penser pouvoir être attaqués, car l'entreprise a du mal à identifier une menace qu'elle ne voit pas (contrairement à un vol à l'arraché dans la rue, par exemple) et a toujours tendance à minimiser son impact. Or, derrière ces attaques, se cachent des structures de destruction massive qui sont à l'œuvre et mettent leur intelligence au service de la destruction d'un tissu économique!

Ces grands réseaux criminels sont-ils liés au financement du terrorisme ?

Nous sommes confrontés à diverses formes de terrorismes: le terrorisme corse, qui mélange l'argent de la criminalité organisée et l'argent des revendications politiques (impôt révolutionnaire par exemple), le terrorisme basque (qui a pour l'instant déposé les armes) et le PKK (qui ponctionne des millions d'euros sur l'Allemagne et la France auprès des commerçants turcs par le biais d'extorsion). Concernant le terrorisme islamique, qui nous préoccupe, nous sommes face à des micro-financements (quelques milliers d'euros) provenant de petites fraudes (petits emprunts non remboursés, etc.): dans le cas d'affaires récentes, la Presse a rapporté qu'un des financements possibles était l'importation en petite quantité de produits contrefaits en Chine pour les revendre sur Internet en France.

Considérez-vous le risque lié à l'outil numérique comme un danger de délinquance non maitrisé ?

Absolument ! La cybercriminalité est avant tout de la criminalité tout court, simplement avec d'autres moyens. Sur le terrain de l'Internet, on observe absolument toutes les infractions connues, Internet servant soit à constituer l'infraction, soit à réaliser l'infraction, soit à évacuer l'objet de l'infraction (données) ou l'argent obtenu. C'est tellement facile, de votre bureau via Internet, de créer une société au Panama et un compte bancaire à Hong-Kong, sans se déplacer. Il y a une nouvelle facilitation des actes de délinquance grâce à cette technologie.

* L'OCRGDF dépend de la sous-direction de la lutte contre la criminalité organisée et la délinquance financière (SDLCODF), elle-même rattachée au directeur central de la police judiciaire (DCPJ) qui rapporte au directeur général de la police national (DGPN). L'OCRGDF couvre la brigade centrale pour la répression des fraudes communautaires (BCRFC), la brigade de recherches et d'investigations financières nationales (BRIFN), la section anti-blanchiment et lutte contre le financement du terrorisme (SAB) et la plate-forme æd'identification des avoirs criminels (PIAC).

** JIRS : juridiction interrégionale spécialisée composée de magistrats du parquet et de l'instruction

• Quels grands enseignements nous livre le commissaire Souvira dans cette interview ?

- Les criminels s'adaptent très vite aux législations pour organiser leur insolvabilité.
- Tout système de blanchiment d'argent est transfrontières.
- Les structures criminelles sont spécialisées : fabrication du produit, transport, vente, financement, etc.
- Il y a des mafias en France !
- La zone Euro est un bienfait pour les criminels qui y circulent librement sans risques de change !
- Les activités des groupes criminels coûtent des points de croissance aux pays européens.
- Les terroristes islamiques n'ont pas besoin de beaucoup d'argent pour faire énormé-

ment de mal (on a pu le constater dans l'année 2016...).
- La cybercriminalité est avant tout de la criminalité tout court, simplement avec d'autres moyens.

Biographie – Jean-Marc Souvira est né à Oran en 1954. Après ses études de Droit en Provence, il passe le concours d'inspecteur de police et, pendant 25 ans, va exercer tous les métiers de policier de terrain au sein de la Police judiciaire avant de devenir commissaire divisionnaire. Il a dirigé l'Office Central pour la Répression de la Traite des Êtres Humains, puis l'OCRGDF (l'Office Central pour la Répression de la Grande Délinquance Financière). Il est actuellement en poste à l'étranger pour la Direction de la Coopération Internationale. Jean-Marc Souvira est aussi auteur de romans policiers : Le magicien (Fleuve Noir, 2008) ; Le vent t'emportera (Fleuve Noir, 2010) ; Les sirènes noires (Fleuve Noir, 2015). Il a été aussi le co-scénariste du film GO FAST qui est sorti au printemps 2008, co-produit par Luc Besson.

* * *

Approfondissons la cybercriminalité avec des extraits de l'interview du Colonel Nicolas Duvinage, Chef du centre de lutte contre les criminalités numériques (C3N) qui dépend du Pôle judiciaire de la Gendarmerie Nationale française, parue le 05 avril 2016 dans SDBR N°147 :

SDBR : Quelles sont les criminalités numériques que vous avez la charge de combattre ?

Nicolas Duvinage : Contrairement à certains de nos voisins européens, nous avons en France une vision extrêmement large des cybercriminalités numériques. Généralement, en Europe ou aux Etats-Unis, la pédopornographie est traitée à part, par des unités dédiées entièrement et uniquement à ce sujet. En France, la pédopornographie est intégrée à la cybercriminalité. De la même façon, dans plusieurs pays européens, ce qui est escroquerie en ligne, vente de stupéfiants sur Internet ou vente d'armes sur Internet, est considéré comme du contentieux armes, délinquance économique et financière ou stupéfiants, pas comme du contentieux cyber. Tout cela est intégré dans les missions du C3N. Bien sûr nous n'intervenons pas seuls, car nous sommes des spécialistes cyber et non des spécialistes armes ou stupéfiants, et nous travaillons main dans la main avec les services spécialisés. Donc la cybercriminalité pour nous va des atteintes aux personnes, aux atteintes aux biens et aux atteintes aux STAD (systèmes de traitements automatisés de données) de la Loi Godfrain.

Quelles sont les atteintes aux personnes ?

Essentiellement pédopornographie, mais aussi « sextorsion » (contraction de sexe et extorsion) ou harcèlement sur Internet. La sextorsion est parfois confondue avec ce que les anglais appellent le « revenge

porn »: des photos ou vidéos prises dans l'intimité du couple puis diffusées par vengeance, par l'un des deux, à l'issue d'une rupture (ex : affaire Laure Manaudou). La sextorsion touche aussi bien les hommes que les femmes avec un mode différent : c'est le fait de se dévêtir et éventuellement de se livrer à des actes pornographiques devant une webcam face à de parfaits inconnus, dans le cadre d'une relation virtuelle, et de se retrouver victime d'un chantage à la diffusion sur Internet des images acquises. Les sextorsions représentent environ 800 victimes actuellement en zone gendarmerie. Dans un autre genre, l'affaire de la diffusion de photos de célébrités aux Etats-Unis relève purement du piratage informatique.

Quelles atteintes aux biens traitez-vous ?

Ce que nous qualifions d'atteintes aux biens concernent toutes les escroqueries sur Internet: locations immobilières, locations de vacances, ventes de biens sur Internet, faux contrats (phishing par faux emails d'une administration ou d'un fournisseur de services), usage frauduleux de cartes bancaires, trafics illicites sur Internet (stupéfiants, armes, faux médicaments, produits dopants ou soumis à ordonnance, contrefaçons de grande marque de luxe, maroquinerie, parfumerie, etc.). Les autres ventes de contrefaçons sur internet (tabac, pièces détachées, etc.) sont du ressort de la Douane. Plus précisément, la contrefaçon est un délit pénal que tout OPJ peut relever (y compris, donc, tout OPJ du C3N) ; toutefois, par choix stratégique, la gendarmerie limite son action anti-contrefaçon à quelques segments spécifiques, alors que la douane combat l'ensemble du phénomène. Entre les atteintes aux biens et les atteintes aux personnes, nous trouvons les usurpations d'identité numérique qui servent à de l'escroquerie ensuite. Nous trouvons aussi l'apologie du terrorisme, qui touche aussi bien les biens que les personnes, que nous avons commencé à traiter en janvier 2015 sur des périodes de mobilisation générale d'un à deux mois.

Et concernant les atteintes aux STAD ?

C'est ce que certains appellent le piratage informatique et qui recouvre en fait le contenu de la Loi Godfrain: piratage de données, piratage de cartes bancaires ou de terminaux de paiement, vol de données, ransomware (ex : Cryptolocker, Locky), atteintes CNIL, défaçage de sites web, etc. Dans ce domaine nous trouvons le RAM-scrapper, un petit logiciel malveillant qui peut être installé sur les caisses enregistreuses ou les terminaux de paiement pour récupérer dans leur mémoire RAM les numéros de cartes bancaires qui y transitent.

La pédagogie faite depuis 4 ans incite t'elle les entreprises à faire des déclarations ?

Pour ce qui est de l'obligation de déclaration faite par la Loi, il est question de fuite

ou de vol de données personnelles, pas de données bancaires, pas de cryptolocker ou autre. Donc il n'y a pas d'obligation légale. Ensuite, je sais très bien que les chefs d'entreprise ne veulent plus entendre le discours «déclarez, déclarez, déclarez», car c'est un discours auquel ils n'adhèrent pas! Les raisons en sont simples: pertes de temps pour des enquêtes dont ils n'entendent plus parler et qui ne résolvent rien de leur préjudice. Donc mon discours est plutôt «portez plainte ou pas, c'est votre choix, mais signalez-nous l'incident» ! Pour nous le signaler, l'envoi d'un simple mail informel, sans ouverture d'un dossier judiciaire et sans convocation, nous permettrait de mieux mesurer le phénomène. Si en plus du signalement, l'entreprise nous envoie quelques logs de l'attaque, nous pourrons en fonction du nombre de signalements ouvrir une enquête judiciaire de notre initiative, sans que l'entreprise ne soit dérangée ou mobilisée, et nous la tiendrons au courant en cas de succès de l'enquête.

Que faites-vous lorsque vous identifiez, par exemple, une apologie du terrorisme ?

Tout dépend du vecteur qui est utilisé. Si nous sommes sur un réseau de jeu, nous travaillons généralement sur signalement (cyber@gendarmerie.interieur.gouv.fr ou plate-forme de signalement ministérielle PHAROS sur https://www.internet-signalement.gouv.fr/) et nous lançons les enquêtes qui conviennent, qui aboutissent pratiquement toujours à des identifications: en 2015, nous avons eu environ 30 dossiers traités. En termes d'apologie sur Twitter, nous avons pu analyser automatiquement plus de 4.000.000 tweets, ce qui nous a permis de lancer plusieurs dizaines d'enquêtes approfondies et d'identifier 20 individus radicalisés.

Voila 9 mois que vous êtes chef du C3N. Quel constat portez-vous sur son fonctionnement ?

En termes de moyens, la DGGN a décidé de nous accorder des moyens budgétaires et matériels supplémentaires importants pour 2016, par exemple des outils spécialisés de recherche sur Internet ou de surveillance du Dark Web, donc je suis confiant. Nous avons des difficultés juridiques pour travailler sous pseudonymes en termes d'achat (par exemple de stupéfiants), car on ne peut provoquer l'infraction mais seulement attendre l'offre. Mais nous savons fonctionner avec cette contrainte. Par contre, le législateur nous autorise à utiliser le pseudo pour certaines infractions et pas pour toutes. De façon simple et rapide, nous avons le droit pour la pédopornographie, les trafics de produits de santé et les produits dopants. Pour les stupéfiants, le trafic d'armes, le piratage informatique, le trafic de faux papiers et de faux billets, il nous faut la condition préalable de bande organisée. En conséquence, avant de nous faire passer pour un acheteur, nous devons obtenir du Procureur l'autorisation sur la suspicion

de bande organisé, ce qui est quasiment impossible de façon préalable. Donc, il y a un vrai travail législatif à compléter.

• Quelles sont les informations majeures livrées par le Colonel Duvinage dans cette interview ?

- Près de 90% des affaires, dont la Gendarmerie Nationale a connaissance, concernent des escroqueries en ligne.
- Mais les entreprises rechignent à signaler les incidents dont elles sont victimes, ce qui fausse les statistiques et ne facilite pas le travail des enquêteurs, pour le plus grand bien de criminels...
- La pédopornographie est un fléau dont la mesure n'est pas suffisamment prise en compte par le citoyen.
- Le législateur français n'a pas donné, jusqu'à présent, aux forces de police et de gendarmerie, les moyens juridiques permettant de traquer efficacement les bandes organisées...Pourquoi ?

Biographie - Polytechnicien de la promotion X95 et titulaire d'un mastère spécialisé en conception et architecture de réseaux de l'école Télécom ParisTech, le colonel Duvinage a choisi de faire carrière comme officier de gendarmerie à l'issue de ses études d'ingénieur. Après une première affectation comme commandant de peloton à l'escadron de gendarmerie mobile de Besançon (25), il est nommé adjoint (2001-2005) puis chef (2005-2009) du département informatique-électronique de l'institut de recherche criminelle de la gendarmerie nationale. En 2009, il prend le commandement de la compagnie de gendarmerie départementale de Rezé (44), forte de 230 militaires et de 13 unités. De 2012 à 2015, il est chef en second de l'office central de lutte contre les atteintes à l'environnement et à la santé publique, à Arcueil. Depuis le 1er août 2015, le colonel Nicolas DUVINAGE commande le Centre de lutte Contre les Criminalités Numériques (C3N), au sein du nouveau Pôle Judiciaire de la Gendarmerie Nationale (PJGN) de Pontoise.

2. Le Renseignement, outil essentiel de lutte contre les menaces numériques

Au travers des extraits de deux interviews parues dans SDBR, le lecteur pourra mesurer qu'il n'y a pas de lutte possible contre le crime organisé et contre le terrorisme, donc contre les ennemis d'un pays démocratique, sans renseignement, qu'il soit intérieur ou extérieur. Encore faut-il que l'organisation du Renseignement soit pragmatique et évolutive, sans pour autant oublier des principes qui ont produit de beaux succès depuis des décennies...

Rôle et missions de la Direction du Renseignement Militaire (DRM), la réalité du quotidien, grâce à l'interview du Général de Corps d'Armée Michel Masson, ancien directeur du renseignement militaire (2005-2008), parue dans SDBR n°136 le 20/10/2015.

SDBR : L'organisation actuelle du renseignement en France vous parait-elle adaptée aux défis qui se posent ?

MM : Je crois sincèrement qu'elle est adaptée, au vu de notre histoire et de notre culture du renseignement et de la sécurité. Toutefois, le rôle, les prérogatives et les moyens du Coordonnateur doivent être revus. Il faut ensuite passer d'une gouvernance centrée sur les ministères à une gouvernance centrée sur les services de renseignement. Dès la mise en place du poste de Coordonnateur, en 2008, les ministres de tutelle des différents services n'ont jamais accepté de se départir de leurs prérogatives organiques. La Délégation parlementaire au Renseignement, avec les pouvoirs renforcés que lui donne la LPM 2014-2019 (à condition toutefois que les parlementaires eux-mêmes s'y intéressent et s'investissent), devrait se pencher sur ce sujet. Pour pouvoir efficacement combiner mutualisation et gouvernance accrues, le rôle du Coordinateur doit être renforcé. Aujourd'hui, il joue au sein de la communauté nationale du renseignement un rôle d'animation et de secrétariat, mais ni de stimulation ni d'impulsion, ce dont la communauté a besoin. Sa lettre de mission ne lui donne pas suffisamment de prérogatives et il ne dispose pas dans son entourage du minimum de compétences opérationnelles et techniques pour pouvoir agir.

L'intégration du renseignement militaire dans le continuum défense et sécurité de la nation est-il souhaitable ?

*Ce continuum existe déjà. Aujourd'hui, dans le domaine du terrorisme, les individus dangereux sont passés par les terres de djihad. Qui, au premier chef, est présent sur ces théâtres si ce ne sont les forces armées. Lors du colloque sur le GEOINT à Paris le 11 septembre 2015, l'actuel DRM, le général Gomart, a précisé que nous n'ignorions rien des flux de migrants depuis la rive sud de la Méditerranée. Il voulait dire que nos moyens (pas uniquement l'imagerie) nous permettent d'avoir une bonne idée des organisations maffieuses et peut-être terroristes (les deux sont liées) qui se cachent derrière ce drame humain. La difficulté est en fait dans la coordination des efforts et des échanges d'informations, qui dépendent en grande partie de capacités techniques, lesquelles se mettent en place mais pas assez vite. La coordination est du ressort du Coordonnateur comme je l'ai déjà dit : il n'a pas assez de pouvoirs, pas assez de moyens, il n'est pas assez proche du P.R.** et il faudrait que ce soit un homme du métier, un ancien directeur de service, par exemple. Pour s'imposer dans ce milieu, il faut en connaître les rouages et les codes. Cela n'a jamais été le cas jusqu'ici et le précédent a jeté l'éponge: c'est révélateur.*

Comment utiliser le renseignement militaire sur le territoire national (Sentinelle) ? Est-ce souhaitable ?

D'abord, il faut poser comme postulat que le renseignement militaire n'opère pas sur

le territoire national, hormis pour les missions régaliennes (interministérielles). L'intervention, sous une forme ou une autre, des armées dans la sécurité intérieure n'est pas bien vue de l'Etat-major et on reste toujours très prudent sur le sujet. En mars 2015, Jean-Marie Faugère (ancien inspecteur général des armées - terre) a montré que l'opération «Sentinelle» était anticonstitutionnelle, puisque déployée en dehors de tout état d'exception (état de siège, état d'urgence, défense opérationnelle du territoire), les armées ayant été réquisitionnées par l'autorité publique sans pour autant être considérées comme des forces dites de 3ème catégorie, destinées au maintien de l'ordre. C'est pour cette raison que le dispositif «Sentinelle» gêne beaucoup les militaires. Pour répondre à votre question, je ne pense pas que ce soit souhaitable.

En 2013, la Commission nationale d'examen des programmes de R&D de la communauté du Renseignement américain a produit un rapport émettant un certain nombre de recommandations. Qu'en tirez-vous comme analyse ?

*Les Américains y font le constat amer qu'ils font maintenant partie du «vieux monde» et que certains risques, non directement perceptibles, émanent de puissances dites émergentes et plus généralement de celles qui veulent se faire rapidement une place dans le panorama stratégique. Ils contemplent avec amertume leurs capacités passées en matière de recherche et d'innovation (programme Corona ***) et se disent qu'ils sont en voie d'être dépassés. Ceci nous interpelle directement: que faisons-nous en ce sens en France? Réponse: pas assez et surtout de façon dispersée. De fait, la DGSE a pris «le lead» et les autres doivent suivre. Je suis favorable à la synergie, au sein d'une même instance, des différents services techniques de la communauté nationale du renseignement, au travers d'un statut lui donnant une certaine autonomie de gouvernance stratégique et budgétaire en matière de R&D, présidée par le Coordonnateur. Une «agence» si vous voulez, dans le genre de ce qu'on a pu faire (toutes proportions gardées) dans d'autres domaines de pointe avec l'ONERA et avec l'ANSSI. Les services ont des besoins communs, des visions très proches et surtout des défis et menaces communs qui ne sont plus compartimentés. Il y a, là aussi, un «continuum» et il faut y faire face ensemble !*

La France a-t-elle fait ce type d'analyse ?

La France ne pouvait faire une telle analyse, parce qu'on ne joue pas «dans la même cour» et que nous n'avions pas la même stratégie. En avions-nous même une? Nos services étaient très mal orientés par l'autorité politique. Les différents P.R. qui se sont succédés depuis 1958 n'avaient que peu d'appétence pour le Renseignement, quand ce n'était pas de la méfiance voire du dédain. En conséquence, dans la compétition mondiale post-guerre froide, on n'a pas orienté nos services au bénéfice de la nouvelle guerre, la guerre économique. Ou trop peu!

Le renseignement français a-t-il fait sa révolution numérique? Avec des fournisseurs de confiance?

Oui, le renseignement national a «fait sa révolution numérique» depuis plusieurs années déjà. Mais de façon non homogène entre les services: en particulier pour des raisons budgétaires, moins pour des raisons culturelles. Le renseignement n'a commencé à véritablement trouver de la considération qu'avec le Livre Blanc de 2008. Non pas par prise de conscience soudaine, mais parce que tout à coup le politique s'est mis de la partie. Quant à l'ex-DST, devenue DCRI, elle n'avait même pas de véritable direction technique. Les services sont devenus étroitement dépendants des moyens numérisés mais les produits informatiques du marché sont intrinsèquement vulnérables, sans correctif réaliste possible. On comprendra aisément que les services ne peuvent se permettre d'être vulnérables. Contrairement à ce qui est préconisé en la matière, pour favoriser l'innovation, le mode de relation contractuelle doit intégrer une grande souplesse dans l'appréciation de la qualité des travaux réalisés par le fournisseur et ne pas voir le donneur d'ordres imposer des obligations de résultats qui brideraient fortement les prises de risques. Or c'est bien ce qu'imposent les services, que ce soit dans l'étude amont, puis dans le développement et enfin dans la production. Un peu la quadrature du cercle. En conséquence, on comprendra que dans ce domaine la «confiance» n'est pas immédiate entre un service et un fournisseur. D'autant que celui-ci n'aura jamais de vision globale du sujet (c'est intentionnel) et il ne sera jamais propriétaire de quoi que ce soit. Donc fournisseurs de confiance, oui, mais choisis par les services (et non l'administration), sur des créneaux très cadrés, triés sur le volet et, s'ils sont performants, fidélisés.

* GCA (2°s) : Général de Corps Aérien en 2e section
**P.R. Président de la République
***Corona : https://fr.wikipedia.org/wiki/Corona_%28satellite%29

• Que nous apprend l'interview du général Masson parue dans SDBR ?

- Le rôle, les prérogatives et les moyens du Coordonnateur National du Renseignement doivent être revus ; son rôle doit être renforcé et son entourage étoffé en termes de compétences opérationnelles et techniques.
- Il faut aller vers plus de mutualisation du domaine du renseignement technique.
- Il faut passer d'une gouvernance centrée sur les ministères à une gouvernance centrée sur les services de renseignement.
- Dans le domaine du terrorisme, les individus dangereux sont passés par les terres de djihad... Nous n'ignorons rien des flux de migrants depuis la rive sud de la Méditerranée : nos moyens nous permettent d'avoir une bonne idée des organisations maffieuses et peut-être terroristes (les deux sont liées) qui se cachent derrière ce drame humain...

- Contrairement aux Américains, qui ont fait leur auto-analyse, la France ne se pose pas réellement la question de la préparation de l'avenir et de l'intérêt qu'elle doit porter aux développements de la R&D chez les adversaires potentiels. Encore une fois, les Français courent après la guerre d'hier et la mise à niveau de leurs compétences sur les problématiques... d'hier !
- Il n'y a pas d'amis ou d'ennemis dans le domaine du renseignement économique. Il faut bien occuper les espions américains en période de détente...
- Le renseignement national a «fait sa révolution numérique» depuis plusieurs années déjà, mais de façon non homogène entre les services. La DGSE est leader, la DRM suit... La DCRI n'avait même pas de direction technique en 2008... Rattrapage culturel et mise à niveau sont nécessaires !

Biographie – Le Général de Corps Aérien Michel Masson (2e section) est issu de l'Ecole de l'air (Promotion 1971). Après une carrière opérationnelle dans le transport aérien militaire tactique et le commandement de deux unités opérationnelles, il se voit confier la responsabilité de la base aérienne de Tahiti-Faa'a en Polynésie française (BA 190) et des éléments air du Centre d'Expérimentations Nucléaires du Pacifique (1994-1996). A l'issue de l'Ecole Supérieure de Guerre Interarmées (ESGI), il rejoint le cabinet du ministre de la défense (1991-94). Stagiaire en 1996 au Centre des Hautes Etudes Militaires (CHEM) et à l'Institut des Hautes Etudes de Défense Nationale (IHEDN - 49e session), il se voit confier en 1997 le cabinet du Chef d'état-major de l'armée de l'air. Nommé général de brigade aérienne en 1999, il sert successivement au Secrétariat général de la Défense Nationale (Affaires Internationales et Stratégiques/ Dir. adj. 1999-2002), à l'Etat-major des armées (Sous-chef d'état-major chargé des relations internationales 2002-05), avant d'achever sa carrière d'active en tant que Directeur du Renseignement Militaire (2005-08) avec le grade de Général de Corps Aérien. Depuis, Michel Masson apporte son expérience au profit des affaires de défense et de sécurité dans différentes enceintes, tant civiles que militaires.

* * *

De façon encore plus précise, avec l'exemple de la DRM, beaucoup de choses ont été faites depuis le Livre Blanc sur la Défense et la Sécurité Nationale de 2008. Mais beaucoup reste à faire. Le Général Christophe Gomart, Directeur du Renseignement Militaire depuis le 1er août 2013, nous expliquait en novembre 2013 le fonctionnement de la DRM et ses axes de travail.

SDBR : La DRM serait un outil d'anticipation stratégique, d'éclairage prospectif de la Défense et d'appui aux opérations primordiales (articulation avec le COS). Pouvez-vous clarifier cette définition ?

Christophe Gomart : La DRM a pour mission de satisfaire, de façon autonome, les be-

*soins du ministre de la défense et du CEMA** en renseignement d'intérêt militaire, ainsi que les besoins des forces en opérations extérieures. Bien souvent, on présente la DRM d'une part comme un outil de veille stratégique et d'autre part comme un outil d'appui aux opérations. Dans ma conception, ces tâches ne s'opposent pas. Elles se complètent et s'harmonisent parfaitement dans le temps, car il y a une véritable continuité du traitement de l'information, depuis la veille stratégique jusqu'à l'appui aux opérations. La veille stratégique va éclairer l'appui aux opérations de demain et les opérations de demain éclaireront la veille stratégique d'après-demain, etc. Le Renseignement est un tout, c'est une chaîne dans le traitement de l'information. Que l'on s'intéresse aujourd'hui à un pays a priori calme, mais où peut naître une crise demain, est intéressant comme est intéressant le renseignement recueilli, par l'appui aux opérations dans un pays en crise, pour éclairer la situation d'après-crise : connaissance et anticipation. Entre veille stratégique, anticipation et appui aux opérations, il y a pour moi une continuité assez naturelle.*

Qu'appelez-vous « éclairage prospectif de la Défense » ?

La délégation aux affaires stratégiques (DAS) du ministère de la Défense participe à l'élaboration de la politique de défense, sur la base de renseignements fournis par les services qui œuvrent à cet éclairage, dont la DRM. Le chef d'état-major des armées préside, pour sa part, le groupe d'anticipation stratégique (GAS) qui, intégrant les orientations données par le CNR (coordonnateur national du renseignement), arrête une liste de zones et des thèmes à suivre, liste qui va ensuite me servir pour déterminer les moyens de la DRM à affecter, en fonction de ces priorités. Toutefois, dans le passé, la DRM a du faire des choix de priorité et arrêter de suivre certains pays, par manque de moyens et d'effectifs suffisants.

Il y a donc des pays qu'on ne suit pas ?

Oui car nos moyens sont limités. Des choix doivent être faits, c'est pourquoi nous concentrons nos moyens et nos efforts sur les priorités stratégiques fixées par le CEMA, pour répondre aux besoins en renseignement de nos décideurs et appuyer nos forces en opération.

Cela sous-entend-il que les signaux faibles sont difficiles à détecter dans certains pays ?

Les signaux faibles sont relativement bien détectables dans le monde surmédiatisé dans lequel nous vivons. Ils permettront, si nécessaire, de réorienter le classement des priorités effectué par le GAS régulièrement. Il faut d'ailleurs comprendre, dans ce cadre, tout l'intérêt de la géographie dans notre fonction. L'interception de communication et l'image ne sont pas suffisantes dans certains cas, et l'infiltration humaine n'est pas toujours possible. Il nous reste alors la géographie ! Dans le cas du Mali, il est fré-

quent de croire que le désert est uniquement plat avec des immensités de sable, or le désert ce n'est pas plat et ce n'est pas que du sable, loin de là : il y a des puits, des oasis, des passes, des pistes, qui sont autant d'indices géographiques nous permettant de trouver l'ennemi. Le massif des Ifoghas, au nord du Mali, est loin d'être plat et sablonneux : des gens y vivent, y cultivent des parcelles et savent profiter de la protection naturelle du relief pour y constituer des caches, des dépôts et des refuges !

Jugez-vous l'organisation actuelle, de la fonction « renseignement d'intérêt militaire » et de la DRM, adaptée aux défis qui se posent et qui se poseront ?

La DRM a été créée il y a 20 ans par Pierre Joxe pour garantir une autonomie d'appréciation de situation, de niveau stratégique, qui n'existait pas auparavant. Cette faculté a depuis lors été utilisée dans les conflits post Guerre froide (ex-Yougoslavie, Kosovo, RCI, RCA, Afghanistan, Libye, Mali), particulièrement grâce aux moyens de recueil nationaux, entre autres dans les domaines des images et des interceptions électromagnétiques. Elle constitue pour notre pays un indéniable facteur de puissance sur la scène internationale. Dans le futur, nous serons confrontés à des défis importants liés à la problématique des volumes d'information à traiter et, dans ce domaine, nous avons encore des progrès à faire. Mes défis techniques sont liés à l'accroissement du volume des images satellitaires, des interceptions radar et des communications militaires qu'il faut traiter, notamment dans le cadre des opérations extérieures. Ce qui nécessite de disposer de personnels qualifiés en nombre suffisant, c'est-à-dire des linguistes adaptés, capables de traduire 7/7 et H24, ou des interprétateurs photos, en nombre suffisant pour être opérationnels en H24 et pour traiter un flux d'image considérable. Cela signifie aussi qu'il faut développer des systèmes automatiques capables d'aller chercher la bonne information, dans une masse gigantesque, pour la soumettre aux analystes.

Avez-vous les ressources humaines nécessaires au sein de la DRM ?

Je dispose d'une ressource de grande qualité, mais je souhaite désormais porter mes efforts sur une sélection plus affinée des différents profils dont j'ai besoin, en pesant plus efficacement sur les processus de désignation. Pour le personnel civil, nous avons besoin qu'une certaine mobilité réciproque entre services de renseignement soit possible. Enfin, nous avons besoin de linguistes et d'interprétateurs images qui sont des spécialistes longs à former.

*ROHUM : recherche d'origine humaine
**CEMA : chef d'état-major des armées

• Que doit-on retenir de l'interview du général Christophe Gomart ?

- Le Renseignement est un tout, c'est une chaîne dans le traitement de l'information.
- La France concentre ses moyens et ses efforts de renseignement sur les priorités

stratégiques fixées par le CEMA, pour répondre aux besoins en renseignement des décideurs (politiques) et appuyer les forces en opération. Il y a donc des pays non suivis par manque de moyens.
- La géographie militaire est vraiment partie intégrante des moyens d'analyse et d'anticipation de la DRM.
- Le défi tient à la problématique des volumes d'information à traiter (images satellitaires, interceptions radar, communications militaires) et, dans ce domaine, il y a beaucoup de progrès à faire. Ce n'est pas tout d'intercepter, il faut ensuite interpréter et analyser, donc il faut des moyens d'automatisation et des moyens humains.

Biographie – Né en 1960, Christophe Gomart est passé par l'Ecole spéciale militaire de Saint-Cyr (1981). Il a été notamment chef de corps du 13e Régiment de Dragons Parachutistes (RDP) en 2003, puis conseiller militaire du Coordonnateur National du Renseignement Bernard Bajolet (qui depuis a pris les rênes de la DGSE jusqu'en 2017...). Il prend en 2011 le commandement des forces spéciales et du COS (Commandement des Opérations Spéciales), avant d'être nommé à la tête de la DRM en juin 2013.

3. Cyber : la menace au quotidien

Comme nous le disons en introduction de ce cahier, en citant Tewfik Hamel, il faut avoir conscience de l'importance de l'apport des nouvelles technologies (internet, cyber, réseaux sociaux, etc.) aux guérillas armées et aux entités criminelles de toutes sortes pour leur permettre de proliférer. Pour aider le lecteur à avoir une vision claire d'une actualité souvent confuse en la matière, nous avons regroupé les interviews significatives parues dans SECURITY DEFENSE Business Review (SDBR) depuis 3 ans en cinq thèmes :
- Le monde Cyber
- Différentes formes de menaces dans le monde Cyber
- La perception des responsables opérationnels confrontés aux risques cyber
- La cybersécurité permet-elle l'éclosion d'un nouvel écosystème ?
- Le rôle de l'Etat français dans la filière numérique

• Le monde Cyber

Dans une interview parue dans SDBR N°86, le 25/06/2013, Kavé Salamatian, professeur d'Informatique à l'Université de Savoie et consultant, nous dressait un panorama mondial intéressant des stratégies de certains pays vis à vis de l'internet et des carences qui pouvaient être relevées dans la politique européenne en la matière. Cette interview réalisée il y a plus de 3 ans est toujours d'actualité...

SDBR : Pourquoi avez-vous un intérêt particulier pour l'Asie ?

Kavé Salamatian : En effet, je porte beaucoup d'intérêt à l'Asie car cette région du

monde est comme une boule de cristal dans laquelle on peut voir notre Futur : exemple, aujourd'hui on commence à parler en France de déploiement massif de fibres optiques, les Japonais et les Coréens en sont équipés depuis des années. S'ils le voulaient, les Chinois pourraient se doter de leur propre infrastructure pour s'occuper de l'Internet mondial mais, actuellement, ils n'en ont pas l'intention, trouvant plus d'intérêt à rester dans un système ouvert. A la différence des pays européens, qui n'ont que récemment réalisé la portée stratégique de l'Internet, les Chinois en ont conscience depuis 15 ans ! Un certain nombre de pays ont construit leur stratégie autour de l'Internet : exemple la Corée du Sud, qui a construit sa stratégie autour de la notion d'ingénierie culturelle et d'Internet. Dans les pays émergents, il faut parler de la Russie. Nous reprenons conscience d'un fait qu'Internet nous avait fait oublier, à savoir que la géographie est importante...La Russie, aujourd'hui, est le moyen le plus fiable pour interconnecter l'Est et l'Ouest, en passant par un satellite. Les Russes ont une émergence très forte sur l'infrastructure de l'Internet avec, en contrepartie, la surveillance et l'espionnage.

Et l'Europe ?

L'Europe d'aujourd'hui a aussi un problème avec Internet et les racines de ce problème sont à rechercher dans l'opposition, entre approche fédéraliste et visions nationalistes, qui est aussi observée dans d'autres domaines. Le numérique en Europe ne pourrait se mettre à niveau que par un plan de relance européen, mais nous continuons à développer des activités pays par pays...

Ne jetez-vous pas là un pavé contre le « numérique à la française » ?

Le numérique à la française n'aura pas grande perspective s'il ne se conçoit pas dans le contexte européen. En France, ainsi que dans d'autres pays européens, la filière informatique ne provoque pas l'enthousiasme des jeunes, et nous ne sommes pas pour autant un acteur moteur sur le sujet. Par exemple, dans mon université, le nombre d'étudiants formés en informatique (pour qui le salaire de sortie d'école est supérieur de 10% aux autres diplômés avec un temps d'attente négatif !) est 6 fois moindre aujourd'hui que le nombre de demandes d'entrée en filière d'ingénieurs du bâtiment ! Alors qu'en Chine, les ingénieurs rêvent de faire des études en informatique et en sont fiers quand ils réussissent ! Le problème en France vient du fait que l'Informatique a mauvaise presse, à cause des SSII qui ont entaché son image, et mauvaise réputation sociale (incompréhension de la population sur les métiers couverts par le terme générique Informatique, etc.). Aujourd'hui aussi, l'innovation technologique n'est observée qu'au travers des prismes Google et Facebook ! Nous avons une vision très utilitaire de l'Informatique et c'est particulièrement vrai dans la culture des entreprises, où ce n'est pas considéré comme une activité noble. Les organisations ne traitent pas l'Informatique

comme leur cœur de métier, c'est incroyable ! Les Allemands, qui se sont rendu compte de ce phénomène, ont recruté des milliers d'ingénieurs indiens pour pallier à leur problème.

Quel est votre sentiment sur l'agitation actuelle en matière de Cyberdéfense ?

Le Cyberespace est un domaine émergent qui mérite d'être cartographié, avant de réagir de façon émotionnelle et sur l'instant. On parle aussi de cyber-guerre, or la guerre est un concept brutal qui tue. A l'heure où nous parlons, nous n'avons aucun phénomène informatique clair et net qui aurait tué des gens. Si on pense aux Scada, c'est bien parce qu'on a confié un outil industriel à un robot défaillant que l'on pourrait observer un accident industriel. La problématique d'une éventuelle cyber-guerre est, de mon avis, plutôt un phénomène de guerre modérée mais de longue durée, donc de la cyber-guérilla, qui ne se résout pas avec la force brute mais avec la réflexion politique.

• Que doit-on retenir de l'interview du professeur Salamatian ?

- L'Asie est comme une boule de cristal dans laquelle on peut voir notre Futur !
- A la différence des pays européens, qui ne se sont rendu compte que récemment de la portée stratégique de l'Internet, les Chinois en ont conscience depuis 18 ans !
- On pouvait souligner dès 2013, chez les Russes, une émergence très forte sur l'infrastructure de l'Internet avec, en contrepartie, la surveillance et l'espionnage...
- Le numérique à la française n'aura pas grande perspective s'il ne se conçoit pas dans le contexte européen.
- En France, la filière informatique ne provoque pas l'enthousiasme des jeunes car l'informatique n'est toujours pas considérée comme une activité noble.
- La problématique d'une éventuelle cyberguerre est plutôt un phénomène de guerre modérée mais de longue durée, donc de la cyber-guérilla, qui ne se résout pas avec la force brute mais avec la réflexion politique.

Biographie de Kavé Salamatian – De formation ingénieur électronicien + MBA, il débute sa carrière comme analyste dans une salle de marchés avant de revenir vers l'Université pour faire un Master de Télécoms suivi d'un DEA d'Informatique théorique et d'une thèse. Après sa thèse, il est recruté comme maitre de conférences à Paris VI. Il est actuellement professeur des universités à l'université de Savoie (Annecy) et chercheur. Parallèlement, il exerce des activités de consulting hors de France.

* * *

Philippe Courtot, Président de Qualys*, est considéré comme un visionnaire des systèmes informatisés. C'est pourquoi SDBR l'a interviewé plusieurs fois. Dans cette interview parue dans "SECURITY DEFENSE Business Review" n°112 daté du 23/09/2014, il livrait une vision claire de

ce qui peut être constaté aujourd'hui. Morceaux choisis :

SDBR : En mai 2013, vous me disiez que les constructeurs devaient se tourner vers plus d'automatisation pour ne pas être submergés par la vague de l'Internet. Pensez-vous toujours la même chose ?

Philippe Courtot : Non seulement je pense la même chose, mais malheureusement nous voyons apparaître de plus en plus de fractures. Comme au début de l'ère industrielle, les nouvelles technologies allaient changer profondément la condition humaine et il y eut beaucoup de fractures importantes. Donc nous voyons aujourd'hui apparaître d'autres fractures mais, dans le même temps, nous assistons à des découvertes scientifiques et techniques époustouflantes, et ce phénomène dépasse largement les technologies de l'information et l'ordinateur: par exemple, l'avenir est proche où nous saurons créer des organismes presque totalement artificiels (génome) ou bien, une découverte passée inaperçue en matière d'énergie nucléaire concerne la fusion catatonique, qui crée plus d'énergie qu'elle n'en consomme.

Nous assistons à des concentrations dans le domaine de la sécurité informatique (Intel / McAfee / Stonesoft, Cisco / Sourcefire, etc.). Quel est votre opinion sur ces évolutions de contours ?

*Je dirais que nous assistons à la consolidation du passé, car ces technologies sont en train de mourir ! Comme nous avions assisté à la consolidation des mainframes avant leur disparition... De cette consolidation, n'était resté qu'IBM qui a changé de métier fondamentalement en passant aux services et au middleware**. Vous assistez comme moi au démarrage de nombreuses start-up dans la sécurité, qui commencent toutes directement avec des architectures Cloud, car le Cloud permet d'avoir une puissance de calcul presqu'infinie, d'avoir des capacités de stockage énormes, d'utiliser Internet comme moyen de communication en ayant, au niveau du Cloud, des bouts de software ou des applications que l'on peut gérer facilement. Nous ne sommes déjà plus à l'époque des « end point » gérés comme avant (le PC, le laptop), ce qui revient à nous plonger dans l'internet des objets, que ce soit des objets physiques ou des bouts de software gérés à travers le Cloud.*

La cybersécurité est-elle aujourd'hui au cœur de la gouvernance de l'organisation ?

Oui et non. Les Boards sont maintenant très au courant des risques qu'ils prendraient si l'entreprise perdaient les données des clients. Le problème a été compris mais il n'y a toujours pas de bonnes solutions, car c'est un problème très complexe et tout cela reste assez nébuleux pour déterminer ce qu'il faut faire et comment le faire. Actuellement les entreprises sont, comme on dit, assises entre deux chaises, à savoir entre les anciennes infrastructures informatiques (post mainframe) et les systèmes Clouds qui sont bien plus faciles à sécuriser. Avec un

Cloud, vous vous retrouvez dans un domaine mainframe, dans lequel les données sont dans un seul endroit très sécurisé et dont on peut contrôler les accès.

Et les réseaux alors ?

*Concernant les réseaux, il s'agit d'une question de protocole. Aujourd'hui les protocoles sont durcis et on parvient à fabriquer des protocoles très sécurisés. L'exemple de la faille de sécurité « Heartbleed » découverte en avril 2014***, qui concernait le protocole open SSL, est un peu une exception car il y avait un faute de code à l'écriture. Lorsque ce genre d'incident arrive, on identifie la faille et on la bouche. Mais il reste du chemin à parcourir pour passer d'une logique d'architecture ancienne, qu'il faut sécuriser, à une autre pour laquelle on doit d'abord penser en termes de sécurité. Cela demande une qualité technique et de compréhension chez les individus en responsabilité, or il n'y a pas suffisamment de personnes spécialisées dans les entreprises et les organisations pour gérer ces problèmes.*

*Qualys : 500 collaborateurs présents dans 106 pays. www.qualys.com

**middleware : en architecture informatique, un middleware est un logiciel tiers qui crée un réseau d'échange d'informations entre différentes applications informatiques (utilisé pour le réseau).

***Heartbleed : faille dans le protocole SSL permettant à un pirate d'obtenir les clés privées qui sont utilisées par le serveur pour crypter les données, et donc se connecter à un compte en disposant du login et du mot de passe.

• Quels enseignements nous donnait Philippe Courtot dès 2014 ?

- L'évolution technologique fait naître beaucoup de fractures dans la condition humaine. En même temps, se déroule sous nos yeux la fin d'une période, avec des technologies en fin de vie et des entreprises qui n'ont pas toujours su anticiper : c'est la consolidation du Passé !
- En 2014, Philippe Courtot nous annonçait la formidable croissance du Cloud... Aujourd'hui cela parait banal, mais il y a 2 ans nous étions encore loin de la banalité...
- La sécurité des systèmes informatiques n'ayant pas été prévue à l'origine, « les bandits de grands chemins de l'âge informatique s'en donnent aujourd'hui à cœur joie »...
- Les entreprises sont assises entre deux chaises, donc difficiles à sécuriser.

Biographie – Diplômé en Physique à Paris, Philippe Courtot s'oriente finalement vers l'informatique au début des années 70. Philippe Courtot est un Français qui a quitté la France tôt, lorsqu'il a compris qu'il était très difficile, voire impossible, d'être recruté chez les grands industriels lorsqu'on n'avait pas le diplôme qui convenait. Il démarre donc en 1972 en tant que Responsable France d'une petite entreprise américaine (Modcomp), spécialisée dans les micro-ordinateurs embarqués. Six ans plus tard, il en devient le Vice-président. Présent depuis

plus de 20 ans dans la Silicon Valley, six fois CEO, Philippe Courtot est reconnu pour ses capacités à transformer les entreprises innovantes en leaders de marché. CEO de Verity, il est à l'origine du développement de cette société devenue incontournable sur le marché de la recherche d'information et en a orchestré l'introduction en bourse en novembre 1995. Par la suite, il fait de Signio un acteur significatif du e-commerce avant de vendre la société à VeriSign. CCMail est devenu grâce à lui un acteur de poids avec 40 % du marché des plates-formes e-mail, revendue à Lotus en 1991. Il est le CEO de Qualys depuis 2000.

4. Le monde cyber : menaces, parades, le rôle de l'État

Xavier Raufer, dans son excellent ouvrage « Cyber-criminologie » paru chez CNRS Editions en janvier 2015, a décrit largement le type d'attaques ou de piratages que les entreprises et les organisations peuvent subir au travers de leurs systèmes informatiques connectés au Web. Il nous a paru intéressant d'évoquer certaines failles de sécurité, pour en montrer les risques, et d'écouter les experts évoquer parfois les limites de la protection contre le risque cyber. Nous avons donc reproduit ci-après des extraits de certaines interviews parues dans SECURITY DEFENSE Business Review.

Aucune entreprise ou organisation ne peut aujourd'hui ignorer qu'elle est forcément exposée à un risque d'origine cyber. Pourtant, comme l'a souligné Franck Greverie dans une interview parue le 24/03/2015 dans SECURITY DEFENSE Business Review n°124, il y a encore beaucoup de chemin à parcourir pour que les dirigeants mettent le risque cyber au rang des risques stratégiques et surtout mettent en place des mesures correctrices adaptées. Extraits de l'interview de Franck Greverie :

SDBR : Considérez-vous que toutes les entreprises soient aujourd'hui sensibles au discours sécuritaire lorsqu'elles envisagent une transformation digitale ?

Franck Greverie : Aujourd'hui, nous constatons que 60% des appels d'offres qui sortent ont des exigences de sécurité détaillées. C'est un réel progrès, puisqu'il y a dix ans le taux d'appels d'offres avec des exigences de sécurité détaillées n'était que de 5%! J'insiste sur le mot «détaillées», car dans tous les appels d'offres est inscrit «qu'il faut que le système soit sécurisé», or ce n'est pas suffisant pour envisager la mise en œuvre une solution de cybersécurité efficace qui corresponde aux besoins du client.

Sur fond d'attaques Carbanak/ Anunak mises à jour par Karspersky, qu'observez-vous sur le risque cyber dans le monde bancaire ?

Ce qu'on peut dire, c'est que depuis deux ans nous constatons une recrudescence des attaques sur les POS (points of sales), distri-

buteurs de billets ou terminaux de paiements, qui sont en fait des objets connectés. Les pirates ont compris qu'il était souvent plus facile d'entrer par les POS que par les data centre. Pendant des années, les grandes banques se sont focalisées sur la protection de leur système IT. Aujourd'hui, elles ont pris conscience que cette sécurité statique, bien que nécessaire, n'est plus suffisante. Elles mettent donc en place des SOCs de troisième génération pour détecter et réagir face aux cyber-attaques. En outre, elles mettent souvent en place une surveillance accrue des comptes à privilèges et des solutions de détection des comportements anormaux.

* http://www.fr.capgemini.com/a-propos-de-capgemini

Biographie – Franck Greverie a commencé sa carrière dans différents postes opérationnels chez Alcatel et au sein de Sema Group (aujourd'hui Atos Origin). Il rejoint Thales en 2004 où il est responsable de la Stratégie, du Développement et du Marketing de l'activité sécurité puis prend la direction de Thales Shield, qui a pour expertise la sécurisation des aéroports, des transports, du pétrole et du gaz, et des villes. En 2008, il est nommé Directeur général des activités de sécurité des technologies de l'information et de cybersécurité de Thales. En 2012, il rejoint Bull en tant que Vice-président exécutif du département Sécurité, qui comprend les activités de cybersécurité du groupe. Il devient en 2014, Corporate Vice President des activités Cybersécurité pour l'ensemble du groupe Capgemini. Il est aujourd'hui Capgemini Cloud & Cybersecurity Leader.

* * *

En décembre 2015, SDBR a interrogé Laurent Heslault, directeur des Stratégies de Sécurité chez Symantec* South EMEA, sur les risques et menaces visant les systèmes d'information, ce qui a donné l'interview suivante parue dans le numéro 140. Extraits :

SDBR : Pensez-vous qu'aujourd'hui la cybersécurité intéresse beaucoup les responsables d'entreprise ?

Laurent Heslault : On peut encore constater que nombre de dirigeants d'entreprises, grandes ou petites, considèrent que la cybersécurité est «un truc pour les geeks»... Par contre, demandez à un grand patron s'il a conscience que son activité est totalement, ou presque, dépendante du cyber pour voir ce qu'il va vous dire? Bien évidemment, vous dira-t-il peut-être, toutes les entreprises sont aujourd'hui cyberdépendantes! Ensuite, demandez-lui si son entreprise est cyber-résiliente? Vous obtiendrez alors un grand silence... Nous savons qu'un jour ou l'autre l'entreprise finira par subir une attaque: ce n'est plus «SI» l'entreprise est attaquée, mais «QUAND» le sera t'elle (si ce n'est pas déjà le cas). Est-on prêt à la détecter? Est-on prêt à y répondre? La résilience est la capacité à revenir à un état normal après un stress ou une attaque. De la même façon que sont évoquées, dans les

forums internationaux, la résilience environnementale, la résilience sociétale ou la résilience économique, il convient de parler de cyber-résilience. Il faut que les dirigeants en prennent réellement conscience.

Quel est votre avis sur les « smart cities », concept dont on parle beaucoup ces temps-ci ?

Il est inquiétant de constater que personne ou presque ne parle de la sécurité lorsqu'on parle de «smart city». Il est envisagé de connecter de très nombreuses données et de systèmes urbains, qui doivent être gérés et sécurisés, ce qui dépasse bien souvent les compétences actuelles des maires. La smart city est un aspect de l'internet des objets, or l'internet des objets met en jeu de l'hyper-connectivité et de l'hyper-compétitivité (individuelle, entrepreneuriale ou gouvernementale): plus nous sommes connectés, plus les environnements sont complexes, plus la compétitivité est globale, plus nous sommes vulnérables. Donc, résumons-le par la formule: hyperconnectivité + hypercompétitivité = hypervulnérabilité. Qu'est-il alors prévu en termes de résilience en cas de problème?

Qu'est-ce qui a fait que Stuxnet ait été découvert finalement ?

*Stuxnet remontait des informations vers un serveur de contrôle et commande, or ses développeurs ont mal contrôlé sa prolifération et Symantec a pu identifier un phénomène inhabituel: remontées d'informations vers des serveurs en Allemagne et en Finlande, notamment vers un serveur de football, ce qui a attiré l'attention. Nous avons identifié 110.000 exemplaires de Stuxnet dont 60.000 en Iran, ce qui signifie que le virus s'était trop répandu. En comparaison, Dragonfly** n'a touché que cinq postes. Ce qu'il faut retenir, c'est qu'il y a eu un avant et un après Stuxnet en matière de zero day et d'attaques ciblées.*

* http://www.symantec.com/fr/fr/atp-network

**Un groupe de hackers, baptisé Dragonfly, est parvenu en 2014 à corrompre certains systèmes de contrôle des opérateurs d'énergie, notamment en France, pour saboter la distribution d'énergie.

• Que retenir de cet entretien avec Laurent Heslault ?

- Nombre de dirigeants d'entreprises n'ont pas encore pris conscience de la nécessité de mettre en place des processus de cyber-résilience. Ils sont conscients du risque incendie et des sauvegardes qu'il faut mettre en place, mais presque jamais du risque cyber.
- Le cyber-risque figure parmi les cinq risques majeurs qui menacent une entreprise ou une administration !
- En 2015, il commençait à être beaucoup question de « smart cities » sans jamais évoquer les questions de sécurité inhérentes.

Biographie – A la suite de ses études supérieures à l'ESTACA (Ecole d'ingénierie aé-

ronautique), il débute sa carrière chez SEMA METRA. Après un passage chez Random puis Computacenter, il rejoint Lotus Software en 1994, puis intègre IBM Software Group en 1999 où il exercera différents postes de management technique et de marketing. Laurent Heslault a rejoint Symantec en 2004 en tant que Directeur des équipes avant-vente. Il est aujourd'hui Directeur de Stratégies de sécurité, avec pour mission de présenter et représenter la stratégie et les solutions Symantec auprès de l'ensemble des clients et partenaires de l'entreprise. Laurent Heslault est détenteur de différentes certifications professionnelles telles que le CISSP (Certified Information Systems Security Professionnal) ou le CCSK (Certificate of Cloud Security Knowledge).

• La perception des responsables opérationnels confrontés aux risques cyber

Il nous a paru important et nécessaire de donner la parole aux opérationnels en charge de la maintenance et de la sécurité des systèmes d'information des entreprises. C'est ce que SDBR a fait en interviewant Alain Bouillé, Président du CESIN, dans le numéro 144 paru le 16 février 2016. Il nous livre entre autres, ci-après, une image très fidèle de la réalité du numérique en France.

SDBR : Le CESIN a fait réaliser par l'institut de sondage OpinionWay une grande enquête sur la perception de la cybersécurité et de ses enjeux au sein des grandes entreprises françaises. Pourquoi cette enquête ?

Alain Bouillé : L'idée de ce baromètre est d'en faire un outil récurrent annuel sur l'état de la cybersécurité et sa perception par les grandes entreprises françaises. Paradoxalement, il y a abondance de rapports et de publications autour de la cybercriminalité, mais une grande majorité d'entre eux sont issus d'études faites par des éditeurs, ce qui n'est pas sans arrière-pensées de leur part car ils ont des produits à vendre. D'autres études sont régulièrement produites par de grands cabinets internationaux de conseils, mais leurs conclusions ne s'appliquent pas forcément en Europe et en France en particulier, car elles s'appuient souvent sur des faits américains qui déforment l'image de notre réalité locale.

Quelle est la place de la cybersécurité dans les grandes entreprises aujourd'hui d'après votre étude ?

Beaucoup parlent aujourd'hui de la digitalisation des entreprises, souvent légèrement, et nous ne savons plus très bien à quelle réalité cela fait référence. Cette digitalisation n'est en fait pas une mode mais bien une réalité qui se traduit par plusieurs phénomènes. La digitalisation vue de l'intérieur : les salariés vont être davantage connectés, on parle « d'extrême mobilité » avec l'utilisation de « devices » multiples (BYOD), l'utilisation de services de collaboration de plus en plus débridés etc., donc un nouveau mode de travail en interne. La digitalisation vue de l'extérieur : pour les clients avec davantage d'outils qui leurs sont proposés, etc. L'étude a donc montré

que 93% des RSSI considéraient que le digital était devenu un enjeu stratégique pour leur entreprise ! Donc c'est une réalité qui dépasse largement la nomination ici ou là d'un CDO (chief digital officer). Par contre, pour nous en charge de la sécurité, la digitalisation se traduit par des portes et des fenêtres qui s'ouvrent à tous vents sur des systèmes d'information qui vont être davantage éparpillés : mobilité, BYOD, Cloud, shadow IT, etc.

Est-ce que les personnels d'entreprises sont réceptifs aujourd'hui au risque cyber ?

La sensibilisation à la sécurité est compliquée et le sera encore plus à l'avenir. Au risque de prendre les utilisateurs pour des enfants, la sensibilisation à l'hygiène informatique a eu du bon, avec des messages assez simples et de bon sens. Aujourd'hui, la sophistication des attaques et la motivation des attaquants que nous observons rendent plus difficiles les messages de sensibilisation. De plus en plus il va être difficile de distinguer le vrai du faux dans nos boites mails, par exemple. Donc il sera plus difficile d'en vouloir à un utilisateur qui aura été abusé par un moyen sophistiqué. Il faudra que les outils de protection soient plus efficaces et que l'on fasse moins reposer la sécurité de nos patrimoines sur la vigilance des utilisateurs.

Sur la réalité des cyber-attaques auxquelles les entreprises sont exposées, quel est l'enseignement de votre enquête ?

*Nous pouvons considérer que les grandes entreprises, étant maintenant en capacité de détecter les attaques, sont à même de les découvrir contrairement au passé. Mais aujourd'hui, tout a changé : si les attaques sont mieux détectées, elles sont bien plus nombreuses aussi. Exemple : le virus Dridex**, apparu à l'été 2015 caché dans des factures factices jointes aux emails envoyés à des millions de personnes, avait pour objectif de prendre le contrôle du poste de travail, pour ensuite récupérer les informations de connections des banques en ligne de l'utilisateur ; l'attaque visait des individus et non les entreprises, mais le danger venait tout de même de postes qui pouvaient être infectés or, au sein du Cesin, nous avons constaté que la prise de conscience du danger n'était pas la même chez tous nos adhérents... Contrairement à ce que clament les rapports, ce ne sont pas les fuites d'informations, les vols de données personnelles et les attaques virales générales qui sont constatées dans les faits comme les plus fréquents mais les ransomware (61%), les attaques virales générales (44%), les attaques par déni de service (38%) et les attaques ciblées (35%) ! Cela signifie que le perçu médiatisé cache la réalité du terrain.*

Est-ce qu'il existe des outils technologiques permettant aux entreprises de mieux se défendre ?

Nous avons vécu une décennie pendant laquelle, à l'apparition de chaque nouveau

danger, on nous expliquait qu'il fallait acheter un nouvel outil : pare-feux, pare-feux applicatifs, outils de détection pour remplacer les outils de prévention, outils anti-APT, etc. Certains éditeurs refont le design d'un ancien produit qui est alors rebaptisé nouveau produit, certains font vraiment de l'innovation (encore faut-il les repérer pour les encourager), d'autres enfin font de la consolidation d'offres, après s'être rachetés entre eux, pour offrir le « tout en un ». Or, dans la vraie vie de l'entreprise, ça ne marche pas comme cela. Si les responsables des SI n'ont pas une vraie réflexion d'architecture pour leur environnement, ils risquent de se retrouver avec des empilements de briques qui ne les protègent pas vraiment. Puisque les virus (Dridex, Cryptolocker, etc.) passent, même dans les grandes entreprises, c'est bien la preuve qu'elles sont mal protégées ou que les technologies utilisées sont inefficaces !

Quel est le constat en termes de moyens humains ?

Nous faisons face à un vrai déficit de compétences qui empêche les entreprises ayant la volonté d'embaucher de pouvoir le faire ! Il faut pouvoir former les jeunes recrues, les entrainer et leur offrir des possibilités d'évolution, ce qui n'est pas toujours simple. Comme la France ne forme pas assez d'experts en sécurité, il risque de se passer le même phénomène qui a été constaté avec les infirmières, à savoir recruter à l'étranger ! Pour ce qui concerne les RSSI il n'y a pas trop de problème, mais c'est pour les analystes, qui travaillent en nombre dans les équipes des RSSI pour superviser la sécurité dans les entreprises, que le problème est crucial.

*Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la sécurité de l'information et du numérique. www.cesin.fr

**http://assistance.orange.fr/ordinateurs-peripheriques/installer-et-utiliser/la-securite/risques-et-prevention/virus/botnet-dridex_138155-150310#onglet1

• Que retenir de cet entretien avec Alain Bouillé ?

- 93% des RSSI considéraient que le digital était devenu un enjeu stratégique pour leur entreprise.
- La digitalisation se traduit par des portes et des fenêtres qui s'ouvrent à tous vents sur des systèmes d'information qui vont être davantage éparpillés.
- Les attaques devenant de plus en plus sophistiquées, la simple hygiène informatique des personnels ne suffit plus : il faut des outils de sécurisation adaptés.
- Alerte maximale au « ransomware » !
- Peut-être pas le « Best of breed », mais sûrement pas non plus le « Tout en un », c'est le message du CESIN aux éditeurs de logiciels de sécurité.
- Il y a un vrai problème de ressources humaines par manque de compétences sur le marché.

Biographie – Alain Bouillé a passé 10 ans dans la banque d'affaires américaines JP Morgan, où il a été notamment en charge du programme sécurité du système d'information pour les régions Europe et Afrique, avant de devenir RSSI du groupe La Poste. Il est depuis 2001 Directeur de la Sécurité des Systèmes d'Information du Groupe Caisse des Dépôts, en charge de l'élaboration de la politique de sécurité du Groupe, de la coordination et du pilotage de sa mise en œuvre dans les entités du Groupe et du contrôle de son efficacité. Alain Bouillé est membre du CLUSIF, du club R2GS, du CIGREF, du Cercle Européen de la Sécurité et préside, depuis juillet 2012, le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) qui regroupe près de 150 RSSI de grandes entreprises.

• LE RÔLE DE L'ETAT FRANÇAIS DANS LA FILIÈRE NUMÉRIQUE

Trois interviews de SECURITY DEFENSE Business Review, permettent de mieux comprendre le positionnement de l'ANSSI, du Ministère de la Défense, du Ministère de l'Intérieur et de la Gendarmerie sur le Cyber. SDBR avait demandé à Guillaume Poupard Directeur Général de l'ANSSI, au Vice-amiral Arnaud Coustillière, Officier général Cyberdéfense à l'Etat-major des Armées, à l'Ingénieur en Chef des Armées Frédéric Valette, Responsable du pôle sécurité des systèmes d'information de la DGA, et au Général d'Armée Marc Watin-Augouard, Directeur du centre de recherche de l'Ecole des officiers de la gendarmerie nationale, de s'exprimer sur ces sujets. Voici l'essentiel des ces interviews ci-après.

SDBR N°126 - 21/04/2015

SDBR : En termes de capacité technologiques n'avons-nous pas déjà une idée assez précise de ce qui va se passer dans le monde Cyber ?

Marc Watin-Augouard : Certes, mais il est aussi important d'anticiper les usages qui vont en naître. Il n'y a que 8 ans que les gens ont commencé à disposer d'un Smartphone. Combien d'usages sont nés de ce téléphone intelligent en 8 ans? C'est considérable! La prospective par rapport aux usages n'est pas simple et l'un des objectifs du FIC est justement d'échanger autour de cette problématique.*

Faut-il avoir peur du risque Cyber ?

Je dis toujours - il ne faut pas avoir peur d'avoir un peu peur - car le stress peut inciter à ne pas baisser la garde. Nous sommes en pleine transformation numérique et digitale, la société va changer de paradigme et nous allons assister à des évolutions considérables avec le Cloud, le Big Data, la Robolution, l'intelligence artificielle, etc. La donnée devenant le centre de gravité du cyberespace, nous allons complètement changer nos rapports à la Santé, à l'Education, à la Culture, à la Démocratie, etc. Tout va très vite. Aujourd'hui nous avons en outre des usages de ces outils qui n'étaient pas imaginés à leur démarrage.

Avez-vous le sentiment que la France anticipe ces changements à venir ?

Le temps du politique est souvent celui de l'immédiat, avec les exigences du traitement des problèmes dans le monde réel. Il faut que nos dirigeants portent en même temps un regard sur le futur. C'est toute la difficulté de l'exercice! Il faut offrir une vision, tout en répondant à l'urgence du quotidien. Le Plan sur la Nouvelle France industrielle ne bénéficiera pas immédiatement à ceux qui l'ont lancé, mais c'est un investissement pour l'avenir. Il ne faut pas sacrifier la prospective face à la pression de l'instant, sinon on risque de prendre de plein fouet les conséquences de la transformation numérique...

N'y a-t-il pas une inadéquation des profils de la fonction publique aux enjeux de demain ?

Il faudra bien se poser la question du recrutement des personnes qui arrivent par concours d'administrations (ENA, Police, Gendarmerie, administrations diverses) et qui vont être en poste pendant plus de 30 ans. Dans 15 ans, si les profils recrutés ont été formés selon les archétypes du 20ème siècle ou qu'ils ont simplement subi une acculturation aux principes cyber du 21ème siècle, il y aura un grave problème pour la France. Cela signifie qu'il faut changer les modes de sélection et qu'il faut instaurer des concours plus axés sur les technologies numériques. Ce sont des enjeux de ressources humaines.

Où en est le concept de souveraineté en matière de Cyber ?

La souveraineté ne sous-entend pas forcément d'être franco-français, car c'est souvent une vue de l'esprit. Etre souverain signifie que nous avons consenti à des abandons de souveraineté mais, pour pouvoir le faire, il faut un minimum de degrés de libertés: avoir des capacités technologiques, de la recherche et du développement, des capacités humaines. Nous avons les ingrédients, mais il faut les structurer et les organiser pour avoir au minimum une réponse, française ou européenne, et à défaut faire partie des réponses. Nous avons perdu la bataille du hardware (plus de fabrication d'ordinateurs), nous avons perdu la bataille du software (sauf cas particuliers), mais nous n'avons pas encore perdu la bataille des données sur lesquelles nous avons beaucoup de potentialités: Big Data, IoT, Robolution, réalité augmentée, intelligence artificielle, etc. S'il y a une volonté politique de faciliter ces développements, avec une vraie vision stratégique, nous pourrons peut-être reprendre le leadership. Pour cela, il faut que la start-up qui porte un projet novateur ne reste pas sur la touche, car les grandes entreprises de demain ne sont pas encore nées.

* FIC : www.forum-fic.com
** CORIIN : http://www.cecyf.fr/activites/recherche-et-developpement/coriin

• **Que pouvons-nous retenir de l'interview du GAR Marc Watin-Augouard ?**

- La révolution numérique en est encore à ses débuts et nous sommes loin d'avoir

tout vu ; beaucoup d'outils peuvent encore apparaître dans les années qui viennent.
- La lutte contre la cybercriminalité ne bénéficie pas d'un soutien fort de l'Etat français, or il faudrait anticiper sur les menaces de demain au lieu d'être focalisé sur les menaces d'aujourd'hui...
- Les prédateurs opèrent un transfert vers le cyberespace. Il faut que la Justice s'adapte rapidement à ce nouveau danger.
- Il va bien falloir adapter les profils de la fonction publique en tenant compte de la révolution numérique. Oui, mais quand...?
- Les grandes entreprises de demain ne sont pas encore nées, donc les start-up novatrices doivent être soutenues.

Biographie – Ancien inspecteur général des armées-gendarmerie, le général d'armée (2S) Watin-Augouard a animé un groupe de travail qui a contribué à la rédaction du rapport de Thierry Breton sur la cybercriminalité (2005). Conscient de l'impérieuse nécessité de développer une coopération interservices et internationale pour mieux lutter contre les prédateurs du cyberespace, il a été, avec le concours actif de Régis Fohrer, le fondateur du FIC en 2007. Le succès croissant de cette manifestation n'est pas la conséquence d'un effet de mode mais témoigne d'une demande d'acteurs publics et privés confrontés à des attaques de plus en plus nombreuses et de plus en plus destructrices de valeurs. Aujourd'hui directeur du centre de recherche de l'Ecole des officiers de la gendarmerie nationale (EOGN), il est l'un des trois membres du comité de direction du FIC. Dans les universités où il enseigne (Paris II, Paris V, Lille II, Aix-Marseille III, Clermont-Ferrand) et à l'Ecole de guerre, il sensibilise les élèves sur les enjeux de la société numérique. Il a contribué aux travaux du Livre blanc de la défense et de la sécurité nationale.

* * *

SDBR N°138 - 17/11/2015 - Interview du vice-amiral Arnaud Coustillière, officier général Cyber-défense à l'Etat-major des Armées et de l'ICA Frédéric Valette, responsable du pôle sécurité des systèmes d'information de la DGA.

SDBR : En 2015, que peut-on dire des remontées d'incidents observées par le Calid ?*

*En 2013 et en 2014, le Calid avait traité environ 800 incidents dans l'année. Il est intéressant d'observer une forte baisse du nombre global d'incidents à traiter sur l'année 2015. Deux raisons à cette baisse: le taux de fausses alertes (ce que l'on nomme les faux positifs), car en 2015 le MTLID** est devenu pleinement opérationnel; l'hygiène informatique des utilisateurs a progressé, ce qui a permis aussi de réduire le nombre d'incidents. A fin juin 2015, nous avions traité 350 incidents, ce qui devrait aboutir à environ 600 incidents pour l'année. Par contre, sur les incidents traités en 2015, nous découvrons des incidents plus ciblés visant le ministère de la Défense.*

Nous n'avons, pour l'instant, pas trouvé de pénétration de nos systèmes, mais nous avons trouvé des choses potentiellement graves. Par contre, nous relevons plus d'incidents venant de l'environnement de nos systèmes d'armes via nos sous-traitants. Chez certains des sous-traitants, l'hygiène informatique est parfois insuffisante.

Certains parlent de menace vraiment effrayante. Qui croire ?

Il faut parler de menace «potentiellement» effrayante. Nous nous protégeons en fonction de l'estimation que nous avons de la menace. Regardez l'attaque subie par TV5 Monde, qui a vu tomber son système de production d'images TV dans ses différents supports: d'après les experts, l'attaque a montré une forte technicité des attaquants, avec une chronologie sur plusieurs mois et une maitrise complète du réseau en profondeur. De la même façon par exemple, une telle attaque pourrait faire tomber le système de distribution de l'eau d'une ville, ou le cœur d'une usine de production ou le centre de régulation du réseau RER en Ile de France, etc. Le risque vient de l'attaque en profondeur qui ne permet pas de voir, pendant des mois, que la menace est déjà entrée. Donc, en effet, cette menace est potentiellement effrayante.

Mais, sur les sites sensibles, ne disposez-vous pas d'outils pour détecter ce type de pénétration ?

*Aujourd'hui, les outils et les méthodes que nous mettons en place sont là pour détecter ce type de comportement: l'analyse des traces laissées par l'attaquant permettant de déclencher une alerte sur la base de signaux faibles, ou le déclenchement des GIR (groupe d'intervention rapide) préventifs, en allant sur place, sortes de patrouilles dans l'espace numérique suite à un incident qui semble bizarre. Sur le périmètre du ministère de la Défense, nous avons en permanence quatre ou cinq GIR qui font de l'investigation. En outre, chaque jour le Calid dispose de nouvelles signatures suspectes, les intègre dans ses bases de données et déclenche une analyse rétroactive sur les anciens logs, de façon à vérifier qu'une attaque ne soit pas passée sous nos radars. En 2011, le Calid était constitué de 17 personnes, aujourd'hui il comprend près de 80 personnes et il atteindra 120 personnes en 2018. A coté du Calid, la Dirisi*** *a créé sa fonction cybersécurité de 25 personnes et, au sein de chaque armée, ont été créées des antennes techniques. La fonction lutte informatique défensive sera passée en gros de 20 personnes en 2011 à pratiquement 500 en 2019.Par ailleurs, la partie SSI classique (architecture des systèmes d'information et homologation) a été dotée d'une centaine de postes supplémentaires.*

Quelle est la place du militaire dans le combat numérique ?

L'espace numérique est un nouvel espace, très complexe, où s'interpénètrent les différents services de l'Etat. Le meilleur exemple est celui d'une mafia russophone, qui un

jour fait de la cybercriminalité, le lendemain se loue à des cyber-activistes et le troisième jour sert à une action stratégique pour déstabiliser un Etat; là, nous ne sommes plus simplement dans une affaire de continuité et de sécurité, mais plutôt dans le relevé de signatures et de comportements. Nous pouvons faire une comparaison avec la mer où les pirates peuvent devenir des corsaires, rester des libertaires et évoluer au milieu des pécheurs. Le combat numérique est une sorte de combat urbain généralisé. Les mêmes outils servent à attaquer des cibles différentes, certaines mafias réalisant un chiffre d'affaires conséquent grâce à la prise d'entreprises en otage. Dans la logique d'emploi des opérations militaires, le militaire se met au cœur du combat numérique pour défendre le Mindef et accompagner les opérations.

De quoi avez-vous encore besoin, en termes de matériels et de moyens techniques ?

Il va nous falloir déployer d'autres systèmes experts et des sondes, par exemple sur les navires. Ce dont nous avons vraiment besoin, c'est de réfléchir avec les industriels à l'évolution de l'architecture des systèmes: par exemple, doit-on rester sur des systèmes complètement à plat où la partie guidage du navire est atteignable depuis n'importe quel PC, donc atteignable par un attaquant ? Il nous faut imaginer une architecture propre au navire, avec des systèmes spécifiques à chaque bateau et à chaque système d'arme embarqué. Sur notre exemple, n'importe quel PC ne doit pas pouvoir parler à l'automate qui gère le moteur du bateau. Cette logique d'apprentissage et de connaissances métiers doit être déployée avec chaque maitre d'œuvre industriel. Nous le faisons pour les bateaux, pour la défense anti-aérienne ou pour Scorpion. L'industriel peut être aidé par la DGA, mais doit aussi pouvoir se faire aider par des entreprises qui connaissent bien la cyberdéfense. DCNS le fait. D'autres industriels doivent s'y mettre.

* CALID : Centre d'Analyse en Lutte Informatique Défensive

** MTLID : Moyens Techniques de Lutte Informatique Défensive

*** DIRISI : Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information

• Quelles informations nous livrent Arnaud Coustillière et Frédéric Valette dans cette interview ?

- Le maillon faible se situe souvent chez les sous-traitants du MINDEF qui ne respectent pas toujours une hygiène informatique suffisante.
- Une attaque comparable à celle qui a touché TV5 Monde a nécessité une longue préparation en profondeur. Une telle attaque pourrait faire tomber le système de distribution de l'eau d'une ville, ou le cœur d'une usine de production ou le centre de régulation du réseau RER en Ile de France, etc.
- Le combat numérique est une sorte de combat urbain généralisé.

- Il faut vraiment réfléchir avec les industriels à l'évolution de l'architecture des systèmes : une logique d'apprentissage et de connaissances métiers doit être déployée avec chaque maitre d'œuvre industriel.

Biographie 1 – La carrière du vice-amiral Coustillière (promotion 1981 de l'Ecole Navale) s'est essentiellement partagée entre des embarquements et commandements opérationnels sur des navires de combat, et des postes de responsabilités en administration centrale, avec une spécialisation plus particulière pour les télécommunications et la cyberdéfense. Il a été nommé officier général à la cyberdéfense le 1er juillet 2011, à la création du poste. Directement rattaché au sous-chef « opérations » de l'état-major des armées, et placé sous la double tutelle du chef d'état-major des armées et du chef de cabinet militaire du ministre, il est responsable de la cyberdéfense du ministère et de sa conduite en situation de crise cybernétique. Le vice-amiral Coustillière est officier de la Légion d'Honneur, commandeur de l'ordre national du mérite, titulaire de la croix du combattant, de la médaille d'outre mer (Moyen Orient) et de la médaille de la défense nationale.

Biographie 2 – L'ICA Frédéric VALETTE est depuis le 2 Avril 2014 responsable du pôle Sécurité des Systèmes d'Information à la Direction générale de l'armement (DGA). Après avoir réalisé pendant dix ans un travail d'expertise en cryptographie dans un premier temps à l'ANSSI puis dans le centre DGA Maitrise de l'Information, il a successivement dirigé le département de cryptologie puis la division SSI qui regroupe les quelques 200 experts du domaine au sein du centre de DGA Maitrise de l'Information. Il est actuellement à la tête de l'ensemble des équipes techniques chargées au sein de la DGA de sécuriser les systèmes qui seront livrés aux forces et de mener une activité de R&D dans le domaine de la cyber-défense.

* * *

(SDBR N°118 - 16/12/2014) Interview de Guillaume Poupard, directeur général de l'ANSSI*

SDBR : 9 mois après votre nomination au poste de directeur général de l'Agence nationale de la sécurité des systèmes d'information, quel regard portez-vous sur l'ANSSI ?

Guillaume Poupard : J'ai trouvé en l'ANSSI une maison remarquable par son dynamisme et la qualité de ses collaborateurs, une maison en ordre de marche qui a su trouver sa place dans son écosystème, comme entité interministérielle faisant en sorte que chacun puisse apporter sa pierre à un édifice de la cybersécurité devenu priorité nationale. La plupart des décideurs publics et privés a compris que le risque est réel, à la hauteur des opportunités portées par le numérique. Mais la tâche est gigantesque, car nous sommes tous concernés par les problèmes de cybersécurité: l'État, les entreprises petites et grandes, les collectivités territoriales, les organisations non gouvernementales et les citoyens. Nous

sommes tous devenus des cibles et chaque type de cible requiert des attentions particulières et adaptées.

Y a-t-il des pistes de progrès identifiées ?

*Nous travaillons au service du gouvernement et des administrations de l'État et nous avons étendu notre action aux opérateurs d'importance vitale (OIV) depuis que la loi nous en a ouvert la possibilité en décembre 2013**. Télécoms, énergie, transports...nous travaillons avec tous les secteurs importants pour la Nation et la vie quotidienne des Français afin d'augmenter la sécurité de leur infrastructure informatique la plus sensible.*

Aux Assises de la sécurité et des SI, en octobre à Monaco, vous disiez que «la période d'évangélisation à la cyber menace était passée et qu'il fallait maintenant réagir et passer à l'action». Qu'entendez-vous par là ?

Nous sommes déjà dans l'action car, aujourd'hui, l'ANSSI a une activité opérationnelle sur les réseaux sensibles qui comprend la détection des attaques informatiques, leur traitement et le renforcement de la sécurité des systèmes d'information visés. En matière d'évangélisation, l'ANSSI et d'autres ont fait beaucoup pour expliciter les risques, la réalité nous ayant bien aidés d'ailleurs à cette prise de conscience. Pour vraiment convaincre d'éventuelles réticences, il convient de parler avec les dirigeants de l'entreprise ou de l'organisation pour leur expliquer que le retour sur investissement en matière de cybersécurité doit être géré différemment des autres investissements, mais qu'il fait néanmoins partie des mécanismes de bonne gestion, car une attaque informatique porte sur l'ensemble de la chaîne de valeur de l'entreprise. La difficulté est de valoriser ce risque, mais le sujet progresse, par exemple grâce aux travaux des assureurs.

«Arrêter de se faire siphonner par nos amis», disiez-vous à Monaco… Pensez-vous qu'il y ait une différence entre se faire pirater par un «ami» ou un «non-ami» (puisque la France n'a pas d'ennemi déclaré) ?

Nous n'avons ni ennemi ni ami dans le cyberespace. Nous avons des alliés dont nous avons besoin, mais ces alliés s'intéressent parfois de près à ce que nous faisons. Nous sommes dans un contexte géopolitique complexe, avec des États ou des groupes qui sont actifs dans les réseaux de communications électroniques et qui peuvent faire appel à des capacités offensives pour nous nuire. Dans le domaine du renseignement, les révélations faites par Edward Snowden depuis deux ans montrent que la France est une cible. Ce qui importe, c'est de se défendre à la hauteur du risque, en y consacrant les moyens nécessaires. Donc soyons crédibles en matière de cybersécurité, défendons nos biens matériels et immatériels les plus précieux, qu'il s'agisse d'informations de souveraineté, de patrimoine intellectuel, de capacités économiques et militaires, ou plus largement de la vie numérique des Français.

La filière numérique française est-elle vraiment encouragée par des commandes concrètes de l'administration ?

Ne nous plaignons pas d'avoir en France un code des marchés publics qui oblige les marchés à se dérouler de façon transparente. Ce code n'indique pas qu'il faut systématiquement acheter auprès de celui qui vend le moins cher, ou qu'il faut obligatoirement mettre en concurrence tous les acteurs de la planète. Si on a la volonté d'acheter des produits de confiance qualifiés par l'ANSSI, c'est tout à fait réalisable. Il faut donc d'une part évangéliser encore les administrations et d'autre part expliquer aux acheteurs la méthode à adopter pour sélectionner des produits qualifiés dans le cadre des marchés publics. C'est pourquoi nous avons produit, avec le ministère de l'économie, des finances et de l'industrie un guide détaillant la marche à suivre. Il est disponible sur le site de l'ANSSI. Je comprends donc très bien que des PME, comme celles du groupement Hexatrust, dont le lancement a été soutenu, souhaitent désormais accéder à des commandes de l'administration. Non seulement la commande publique crée du chiffre d'affaires pour les PME - c'est essentiel - mais elle crée également une référence qui a une valeur, notamment à l'export.

«Relocaliser les données en France» disiez-vous à Monaco. N'y va-t-il pas un problème de coûts ?

Peut-être un peu, encore faut-il regarder précisément de combien. Aujourd'hui, dans un Data Centre, il n'y a pratiquement aucun humain, donc pourquoi l'implanter dans un pays à la main d'œuvre peu chère? Autant les activités à forte présence humaine peuvent entrainer des surcoûts importants attachés aux salaires et aux taxes sur les salaires, autant quand il n'y a pratiquement personne on peut se demander quelle est la justification économique d'une délocalisation? Si le surcoût est minime, on doit pouvoir l'assumer. Un dumping trop accentué doit nous conduire à nous interroger sur d'éventuelles arrière-pensées obscures...

Quel est votre objectif pour l'année 2015 ?

C'est clairement la définition précise des règles de sécurité, dans le cadre de la loi de programmation militaire, pour les opérateurs d'importance vitale. Ce ne sont pas que des mots, puisqu'il est impératif de définir en collaboration avec eux les règles de sécurité qui vont significativement élever leur niveau de sécurité tout en restant soutenable humainement et financièrement. L'autre objectif est de continuer à développer une politique industrielle afin de doter la France d'une industrie de la cybersécurité forte et sérieuse. Elle devra offrir des solutions fonctionnelles de bon niveau de confiance, sans pour autant être enfermée en France, ce qui signifie que la coopération doit rester ouverte avec des partenaires hors de France pour pouvoir aborder la compétition internationale.

*ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information www.ssi.gouv.fr
** Articles 21 à 25 de la loi n°2013-1168 du 19 décembre 2013.

• Que doit-on retenir de l'interview de Guillaume Poupard ?

- Le risque cyber concerne l'État, les entreprises petites et grandes, les collectivités territoriales, les organisations non gouvernementales et les citoyens. Nous sommes tous devenus des cibles et chaque type de cible requiert des attentions particulières et adaptées.
- Un client, quel qu'il soit, doit pouvoir se tourner vers des prestataires de confiance qui s'engagent à respecter une charte de confiance et sont compétents pour intervenir.
- La valorisation du risque cyber est une tache difficile.
- Il n'y a ni ennemi ni ami dans le cyberespace.
- Dans un Data Centre il n'y a pratiquement aucun humain, donc pourquoi l'implanter dans un pays à la main d'œuvre peu chère ? Sauf à avoir des arrières-penses obscures…
- Il faut continuer à développer une politique industrielle afin de doter la France d'une industrie de la cybersécurité forte et sérieuse.

Biographie - Guillaume Poupard débute sa carrière comme expert puis chef du laboratoire de cryptographie de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). Cette direction sera transformée en 2009 pour devenir l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Il rejoint en 2006 le Ministère de la défense, toujours dans le domaine de la cryptographie gouvernementale, puis de la cyberdéfense. En novembre 2010, il devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la Direction Générale de l'Armement (DGA), responsable de l'expertise et de la politique technique dans le domaine de la cybersécurité. Le 27 mars 2014, il est nommé directeur général de l'Agence nationale de sécurité des systèmes d'information.

Guillaume Poupard est ancien élève de l'Ecole Polytechnique, promotion X92. Ingénieur de l'armement en option recherche, il est titulaire d'une thèse de doctorat en cryptographie réalisée sous la direction de Jacques Stern à l'Ecole Normale Supérieure de Paris et soutenue en 2000. Il est également diplômé de l'enseignement supérieur en psychologie.

5. Les interceptions de communication

Il ne peut y avoir de lutte contre la criminalité petite ou grande, contre les trafics illicites, contre les prédateurs de type pédophile, contre les pilleurs du savoir-faire des entreprises ou contre les terroristes sans écoutes téléphoniques et interceptions de communications, quelles qu'elles soient. Les interceptions de communications peu-

vent relever soit du ministère de la Justice (enquêtes de police judiciaire), soit des services du Premier ministre, du ministère de la Défense et du ministère de l'Intérieur pour les affaires touchant à la Défense nationale et à la Sécurité.

Régulièrement des polémiques surgissent dans les medias sur les interceptions de communications, eu égard à la nécessaire protection de la vie privée des individus. Il est vrai que certaines écoutes de personnalités ont un caractère purement politique et rappellent, à bien des égards, l'époque des gouvernements gaullistes et mitterrandiens. Au-delà de ces anecdotes marginales, la population a bien compris, surtout depuis les attaques djihadistes sur le sol européen, que sans écoute les forces de police et de gendarmerie étaient aveugles ou presque, donc que les méchants et les voleurs pouvaient bien être bousculés dans leur vie privée : du bon sens en fait ! Il est par contre regrettable que la CNIL (commission nationale informatique et liberté) fasse en permanence de l'orthodoxie rétrograde face à des menaces grandissantes, en privant les autorités d'outils modernes (exemple la carte d'identité biométrique toujours pas adoptée en France) ou face à des évolutions technologiques bien plus rapides que sa capacité à émettre des avis et qu'elle bride en cela les performances de certaines sociétés françaises innovantes.

Pour mieux comprendre ces problématiques, SDBR a donné la parole à Alain Juillet, ancien Haut Responsable à l'Intelligence Economique (HRIE) auprès du SGDSN, et à Constant Hardy, commissaire aux communications électroniques de Défense.

(SDBR N°130 du 23/06/2015) - Interview d'Alain Juillet Ancien Haut Responsable à l'Intelligence Economique, président du CDSE*

SDBR : Ne trouvez-vous pas étonnant qu'une loi sur la protection du secret des entreprises ne puisse être votée, en même temps qu'une loi très controversée sur le renseignement soit votée dans l'urgence ?

Alain Juillet : Je suis pour la loi sur le renseignement, qui a été votée en force, car la France doit disposer d'un certain nombre d'armes face au terrorisme. Cette loi a pu être votée du fait de l'émotion provoquée par les attaques terroristes et de la volonté d'appliquer une forme de principe de précaution face à la menace. La loi a été préparée durant l'été 2014, mais le vote de la loi a bénéficié de l'impact émotionnel des attentats de janvier 2015 à Paris. Nous sommes sur un terrain difficile, car d'un côté il faut pouvoir protéger la population et d'un autre coté on ne peut accepter un affaiblissement trop fort de nos libertés individuelles, même si les individus sont dans une logique nouvelle de réduction de leurs libertés, au profit de leur sécurité ou pour des raisons mercantiles (par l'utilisation du mobile).

Que voulez-vous dire ?

Lorsque vous achetez un mobile et que vous activez son GPS, tout le monde peut savoir

où vous êtes. Lorsque vous achetez un livre sur Amazon ou une réservation sur Booking, vous tombez dans les filets technologiques d'entreprises comme Cisco, qui vont vous définir comme lecteur potentiel de telle publication ou comme client potentiel de tel ou tel hôtel ou destination. C'est une forme d'espionnage et une perte manifeste de liberté individuelle. Grâce aux cookies, les individus aliènent leur liberté personnelle sans le savoir. Dans d'autres domaines, comme la conduite automobile, on assiste aussi à la perte totale de la liberté individuelle, au nom de la sécurité prônée par la raison et des groupes de pression. Le numérique amplifie aujourd'hui ce phénomène et les individus ne s'en rendent pas compte. Vous constatez les mêmes problématiques sur les mots et sur la liberté de penser. En matière d'intelligence économique, nous sommes aussi face à une forme de pensée unique qui bride la pensée concrète: nos amis sont nos amis et il est interdit de dire qu'ils peuvent nous voler...

Pourtant, l'actualité n'apporte-t-elle pas régulièrement des preuves tangibles de l'espionnage fait par « nos amis » ?

Nous savons, depuis longtemps, qu'il y a un accord entre Britanniques et Américains pour collaborer très étroitement dans le domaine de la recherche et de l'échange d'informations. Nous comprenons aujourd'hui que ce type d'accord existe aussi entre les Américains et les Allemands; c'est le droit des Allemands. Ce qui est gênant, c'est d'apprendre qu'ils regardent ensembles ce qui se passe en France et dans les pays du sud de l'Europe, car les Allemands sont nos plus proches alliés! J'ai toujours dit qu'en matière économique il n'y a pas d'amis, donc rien d'étonnant, mais pourquoi eux pourraient-ils le faire et pas nous? Peut-être l'affaire de l'espionnage d'Airbus par les Allemands, sortie récemment dans la Presse allemande, n'est-elle qu'une manipulation, faite par ceux qui ont intérêt à semer la zizanie entre l'Allemagne et la France? A qui profite l'affaire? L'immense mérite d'Edgar Snowden est d'avoir fait comprendre, à des gens qui ne voulaient absolument pas y croire, que ce que nous disions depuis au moins dix ans était réel. Le paradoxe aujourd'hui, dans l'esprit des Français en général, est de penser «oui c'est normal, les Américains nous écoutent»... Ce constat est très grave! La pensée unique se satisfait d'un certain nombre de choses ou bien, lorsque les faits ne conviennent pas, s'y substitue la politique de l'autruche à savoir «ça n'existe pas...je ne vois rien...». Nous sommes en plein déni de réalité. A l'inverse, lorsque le législateur envisage de renforcer nos moyens de défense (loi sur le secret des affaires), nous assistons à un tollé d'indignation! C'est le monde à l'envers!

Alors, que faire dans ce monde violent pour protéger nos pépites industrielles ?

La première chose à faire est d'être réaliste et d'arrêter de faire du déni de réalité. Cela

sous-entend de se connaitre, de connaitre l'adversaire, de le nommer et de ne pas se tromper d'ennemi. Ensuite, il faut décider de se battre pour préserver nos intérêts et les défendre. Je ne suis pas sûr que l'intelligence économique joue son rôle en France, quand j'observe certaines dernières affaires de cessions (de grandes entreprises ou de PME) ou de transferts d'activité. Nous devrions au moins nous demander: pourquoi partent-elles? Répondre que c'est la fiscalité qui provoque les départs est insuffisant, car ce n'est jamais la seule raison! Notre société de l'entre-soi, construite autour de dirigeants issus du même monde et des mêmes écoles, ne comprend rien au monde des start-up et ne le fréquente pas, sinon en surface. Or l'avenir est dans le monde des start-up. L'Etat français n'a pas su protéger certaines entreprises de grande valeur, au moins espérons qu'il soutiendra réellement enfin les start-up! Pour cela, il faudrait avoir une vision stratégique de long terme qui manque depuis la fin du Commissariat au Plan.

*CDSE : Club des Directeurs de Sûreté des Entreprises https://www.cdse.fr

• Que doit-on retenir de l'interview d'Alain Juillet ?

- D'un côté il faut pouvoir protéger la population et d'un autre coté on ne peut accepter un affaiblissement trop fort de nos libertés individuelles, même si les individus sont dans une logique nouvelle de réduction de leurs libertés, au profit de leur sécurité ou pour des raisons mercantiles (internet et mobiles).
- Grace aux cookies, les individus aliènent leur liberté individuelle sans le savoir...
- Le numérique amplifie ce mouvement d'aliénation. On est loin des écoutes téléphoniques de l'Etat...
- L'immense mérite d'Edgar Snowden est d'avoir fait comprendre, à des gens qui ne voulaient absolument pas y croire, que ce que nous disions depuis au moins dix ans était réel ! Nous sommes cependant encore en plein déni de réalité !
- L'intelligence économique ne joue pas son rôle en France lorsqu'on voit certaines cessions se faire à des groupes étrangers !
- Il n'y a plus en France de vision stratégique de long terme, depuis plus de 15 ans.

Biographie - Aujourd'hui conseiller chez Orrick Rambaud Martel, Alain Juillet a été Haut Responsable chargé de l'Intelligence Economique (HRIE) auprès du Premier ministre de 2004 à 2009, après avoir été Directeur du Renseignement à la DGSE de 2002 à 2003. De 1967 à 2002, il a exercé différents postes dans différents groupes dont le groupe Pernod-Ricard et le groupe Jacobs-Suchard. Alain Juillet est colonel de réserve parachutiste, diplômé d'Etat-major (Esorsem), breveté parachutiste français et anglais, et a été auditeur de l'Institut des Hautes Etudes de la Défense Nationale. Il est aussi diplômé de l'Institut des Hautes Etudes de Sécurité Intérieure, du Stanford Executive Programm 88 (Stanford / Californie), du Centre de Perfectionnement aux

Affaires (1981). Alain Juillet est Commandeur de la Légion d'Honneur et chevalier de l'Ordre National du Mérite à titre militaire. A titre civil, il est Officier du Mérite agricole ; chevalier des Palmes académiques et chevalier des Arts et des Lettres.

* * *

Dans l'interview qui suit, parue le 11/03/2014 dans SDBR N°101, Constant Hardy, Commissaire aux Communications Electroniques de Défense (CCED) nous explique comment fonctionne ce commissariat en charge des moyens d'interceptions de communications.

SDBR : Quelles sont les attributions du CCED ?

Constant Hardy : A l'origine, le CCED s'occupait essentiellement des réseaux spécialisés (sirènes d'alerte et autres), puis il est devenu une fonction interministérielle car il y a des problématiques de défense (non militaire) et de sécurité multi-opérateurs, souvent interministérielles, s'occupant des réseaux de communications électroniques : il s'agit de toute communication par voie électronique (filaire, radio, etc.). Dans les définitions du code des postes et communications électroniques, sont évoquées les notions de transmission à distance et d'acheminement, de réseaux et de services de communications électroniques ouverts au public. Concernant les réseaux, il peut y avoir plusieurs couches avec des artères de transmission et des nœuds d'acheminement ; c'est le cas du traitement des mails ou des messageries instantanées. Les réseaux en couches sont de plus en plus fréquents dans le cas des services over the top (OTT), ces sociétés de services qui exploitent le réseau de l'opérateur pour proposer des services aux consommateurs (transport d'informations audio et vidéo sur Internet), sans cotiser auprès de l'opérateur pour l'utilisation du réseau, comme par exemple Skype ou WhatsApp. Ce qu'on appelle l'internet grand public aujourd'hui, ce sont toutes les ressources de ces interconnections de réseaux qui sont accessibles à tous les utilisateurs de l'internet.

Concrètement, avec qui traitez-vous les sujets qui sont de votre ressort ?

Sur tous les réseaux ouverts au public, nous nous occupons de tous les aspects de défense et de sécurité ou de sécurité publique. Dans ces aspects, certains ne sont pas confidentiels et sont traités dans la CI-CREST (commission interministérielle de coordination des réseaux et des services de communications électroniques pour la défense et la sécurité publique, à laquelle participent la FFT et les grands opérateurs) ; c'est le cas par exemple des sujets qui touchent aux appels d'urgence (le 112), aux alertes aux populations, aux processus de déclarations d'incidents ou aux conditions de sécurité à introduire dans les marchés publics concernant les communications électroniques. D'autres nécessiteront d'appliquer le « besoin d'en connaitre » (restriction de l'accès à une information considérée*

comme sensible), par exemple les besoins d'interception de communication ou de mise à disposition de données. Certains sujets sont intermédiaires, par exemple les moyens de contrôles de sécurité dans les réseaux dont nous parlons avec la FFT ; lorsqu'on définit des profils de sécurité, nous sommes déjà dans un niveau de confidentialité qui ne doit pas sortir d'un cercle restreint (FFT plus CCED) ; mais lorsqu'un contrôle de sécurité est effectué sur un réseau, il n'y a aucune raison que cela soit partagé avec les autres opérateurs (donc avec la FFT).

Qu'est-ce qui mobilise le plus votre attention ?

Les interceptions de communication et la mise à disposition de données accaparent une grande partie de nos travaux car les réseaux évoluent, d'où la nécessité de disposer de systèmes performants. Pour quantifier en volume le besoin de performance des systèmes, il faut se référer au nombre de condamnations en correctionnelle annuel qui est de 500.000 (source ministère de la Justice). Le nombre de condamnations (donc d'affaires résolues) permet d'évaluer le nombre d'enquêtes qui sont générées chaque année... En s'en tenant uniquement au nombre des condamnations, ce chiffre permet d'estimer le nombre de requêtes annuelles faites aux opérateurs dans le cadre des enquêtes. Ces volumes ne sont évidemment pas liés à une quelconque curiosité des enquêteurs, mais au nombre d'actes de délinquance. Les services d'enquêtes de l'Etat doivent avoir une certaine efficacité face à des délinquants très organisés, donc nous travaillons à leur fournir des systèmes performants, voire à « industrialiser » certaines méthodes de réquisition, pour en augmenter la standardisation et la rapidité de réponse tout en en diminuant les coûts. Par exemple, dans l'affaire Merah, c'est grâce à ce type de questionnaire standardisé que les enquêteurs ont pu remonter jusqu'à la mère du terroriste (quelle adresse IP a été utilisée sur tel site web et quelle est la personne qui détient cette adresse IP ?).

Comment techniquement se passe une interception ? Nous ne sommes plus à l'époque de l'enquêteur qui pose des fils dans la cave de l'hôtel, n'est-ce pas ?

Cette méthode, que vous rappelez, marchait très bien sur le réseau fixe traditionnel jusqu'à la fin des années 80 et d'ailleurs, dans les petites bourgades, des fils étaient branchés entre l'autocom et le poste de police ou de gendarmerie, ce qui facilitait une éventuelle interception. Au début des années 90, les américains ont voulu passer à une méthode évitant des branchements physiques et sortant l'interception du contexte local, en mettant en place des fonctions directement au niveau des commutateurs numériques. Mais ce qui a totalement changé le paysage fut l'arrivée des réseaux mobiles, nous obligeant à poser des systèmes directement intégrés dans les réseaux, qui créent une copie et la renvoient vers le service d'enquête. Le CCED fait donc

des prescriptions d'interface, comme cela est fait dans tous les pays du monde, sur la base des standards que nous choisissons ou que nous adaptons. Nous sommes aussi prescripteurs sur la façon de procéder à l'interception dans le réseau, en fonction des nœuds et des choix qui se présentent techniquement à l'opérateur. Dans le monde de la voix, les choix d'architecture sont relativement limités ; dans le monde de l'internet, c'est plus varié et il y a de vrais choix d'architectures possibles. Ensuite, les opérateurs passent à la phase d'achat auprès des équipementiers (matériels et programmes) en coordination avec le CCED: pour des équipements mis à l'intérieur des réseaux et liés aux cœurs de réseaux, ils proviennent obligatoirement du fournisseur du cœur de réseau (et il y en a peu) ; pour des équipements de médiation, il y a quelques fabricants français et quelques européens. Nous remboursons ces équipements, autorisés par l'ANSSI, aux opérateurs mais ils en restent propriétaires et responsables.

Nous avons parlé de déclarations d'incidents. Pouvez-vous nous en dire plus ?

Sous l'angle de la sécurité, nous faisons l'analyse de tous les incidents d'importance qui peuvent se produire chez les opérateurs, pour transmettre aux pouvoirs publics une image fidèle de la nature des incidents qui puisse servir d'aide éventuelle à la décision. Est important pour nous un incident qui aura impacté quelques centaines de milliers d'abonnés, soit pour l'instant un ou deux par an. Le Retex de ces incidents fait apparaitre 2 causes majeures : en premier lieu, une erreur humaine de manipulation ; en deuxième, un défaut de conception du matériel (exemple, un enchaînement de commandes incompatibles provoquant une panne de serveur).

*Avez-vous un commentaire sur l'article 20** de la LPM dédié à l'accès administratif aux données de connexion ?*

Par nature, en matière de sécurité, l'Etat fait du préventif en s'autosaisissant, alors qu'en matière criminelle le fait générateur de l'enquête est le fait délictueux avéré. Il y a eu une polémique sur la vie privée des personnes. Le problème de fond, c'est que tout délinquant considère que son délit ou son crime fait partie de sa vie privée, donc il y a un problème d'équilibre entre la vie privée à préserver et la possibilité pour les enquêteurs d'aller fouiller quelques éléments de la vie privée des délinquants. Il faut souligner qu'aujourd'hui les moteurs de recherche, la NSA peut-être aussi grâce au Patriot Act, détiennent beaucoup plus d'informations sur votre vie privée que les services d'enquête européens... La LPM a aussi introduit la possibilité d'avoir les données de connexion en temps réel, avec éventuellement une mise à jour par le réseau de ces données, données précisées dans la LPM. La sollicitation des réseaux pour la mise à jour est faite par l'opérateur (sous contrôle) et concerne essentiellement

la géolocalisation. Rassurez-vous, nous ne sommes pas dans le monde de Georges Orwell...

*FFT : Fédération Française des Télécoms
**l'article 20 de la LPM votée a longtemps été nommé article 13 dans la discussion parlementaire

• **Que nous apprenait l'interview de Constant Hardy ?**

- Le CCED est un organisme interministériel.
- L'essentiel des activités du CCED se concentre sur les interceptions de communications et la mise à disposition de données, ce qui nécessite de disposer de systèmes performants.
- 500.000 condamnations en correctionnelle en France par an, ce qui donne une idée du nombre d'enquêtes en cours... et ce n'est que le volet judiciaire des écoutes. D'où la nécessité « d'industrialiser » certaines méthodes de réquisition.
- Les équipements d'interception, mis en place au niveau des commutateurs et des cœurs de réseaux sont autorisés, au plan technique, par l'ANSSI.
- Le Retex des incidents touchant les opérateurs fait apparaitre 2 causes majeures : en premier lieu, une erreur humaine de manipulation ; en deuxième, un défaut de conception du matériel (exemple, un enchaînement de commandes incompatibles provoquant une panne de serveur).
- Aujourd'hui, les moteurs de recherche et la NSA, grâce au Patriot Act, détiennent beaucoup plus d'informations sur votre vie privée que les services d'enquête européens... A méditer par la CNIL ?

Biographie – Constant Hardy a débuté sa carrière chez France Télécom où il a d'abord été responsable des infrastructures de distribution et du raccordement des abonnés pour la région Auvergne avant d'exercer différents postes de direction générale à l'échelon régional puis central. En 1991, il devient directeur technique de la région Ile de France du groupe La Poste, puis directeur de la recherche-développement du groupe. De 1998 à 2006, il sera chargé du projet VIGIK et responsable de la normalisation. Depuis 2006, il est Commissaire aux communications électroniques de défense rattaché au Ministère des Finances. Constant Hardy est ingénieur des Mines, diplômé de l'Ecole Normale Supérieure (rue d'Ulm), de l'Ecole Nationale Supérieure des Télécommunications, Agrégé de physique et de chimie. Il a été en 1991 auditeur de la session Ile de France de l'Institut des Hautes Etudes de la Défense Nationale.

La sécurité informatique pour l'usager de base.
Un expert de terrain, dix fondamentaux

*Jean LUCAT**

La tenue des dossiers d'archives et de données des entreprises, et leur circulation, est une activité cruciale et la gestion des risques associés à ces documents et à leurs supports, fort complexe. Un rapport de la délégation parlementaire au renseignement publié en avril 2014 place la cybercriminalité au second rang des menaces contre les intérêts français et relève que les moyens déployés par les adversaires se diversifient et s'appuient toujours plus sur les technologies numériques.

D'autre part ACONIT produit depuis 2014 une veille médiatique mensuelle sur les menaces criminelles visant les entreprises et collectivités locales. Parmi ces menaces, la cybercriminalité occupe une place de choix. Deux années et plus de recul sur ce phénomène, nous permettent ici de dégager des considérations stratégiques et tactiques.

Avant d'exposer les divers aspects dangereux ou menaçants de cette cybercriminalité, précisons que notre étude, en forme de *diagnostic*, résulte d'une pratique de la cyber-sécurité par un praticien des risques de l'entreprise et n'est pas un recueil de recettes de sécurité informatique, car il existe déjà maintes de recommandations de ce genre.

1. Changement de nature et nouvelles tendances

La cyber-sécurité est passée du stade de simple pratique informatique à une priorité majeure des dirigeants d'entreprise. Les entreprises occidentales liées à l'énergie sont souvent visées par des cyber-attaques restant parfois indétectables pendant des mois.

Les deux-tiers des entreprises en sont informées par une source externe. La sensibilisation à la sécurité informatique a encore à gagner en maturité, surtout pour les PME, sachant que celles-ci sont les plus visées. Les spécialistes craignent des attentats déclenchés à distance, qui auraient des impacts environnementaux lourds, tels que pollution de l'eau, déraillement d'un train.

Même si l'on prend soi-même les précautions nécessaires, on n'est pas à l'abri de voir ses données capturées lorsqu'elles sont confiées à des entreprises dont nous sommes les clients, tels des hôtels par exemple : les groupes Hilton ou Hyatt ont ainsi été attaqués et un *malware* découvert dans les systèmes de paiement. Début 2015, un vice-président de Gemalto a indiqué que nous assistions à un tournant dans la tactique des cybercriminels, le vol d'identité à long terme se substituant toujours plus à l'immédiateté qui caractérise le vol des numéros de cartes de crédit. Il soulignait que le vol d'identité peut entraîner l'ouverture de nouveaux comptes de crédit frauduleux et la création de fausses identités à des fins criminelles.

Le cabinet d'audit PWC a interrogé les entreprises françaises, composées à 99,8 % de TPE-PME sur leur rapport à l'assurance cyber. Il est surprenant de constater que 5 % du panel est équipé et que les principaux freins à la souscription demeurent le sentiment de ne pas avoir besoin de protection, l'absence d'information et le manque de clarté des offres. A n'en pas douter, il y a un gros travail à engager dans ce domaine. Début 2016, une note des services français révélait qu'un groupe d'informaticiens aurait été constitué afin d'aider les djihadistes à communiquer le plus discrètement possible. Ces experts, titulaires de diplômes universitaires, fonctionneraient comme une « cellule d'assistance informatique ».

Le jour où les terroristes pourront s'attaquer à nos réseaux, et donc à tous les objets connectés, 18 milliards aujourd'hui, sans doute 50 milliards en 2020, les dégâts pourraient être très importants, beaucoup plus meurtriers que ne peuvent l'être les attentats suicides. Le leader cyber-sécurité de KPMG a signalé en mars 2016, qu'à l'origine, les cybercriminels voulaient essentiellement nuire aux entreprises qu'ils attaquaient, mais depuis quatre ou cinq ans, la motivation est différente. On voit l'infiltration du crime organisé dans des groupes de hackers et le but est principalement de faire des gains financiers.

Selon l'ANSSI, on voit entrer toujours plus d'attaquants dans les réseaux informatiques. Ils ne viennent pas voler des informations, pour infiltrer les entreprises et rester à l'état dormant. Ils prennent pied progressivement et on les retrouve très profond au sein des réseaux d'entreprises. Il semblerait qu'il devienne plus facile d'infiltrer et de faire le mort que d'agir rapidement pour voler des données. L'ANSSI observe aussi que les terroristes ont les moyens financiers, mais pas les compétences nécessaires pour perpétrer des atten-

tats numériques, mais pourraient faire appel, moyennant rétribution à des cyber-mercenaires.

Au Royaume Uni, l'Agence nationale contre le crime estime que le niveau d'équipement des groupes criminels dépasse les capacités de ceux qui les combattent. Une lutte inégale où dominent quelques centaines de criminels, notamment des bandes internationales. De plus, la coopération serait le maillon faible avec les géants de l'informatique tels que Microsoft, Google ou Facebook, où les enquêtes en cybercriminalité sont encore souvent confrontées au refus de partage de données.

2. La menace intérieure

Entreprise britannique experte ès-analyse stratégique des réseaux et télécommunication, Ovum a conduit une enquête « Insider threat » dédiée aux menaces internes. Elle révèle que les menaces intérieures ne proviennent plus des seuls utilisateurs habituels ayant des droit d'accès légitimes, qui en abuseraient pour voler des données et en retirer un gain personnel. Les administrateurs des systèmes et des réseaux ont bien sûr un accès à toutes les données sensibles et représentent désormais un souci supplémentaire.

Quand on réalise des audits de sûreté dans les entreprises et qu'on en arrive à la cyber criminalité, la réaction du chef d'entreprise est toujours la même. Il s'appuie sur son DSI. Le mettre en cause est toujours délicat. Les responsables d'entreprises peinent souvent à comprendre que le danger peut provenir du sein même de l'équipe chargée de la protection. Il est souvent délicat d'aborder le fait que « La confiance n'exclut pas le contrôle ».

Un rapport de CyberArk détaille les tendances récentes des cyber-attaques. Il en ressort que les comptes à privilèges (ceux des administrateurs) sont les clés de voute de l'infiltration des hackers dans les systèmes, « presque chaque attaque avancée implique une exploitation de comptes à hauts pouvoirs... Ces comptes permettent aux assaillants d'accéder à des réseaux et bases de données sécurisées, d'effacer toute trace d'infraction, d'éviter toute détection et de créer des portes de sorties rendant quasi-impossible leur éviction des réseaux ».

Cette menace est sous-estimée : « les entreprises sous estiment grandement le nombre de comptes à hauts pouvoirs qu'elles possèdent et ignorent les systèmes qui les hébergent ». Selon un rapport d'IBM Security, 60 % des attaques informatiques ayant visé des entreprises en 2015 ont été initiées par quelqu'un de confiance, mais il ne s'agit pas toujours d'inadvertance. Selon ce rapport, 15,5 % des cyber-attaques d'origine interne en 2015 étaient involontaires, les autres sont intentionnelles.

3. L'externalisation des archives

L'usage des nouvelles technologies d'archivage (Cloud et Big Data) rendent les processus de sécurisation toujours plus complexes et les entreprises dans ce domaine perdent la visibilité sur les mesures de sécurité. Selon Jean Paul Pinte, docteur en information scientifique et technique, les données confiées à un site distant, sont difficiles à sécuriser. Il préconise de les conserver sur un disque dur externe, à son entreprise ou à domicile. De fait, lorsque le fournisseur indique que les données sont sauvegardées dans le Cloud, nul ne sait indiquer à quel endroit physique de la planète les données seront accessibles, quelles seront les procédures de sécurité adoptées et qui y aura accès. Il faudrait alors localiser l'hébergeur et vérifier les législations qui sont appliquées, car ces dernières diffèrent selon que la structure d'hébergement est située dans un pays ou dans un autre.

4. Les *ransomwares* et la fraude au président

Le ransomware consiste à bloquer les logiciels d'un système informatique tant que l'utilisateur n'a pas versé une rançon. Ces pratiques impliquent d'abord le « social engineering » et concerne des demandes d'informations venant d'étrangers à l'entreprise, sous diverses forme, appel téléphonique ou envoi de mail. Par ces demandes, des personnes, animées d'intentions malveillantes à l'encontre de l'entreprise, cherchent à contacter des salariés pour récupérer, sous divers prétextes, des informations sur les dirigeants, le personnel, les projets et l'activité de l'entreprise. Cela, dans le but d'utiliser les informations recueillies pour nuire à l'entreprise.

Rappel : La « fraude au président » consiste à se faire passer pour le dirigeant de l'entreprise ou quelqu'un habilité à parler en son nom, pour demander aux services comptables de l'entreprise des informations permettant de réaliser des virements sur des comptes étrangers. Sur ce type particulier de fraude, le chef de l'office central pour la répression de la grande délinquance financière indiquait avoir connu, en pareil cas, des suicides et tentatives. L'escroc invente toujours un péril imminent et celui qui engage le paiement pense le faire pour une bonne cause : le préjudice humain est donc très important.

Chaque année, en France, environ 400 millions d'euros s'évanouissent dans la nature par la seule technique de la fraude au président. Interrogeons-nous cependant : n'y a-t-il pas dans certains cas, quelque complicité ? Car les victimes manifestent parfois une grande naïveté, voire plus. Remarquons ainsi que les sommes détournées par ce biais échappent à l'impôt. Il serait étonnant que nul n'y ait pensé.

5. L'acquisition des données nécessaires pour les cybercriminels

Ces techniques utilisées par les cybercriminels nécessitent d'obtenir au préalable des informations sur l'entreprise qui va être la victime. Le rapport de Symantec précise que les cybercriminels visent d'abord deux professions, les assistants personnels et les spécialistes des relations publiques afin d'accéder aux données des chefs d'entreprise. Une pratique d'entreprise toujours plus populaire est aussi une vulnérabilité. Celle permettant aux employés d'utiliser leurs terminaux mobiles personnels au travail. Selon Jean Lavoir, chef des opérations au centre de recherche informatique de Montréal, mettre des données dans un environnement incontrôlé par l'entreprise est un risque. Les données sont dispersées partout. Un individu décodant les mots de passe personnels d'employés accède aisément à de l'information professionnelle.

Les réseaux sociaux constituent aussi un bon moyen pour les criminels d'obtenir des données. Les faux profils sur Facebook ou Linkedin pullulent. Ils permettent d'approcher les salariés d'une entreprise cible et les faire parler. En face, les salariés n'ont pas toujours conscience d'être approchés, d'autant que ce type d'attaque résulte d'un travail de longue haleine. La menace concerne les TPE-PME qui ne pensent pas intéresser les pirates, comme les grands comptes qui se croient bien protégés. Troel Oerting, directeur du centre européen de lutte contre la cybercriminalité a déclaré fin 2014 qu'elle était l'activité d'une centaine de bons programmeurs, mais que leur nombre augmente inévitablement. Ce «noyau dur» serait à l'origine de la plupart des cyberattaques.

6. La publicité sur les attaques informatiques

On déplore la frilosité des entreprises à parler de leurs failles, alors qu'il est de l'intérêt des entreprises d'échanger sur le sujet et d'en informer les pouvoirs publics. En effet, en dépit de la complexité des attaques et de la multiplication des pirates, Jérôme Billois, expert en sécurité informatique de Solucom, souligne que les méthodes d'attaque restent les mêmes. Le nombre de victimes augmente alors que le nombre d'attaquants reste au final réduit. Ce constat montre clairement la nécessité de partager les informations relatives à ces attaques, comme les adresses IP ou les noms de domaines utilisés par les attaquants, appelés IOP.

Le Clusif, club de la sécurité de l'information français, a signalé dans un rapport de 2014 l'insuffisance des données concernant les attaques. L'absence d'obligation de déclaration gêne l'appréciation du phénomène et ainsi, l'élaboration de stratégies défensives. Le souci de confidentialité freine à l'efficacité de la lutte contre ce phénomène et les entreprises ont intérêt à rejoindre les structures qui s'installent pour les partages d'informations. Ces pe-

tites entreprises sont souvent silencieuses quand elles se font attaquer par des pirates informatiques. Pour elles, faire appel à une grande société de sécurité informatique n'est pas évident compte tenu des tarifs pratiqués. La mise en place de séries de firewall est une solution couteuse et n'est pas une protection à toute épreuve.

7. Les changements dans les méthodes de protection

Un tel changement a été mis en œuvre par Cisco qui considère que les antivirus actuels laissent passer une majorité des attaques et préconise de sécuriser les réseaux d'entreprises en temps réel pour contrer divers types de menaces. La sécurité connectée est une nouvelle approche qui s'impose et correspond à une réactivité rendue nécessaire par l'étendue et la complexité des cyber-attaques. Cet avis est partagé par Symantec pour qui l'antivirus est mort et qui préconise également de se concentrer sur la détection d'intrusion.

Ainsi, Bouygues Telecom a-t-il créé un nouveau service de sécurité virtuelle pour moyennes et grandes entreprises, offrant aux clients le contrôle de la sécurité des accès internet, la protection contre les intrusions. Les fonctionnalités de sécurité sont mises à jour en continu, par une équipe internationale de chercheurs ; our une meilleure sécurité, les services et données des clients sont hébergés sur les serveurs de Bouygues, en territoire français.

Une faille dans les méthodes de protection tient également au manque d'entretien des logiciels. Selon une étude réalisée par Next Content auprès de dirigeants de PME françaises, 36 % des entreprises interrogées ne mettent pas régulièrement à jours les logiciels installés sur leurs ordinateurs. Cette démarche simple permet pourtant de réduire de beaucoup les risques d'attaques. En effet, 70 % des attaques observées par l'étude, résultent de failles logicielles présentes dans des applications non mises à jour. Non pas les logiciels de sécurité, mais des applications en général, comme Java, Flash, Adobe. Pour 90 % de ces attaques, des mises à jour correctives disponibles auraient pu bloquer l'intrusion.

Kaspersky Lab a aussi dévoilé le fonctionnement des attaques Darkhotel visant à dérober des informations sensibles aux cadres supérieurs lors de leurs voyages d'affaires, surtout via les bornes d'accès Wi-Fi mises à disposition des clients dans les hôtels de luxe. Les pirates exploitent des failles logicielles à travers les réseaux Wi-Fi « privés et sécurisés » de ces établissements de luxe. Une directive européenne va cependant obliger les entreprises à sécuriser leurs infrastructures et systèmes informatiques. Le texte devrait sortir en 2018, avec un futur règlement sur la protection des données personnelles s'adressant à tous les organismes publics et privés.

Deux millions de personnes ont été victimes de « phishing » en 2015, soit 100 fois plus qu'il y a deux ans. Croyant répondre à

sa banque, son opérateur télécom ou aux impôts, les victimes donnent en fait leurs informations confidentielles à des pirates. Or, en cas de doute sur un mail, on peut maintenant le faire vérifier sur le site Phishing-initiative.fr. En 20 minutes, un expert dira s'il s'agit d'une page frauduleuse. Ce site fonctionne 24/24 et 7 jours sur 7 et a permis à 20 000 internautes d'éviter d'être victime de ces attaques.

8. La sécurité des objets connectés

Il s'agit d'une des principales menaces, le nombre d'objets connectés se développant rapidement, objets touchant à tous les aspects de la vie professionnelle et domestique. On prévoit 50 milliards d'objets connectés en 2020. Des spécialistes indiquent qu'il seraient possible de prendre à distance le contrôle de climatiseurs, de chambres froides, de scanners, d'imprimantes, de portes de garage etc. Souvent les mots de passe sont inexistants dans les objets connectés et les utilisateurs doivent songer à les paramétrer. Le rapport du Clusif avait ainsi souligné l'omniprésence du système Scada dans l'informatique industrielle, dont les failles sont perméables à l'intrusion de virus malveillants.

Le logiciel Scada est un système de contrôle et d'acquisition de données, un système de télégestion à grande échelle permettant de traiter en temps réel de multiples mesures et de contrôler à distance des installations techniques. Cette technologie industrielle Scada est notamment présente dans la surveillance des processus industriels, des transport, des produits chimiques, d'approvisionnement en eau ou de production d'énergie.

La fiabilité de ces systèmes devenus omniprésent dans l'industrie est de fait un enjeu majeur. Une étude du cabinet Roland Berger estime qu'en 2018, les véhicules connectés formeront 67 % des ventes mondiales. Un paramètre à intégrer à la sécurisation des systèmes est leur diversité, si bien qu'il n'y a pas d'antivirus universel à venir en pare-feu.

Certaines caméras de surveillance ne se contentent pas de filmer et transférer leurs images à leur propriétaire. L'entreprise américaine de sécurité informatique Sucuri a récemment découvert que 25 000 d'entre elles, disséminées partout dans le monde, pouvaient également mener des attaques informatiques. Ces caméras ont été piratées pour former un réseau capable d'agir de concert. Voici un bon exemple d'attaque via un objet connecté.

9. Les failles dans le système

Une étude du *Cyber Risk Report* mentionne que 44 % des infractions concernent des failles connues depuis 2 à 4 ans. Même si le monde de la cyber-sécurité continue à

évoluer rapidement, il ne faut pas perdre de vue les failles fondamentales. Cette étude montre que les plus gros problèmes liés à des risques de sécurité sont connus depuis des années, voire des décennies. Impossible de progresser conclut l'étude, si on ne résout pas les failles primaires qui restent une plaie pour les systèmes.

Les monnaies alternatives représentent aussi un danger et une vulnérabilité. Ces plates-formes permettent de déposer des montants en cash, en se passant des vérifications qu'exigeraient les banques, et les transformer en monnaies virtuelles, transférables à l'autre bout du monde. Ces monnaies constituent une facilité au blanchiment. En attendant qu'existent les moyens techniques et de surveillance de ces monnaies, et de leurs échanges, si tant est que cela soit possible, les entreprises ont tout intérêt à les utiliser avec grande prudence. Le risque de voir disparaître son portefeuille de Bitcoins, ou ceux de ses clients est aujourd'hui majeur : mieux vaut s'abstenir de s'aventurer dans ce domaine.

10. Le facteur humain, source de vulnérabilité

Dans toute procédure de sécurité et de protection, le facteur humain est le véritable maillon faible. C'est ainsi sur lui qu'il faut concentrer son attention quand on réfléchit à la fuite de données. L'être humain peut réaliser des actes qui entraînent involontairement des fuites d'informations du fait de comportements tels que la distraction et l'étourderie, la maladresse et l'inconscience, la fatigue et l'épuisement.

A cela s'ajoutent les risques liés au non-respect du devoir de discrétion, ou des mauvaises pratiques, telles que les discussions et réunions dans des lieux publics (restaurants, transports en commun) ou des habitudes à risques : lecture de documents dans un lieu public, communication d'un mot de passe à un collègue ou a un prestataire extérieur pour qu'il effectue une opération à partir du poste, branchement d'une clé USB dont la source n'est pas connue. Tout cela peut dévoiler des informations importantes ; des logiciels malveillants peuvent être installés.

Des collaborateurs révèlent des informations volontairement, mais en ignorant la véritable utilisation finale, car victimes d'ingénierie sociale. 67% des entreprises françaises reconnaissent avoir subi un détournement de données et 92% de ces détournements ne sont pas révélés. L'ingénierie sociale est une forme d'acquisition « déloyale » de l'information par usage de techniques d'élicitation pour obtenir d'autrui un bien, des services ou de l'information importante.

Issue de la psychologie sociale et cognitive, l(identification et exploitation des failles humaines) l'élicitation est le fait de prédateurs professionnels qui recueillent des informations en faisant parler une personne

sur ses connaissances et son savoir. Se prémunir contre l'ingénierie sociale, c'est d'abord connaître son fonctionnement. Il faut donc former son personnel à la « discrétion professionnelle », dans ou hors des locaux de l'entreprise, sur les informations données à des tiers non identifiés et habilités.

La « discrétion professionnelle » doit devenir un réflexe, surtout pour les petites entreprises. La protection contre la cyber criminalité est souvent affaire de bon sens et de mesures peu couteuses, comme quitter chaque soir son bureau en ayant fait sa sauvegarde, et de l'amener à son domicile. Internet est un réseau peu sûr. L'architecture en a été conçue sans intégrer la sécurité et cette dernière se fait maintenant au coup par coup, par réaction à chaque attaque pour protéger tant bien que mal les réseaux.

Cependant, de nos jours et dans tous les pays industrialisés, tous les processus en dépendent et ils sont largement exposés. Ces craintes sont cependant pondérées par ceux qui assurent que les progrès continu de la sécurité informatique permettront de ne pas voir une attaque comme celle du virus Stuxnet, utilisé pour attaquer les capacités nucléaires de l'Iran, se reproduire avant une dizaine d'années.

Une autre source de vulnérabilité consiste dans le fait que huit infections sur dix (selon Kaspersky Lab France) sont provoquées par l'envoi de mail, d'usage parce que l'utilisateur a ouvert une pièce jointe contenant un logiciel malveillant. Les employés ne sont pas assez formés aux risques du numérique. Le risque majeur restant la naïveté de l'utilisateur, la paresse humaine, le manque de volonté et une certaine mollesse. Voici pourquoi il faut insister sur les actions de prévention et de régulation.

Notamment, la gestion des mots de passe n'est pas réalisée avec tout le soin requis. Trop de mot de passe permettent d'entrer dans trop d'applications et il y a un manque de rigueur dans la plupart des entreprises à ce sujet. Les mesures les plus efficaces sont souvent les mesures de bon sens. Il ne faut pas hésiter à revoir toutes les procédures, ce qui est par exemple le meilleur moyen pour éviter la fraude au président.

Lors d'un colloque à San Francisco, Tim Berners Lee (père fondateur du Web) a déclaré que le Web devait aujourd'hui passer à une nouvelle phase et placer les problématiques de centralisation et de protection des données personnelles au cœur de ses préoccupations. En fait, toute l'architecture du Web serait à reconsidérer.

Note

* Jean Lucat, a servi vingt ans dans les services de l'Etat (contre-espionnage et anti-terrorisme) ; il est le fondateur d'Aconit, société de conseil en intelligence économique et gestion de risques d'entreprise, créée voici une décennie.

La NSA, « mauvais génie » du cybermonde ?

Claude DELESSE [i]

En 2014 Sony Pictures subit un raid informatique de grande envergure, attribué à la Corée du Nord. Deux ans plus tard des chercheurs de Symantec et aussi ceux de BAE Systems établissent un point commun avec les cyber casses réalisées contre plusieurs banques asiatiques dont la banque centrale bangladaise à qui 81 millions de dollars ont été dérobés. Un établissement philippin et un vietnamien auraient été également touchés. En fait, une douzaine de banques dont une européenne seraient concernées par ce type de piratage. Derrière « Lazarus », le groupe de pirates informatique qui serait à l'origine de toutes ces intrusions digitales, se cacherait en effet la Corée du Nord. Ainsi, un État se procurerait des fonds en exploitant les failles des réseaux informatiques des institutions bancaires cibles. Modus operandi bien rodé. Les pirates s'y introduisent et espionnent les employés afin de récupérer les identifiants et les mots de passe leur permettant de se connecter au réseau Swift (*Society for Worlwide Interbank financial Telecommunication*) où ils effectuent les ordres de transfert de fonds[ii].

Dimension à l'évolution démentielle, l'infosphère s'enchevêtre avec les économies réelles et informelles décuplant ainsi les capacités des hackers à exercer leur malignité, en tant que mercenaires ou à titre personnel. Internet est une aubaine pour des prédateurs à l'imagination débordante et à l'aise dans les espaces cyber, jungles en partie inextricables. D'autres acteurs maléfiques, terroristes en tout genre, manipulent, recrutent, menacent et donnent des ordres. Or, les maillages d'intérêts entre le crime organisé, des groupuscules terroristes, des individus ou des entités corrompus créent une hybridation des menaces. Confrontés à ces mutations préoccupantes les services de renseignement ont tenté de se transformer dès la fin des années quatre-vingts. Mais, face à des réalités fluides, opaques et indescriptibles, ils recherchent

aveuglément des solutions en abusant de technologies. Ils sont en cela soutenus par des autorités politiques qui font - semble-t-il - plus confiance au à des algorithmes censés tout détecter qu'au renseignement humain. James Clapper, directeur du renseignement national DNI, considère le renseignement d'origine électromagnétique comme essentiel et complémentaire pour détecter les tendances et estimer la réalité des menaces.

Mais, la fusillade meurtrière dans une discothèque d'Orlando le 13 juin 2016 a prouvé, une fois encore, l'inefficacité d'une surveillance massive et indiscriminée des citoyens du monde entier. Entravées par le caractère exponentiel des données ainsi que par la montée des phénomènes criminels et des actes terroristes, les investigations humaines peinent à détecter de manière proactive la dangerosité d'individus qui devraient faire l'objet d'une observation permanente et étroite. L'instinct policier, réactif, tendrait plus à chercher des données signifiantes a posteriori afin de prouver la culpabilité des auteurs d'attentats.

Le renseignement électromagnétique cohabiter avec le hasard, l'impensable, l'imprévisible. NSA, Ô NSA à quoi sers-tu ?[iii] Réputée être l'agence de renseignement la plus puissance au monde, l'agence nationale de sécurité américaine regorge pourtant de ressources financières, technologiques et d'informations. Relevant du département de la défense, cette espionne insatiable, véritable transnationale du renseignement, a pour rôles d'intercepter et de collecter le renseignement des signaux (SigInt) – y compris par des moyens clandestins, et de déchiffrer les transmissions étrangères d'origine électromagnétiques afin de soutenir les missions des autorités gouvernementales US et leurs partenaires. Elle a pour seconde mission de protéger l'information sensible et les systèmes de sécurité nationale vitaux (Information Assurance). Son directeur Michael Rogers qui commande aussi l'US Cyber Command est à la tête d'un empire chargé de comprendre les menaces et d'être à la pointe de la détection, d'apporter le renseignement utile à temps à des officiels ou aux hauts gradés, de soutenir les opérations militaires et de protéger les soldats, de sécuriser les réseaux et les données, de développer la cyber sécurité, de protéger et déployer les armes stratégiques digitales, de dominer la recherche et les avancées technologiques. Les citoyens seraient-ils oublieux de tout cela ? Et, qu'elle fut créée en 1952 pour espionner, en temps de paix, le monde communiste mais que la paix est devenue depuis illusoire et que les ennemis se propagent comme la vermine. Sidérés par les révélations d'Edward Snowden en 2013, ils sembleraient pour la plupart focaliser leur acrimonie sur l'outrance de la surveillance. Certes, le sentiment d'une intimité violée est fondé. Défendre les droits privés ainsi que les libertés civiles et d'expression au combien bafouées est une action salutaire pour le maintien des démocraties. Mais à trop dénoncer ces dérives ne s'enferme t-on pas dans l'incompréhension des ques-

tions de renseignement, qui mériteraient une attention plus globale. Ne réduit-on pas le modèle de risque ? N'est-il pas davantage opportun d'exiger plus d'efficience de la part de la NSA et de ses partenaires ? Ne se trompe-on pas dans l'identification de l'ennemi ?

Face à l'évolution et l'hybridation des menaces, la NSA, dans l'obligation de répondre aux attentes du gouvernement américain, déploie des programmes démentiels au premier rang desquels figure Échelon (I). Accusée d'être attentatoire aux libertés civiles, elle s'efforce de maintenir l'ombre sur des guerres plus secrètes (II), porteuses de risques encore plus insidieux et face auxquels il serait malgré tout possible d'envisager des comportements adéquats (III).

Légitime surveillance, totale et indiscriminée !

Les documents internes subtilisés à la NSA par Edward Snowden ont apporté la preuve qu'elle espionne, sous prétexte de lutter contre le terrorisme et la criminalité organisée, à des fins non seulement politique, diplomatique et militaire mais aussi socio-économique. Les cibles prioritaires sont fixées en fonction des intérêts et des stratégies nationales. C'est ainsi que les citoyens du monde entier y compris les Américains sont considérés comme des ennemis en puissance. Toutefois, bien que les moyens de collecte et d'interception soient démesurés, les analystes ne parviennent pas à assurer un traitement exhaustif et efficace des données ratissées par de puissants algorithmes.

L'Hybridation des menaces

Drame humain, les attentats du 11 septembre 2001 ont atteint la fierté américaine touchée au cœur même de son territoire. Mais ce fut une aubaine pour les services de renseignement, appelés par le gouvernement George W. Bush à développer leurs activités[iv]. Des moyens colossaux leur furent attribués y compris pour combattre le crime organisé transnational dont la complexité s'intensifie depuis une quinzaine d'années. Le FBI considère que tous les groupes identifiés (russes, africains - Nigeria en particulier -, chinois, japonais, d'Europe de l'Est - plus précisément Hongrois et Roumains) sont présents aux États-Unis ou ciblent à distance les américains grâce à Internet et d'autres technologies. Les réseaux du crime organisé (*Organized Crime Groups*, OCGs) dont les profits sont estimés à mille milliards de dollars par an tendent à coopérer entre eux en oubliant leurs rivalités. Ils manipulent et ils contrôlent les marchés financiers, les syndicats de travailleurs, les industries du bâtiment et des déchets. Trafiquants de drogue, ils élèvent le niveau de violence dans les cités, ils corrompent les personnalités et ils baignent dans les pots de vin, extorquent, intimident et assassinent. Ils infiltrent le monde des affaires, de la prostitution, se livrent aux tra-

fics d'humains, à la fraude à grande échelle, à des arnaques financières et blanchissent des sommes considérables. Or, les services de renseignement, les auditions du congrès américain et les médias pointent sur une convergence internationale des organisations criminelles et terroristes, qui profitent réciproquement de leurs expertises et de leurs capacités[v].

La NSA comme les autres agences reçoit des instructions gouvernementales. Au rang des priorités il lui faut renforcer les collaborations avec les autorités judiciaires et les forces de police, améliorer les protocoles pour assurer la diffusion des données aux agences chargées de veiller afin de contrecarrer les activités TOC aux frontières et en certains points sensibles des chaînes logistiques. Elle est également supposée collaborer avec les centres de renseignement spécialisés dont la division des opérations spéciales (*Special Operations Division*, SOD) au sein de la DEA.[vi] Selon le Conseil de sécurité nationale (NSC) les efforts doivent porter sur tous les types de renseignement : renseignement d'origine électromagnétique (SigInt), renseignement d'origine humaine (Humint) et renseignement à partir des sources ouvertes (OSInt)[vii]. Redéfinies, les priorités focalisent sur les menaces inhérentes à la criminalité organisée transnationale (TOC) qui pourrait faciliter des actes terroristes perpétrés au moyen d'armes de destruction massive. Forte est aussi l'incitation à exploiter la littérature grise ouverte, les organes de presse étrangers qui couvrent les questions de criminalité, et à explorer les réseaux sociaux afin de dresser des profils d'individus d'entreprises et d'institutions liées au crime organisé.

Le National intelligence Priority Framework (NIPF) définit pour la communauté du renseignement les priorités fixées par la Maison Blanche. Cette matrice croisant un État ou un acteur non étatique avec un thème cible est établie deux fois par an dans le cadre du *SigInt Requirements Process* (NSRP). Elle hiérarchise les priorités de 1 à 5. L'Agence internationale de l'énergie atomique, le contrôle des armes ainsi que l'émergence des nouvelles technologies en Chine, les capacités militaires et les velléités de leadership chinoises de même que l'instabilité politique égyptienne et les questions militaires figuraient au top niveau des besoins de renseignement (1) dans celle d'avril 2013. Les priorités 1 et 2 sont réservées au Président et à la Maison Blanche, la 3 a pour destinataires le cabinet des ministres, les chefs d'état-major, le Pentagone. Les renseignements sont collectés en majorité à partir de ressources clandestines. Les sources ouvertes sont considérées comme en principe suffisantes pour les catégories 4 et 5 qui répondent globalement à des besoins d'analyses politiques.[viii] Par exemple, le trafic de drogue en particulier en République dominicaine, en Equateur et au Salvador, le crime organisé en République dominicaine, en France, en Géorgie (5) et au Salvador (4).

Les cinq niveaux du NIPF sont transformés par le Sig Com (SigInt Committee) en neuf degrés de priorités établies par rapport à l'importance de la contribution du renseignement électromagnétique. Michael Hayden a apporté des changements significatifs en prenant la peine, à son arrivée en 2009, de lister pour l'administration Obama et la CIA les menaces qu'il jugeait au plus haut point préoccupantes: Al-Qaïda, la guerre contre le trafic de drogue au Mexique, le programme d'armes de destruction massive en Irak, les divergences de vues entre l'Europe et les États-Unis sur le problème du terrorisme, les questions pétrolières au Venezuela et en Iran, la situation au Pakistan, l'Afghanistan et la traque de Ben Laden, la Corée du Nord et son arsenal nucléaire, la République populaire de Chine, le Proche-Orient. Mais paradoxalement, il s'est montré frileux et peu perspicace dans les orientations et les directives de travail face à la montée du terrorisme Al- Qaïda !

La conception des besoins stratégiques de renseignement demeure une affaire complexe mais la NSA semble finalement déployer à sa guise ses « grandes oreilles ». Ses ressources sont multiples à commencer par le système Échelon.

Échelon, l'essor d'un réseau tentaculaire

Conçu durant la guerre froide et outil central de surveillance dans le cadre de la lutte contre le communisme, le système Échelon s'est modernisé et continue à espionner au nom de la lutte contre le terrorisme, contre le crime organisé et la corruption. Il est perçu comme l'emblème d'une surveillance planétaire des télécommunications. Echelon est en effet le nom de code du programme P415 qui a été conçu en collaboration avec Lockheed Space and Missile au début des années 80. Il correspond au système d'interception des satellites de télécommunications commerciaux, système que la NSA domine et qu'elle partage avec les quatre partenaires du traité UKUSA de 1947 : le *Government Communication Headquarter* (GCHQ) britannique, le Centre de la Sécurité des télécommunications Canada (*CSTC*), l'actuel *Australian Signals Directorate* (ASD, ex DSD) et le *Government Communications Security Bureau* néo-zélandais. Cette alliance des *Five Eyes* (FVES) est un club orchestré par les Américains et où chaque membre bénéficie d'un statut plus ou moins privilégié.

Le programme Fornsat dépend de la division Global Access Operations (GAO) de la NSA[ix]. Il correspond à l'interception des signaux émanant des satellites de communication étrangers. En 2003 un plan de modernisation prévoit de renforcer sa structure afin d'intercepter les données numériques[x]. L'ancien système jugé insuffisant reposait sur plus d'une douzaine de stations gérées par les américains ou par les partenaires de second rang et avait été conçu pour intercepter les voix. Pendant « 30 ans il a fourni des informations sur les trafics, le crime international, les armes de destruction massive, la prolifération, le

contrôle des armes, la finance internationale et le commerce. Il a espionné des communications diplomatiques, des réseaux commerciaux privés, des réservations d'avions et des données de facturation»[xi]. En 2002, le département d'État a demandé à la NSA des renseignements sur un gangster russe, « Mr Kumarin », supposé leader du syndicat du crime Tambov. Il voulait connaître les liens entre les syndicats de St Petersbourg et Poutine. Celui-ci avait été député maire de St Petersbourg au milieu des années 90. Ciblage difficile car les analystes de la direction des signaux n'avaient ni numéro de téléphone ni enregistrement de voix. En collaborant avec leurs collègues du groupe de recherche de mathématiques et l'office du crime et des narcotiques (Office of Crime and Narcotics, OCN) ils réussirent à cartographier des chaînes de contact et à repérer le numéro de téléphone de Kumarin rendant ainsi possible la collecte d'informations sur son organisation et ses activités.[xii] Pendant des années, le système Fornsat a fourni 25 % des informations utiles au renseignement élaboré. Le plan visait également à renforcer les moyens accordés aux partenaires, les stations ne suffisant pas à exploiter la multitude de signaux interceptés par les satellites mobiles (Thuraya, ACeS, Inmarsat et d'autres)[xiii].

Dénoncé à maintes reprises, en particulier dans les pays partenaires et en Europe, et accusé depuis des années d'espionner les citoyens du monde entier, le système Échelon (alliance des Five Eyes a évolué avec la transformation de la menace. Dans son livre « Inside Pine Gap »[xiv], David Rosenberg, analyste électronicien crédité de la plus haute habilitation américaine ayant opéré à la base de Pine Gap de 1990 à 2008, évoque par exemple la recherche des armements irakiens, la surveillance des rebelles en Somali, l'interception des communications des leaders serbes pendant le conflit du Kosovo en 1998, la surveillance des installations nucléaires en Corée du Nord et la traque menée contre Ben Laden. En 2003, Mike Rogers, Président de la Commission renseignement de la Chambre des représentants rappelait qu'Echelon est quelque chose de salutaire que les français devraient approuver : « Il protège la France, il protège l'Amérique, il protège les alliés européens ». Ignorait-il que François Hollande, Angela Merkel, de nombreuses personnalités politiques et des institutions européennes étaient la cible des grandes oreilles US ![xv]

Échelon n'est qu'un programme parmi tant d'autres dont certains ont été médiatisés par Edward Snowden et dont probablement beaucoup fonctionnent dans la plus grande clandestinité. Un ancien officiel de la NSA a avoué en 2012 que la raison pour laquelle tout ce truc était si secret est que cela flanquerait la frousse à beaucoup de gens. Russell Tice, ancien analyste, avait lui aussi déclaré que ce qui avait lieu dépassait largement et globalement tout ce que personne n'avait jamais suspecté ou imaginé.

L'explosion de programmes démesurés

Le 11 septembre 2001 a été saisi comme une aubaine par Michael Hayden directeur de la NSA qui a imposé sa vision d'une surveillance de masse en renforçant considérablement la sous-traitance. Un cercle puissant d'industriels, très proches du pouvoir et du renseignement se mit à bénéficier de l'adoption d'une politique de collecte massive indiscriminée et participa à la mise en place de programmes démentiels, lucratifs pour eux. Son successeur le général Keith Alexander joua de son influence pour obtenir, au nom de la sécurité nationale, les ressources et le pouvoir juridique lui permettant de soutenir des programmes démentiels de collecte généralisée et des projets avancés d'intelligence artificielle. Il imposa sa philosophie de collecte, aussi appelée « *phishing expédition* », consistant à siphonner massivement les données puis à rechercher ensuite dans le tout ce qui peut être pertinent ou utile à examiner. Les premières révélations de Snowden en 2013 dénonçaient deux techniques de collecte. Le système Upstream[xvi] permet d'intercepter en amont le trafic Internet ou téléphonique à partir des câbles à fibre optique internationaux et des nœuds des infrastructures d'Internet, cela à l'insu ou avec la complicité d'opérateurs (AT&T, Verizon, etc.). Le système Prism correspond à une collecte directe des métadonnées sur les serveurs des opérateurs Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple en vertu de la section 215 du Patriot Act expirée en juin 2015 et conformément au FISA Amendements Act (FISAA) de 2008. La loi US Freedom Act de 2015 substitutive s'avère plus contraignante pour la NSA. Les métadonnées sont stockées chez les opérateurs. La demande de consultation doit se faire pour une cible précise et nécessite une autorisation de la cour FISA. Elle n'améliore cependant que la protection des citoyens américains ! Muscular, complémentaire de PRISM, permettrait l'interception des données entre les Datacenter de Google et de Yahoo! qui sont répartis à travers les continents. Google aurait renforcé le chiffrement.

Le public découvre depuis 2013 de nombreux programmes aux noms surprenants qui captent les messages, les documents numériques, les données de navigation ou géolocalisation, les voix, les photos[xvii], les métadonnées. XKeyScore, ensemble d'interfaces et de bases de données et métadonnées permet une analyse en grande partie automatisée. Les éléments d'informations jugés intéressants sont stockés dans des bases dédiées[xviii]. Depuis 2009, le service SSO de la NSA a mis en place un système de surveillance vocale du nom de Mystic[xix], ensemble de programmes qui collecte 100% des métadonnées et des messages des téléphones cellulaires utilisés par les résidents et les touristes de certains pays (Bahamas, Mexique, Philippines, Kenya... Retro remonte les écoutes dans le temps, extrait et stocke des morceaux d'enregistrement de voix qui seront traités ultérieurement. Certains programmes ont des fonctions très spécifiques. Par exemple, Skynet analyse

les métadonnées d'appels téléphoniques et Gilgamesh géolocalise les cartes SIM grâce à des drones Predator[xx]. Les programmes Smurfs (les Schtroumpfs) pénètrent dans les appareils Androïd et iphone, espionnent, géo localisent, activent le micro ou manipulent la batterie, etc., etc.

Outre des méthodes de surveillance à large spectre, la NSA procède en fait à l'exploitation de réseau Internet (*Computer Network exploitation*, CNE) par piratage. Elle consacrerait des centaines de millions de dollars par an pour introduire des failles dans les systèmes de cryptage commerciaux, dans les réseaux informatiques ou dans les équipements commercialisés par Microsoft, RSA, Cisco et d'autres sociétés d'informatique. Elle s'assure ainsi l'accès aux systèmes d'information d'entreprises étrangères peu vigilantes qui se laissent piéger par leurs choix d'équipement et de solutions inconséquents. Elle accède aussi directement aux serveurs et aux routeurs via les administrateurs systèmes (programme Discoroute)[xxi]. L'agence dispose d'une unité spéciale de hackers d'élite, le TAO (*Tailored Access Operations*) qui piratent les routeurs, s'introduisent dans les systèmes, implantent des malwares, commandent à distance des logiciels espions. Ils développent des capacités de déploiement et de management des attaques réseaux (*Computer Network Attacks*, CNA) visant à corrompre, détruire des données ou à mener des dénis de service. L'Executive Order 12333 offre une base légale aux activités les plus controversées et le Congrès exerce un contrôle limité sur ces activités. S'introduire dans le système IT d'un opérateur et y implanter un malware est un excellent moyen d'extraire une quantité énorme de données. La filiale de Belgacom, BICS, responsable de l'itinérance (*roaming)* de télécommunication dans plusieurs régions du globe a fait les frais d'une telle attaque (Operation Socialist) menée par le GCHQ en collaboration avec la NSA. Des milliers de systèmes informatiques à travers le monde auraient été infectés de la même manière. « *Owning the Net* » (posséder le net) est une préoccupation permanente de la NSA. L'automate intelligent Turbine implante des logiciels espions dans des dizaines de millions d'ordinateurs qu'il commande et contrôle. Opérationnel depuis 2010, il accroît les capacités de déploiement et de management de centaines d'attaques de réseaux visant à corrompre, détruire des données ou à mener des dénis de service. Il procède par imitation de sites tels que Facebook ou par envoi de courriels piégés. La NSA a toute une panoplie d'implants sophistiqués dédiés à diverses applications. Unitedrake prend le contrôle total de l'ordinateur infecté, Captivateaudience piège les micros d'ordinateurs et enregistre les conversations, Gumfish s'occupe des webcams, Foggybottom récupère les historiques de navigation, les logins et mots de passe tandis que Grok détecte les frappes clavier et que Salvagerabbit extrait les données des lecteurs amovibles connectés à un ordinateur infecté[xxii]. Ce ne sont là que quelques uns d'entre-eux. Turmoil correspond à un réseau de « sensors » exploités en particulier

à Misawa au Japon et Menwith Hill en Angleterre. Ces détecteurs (cookies, numéros de série, messages d'erreur renvoyés vers Microsoft, identifiants de machines et périphériques, etc.) capturent automatiquement les données et les envoient aux analystes de la NSA. Turbine et Turmoil font partie de l'architecture Quantum présentée avec toutes ses déclinaisons[xxiii] par le site *The Intercept*[xxiv]. Quantum fut révélé dans le *New York Times* par David E. Sanger et Thom Shanker, en janvier 2014, à deux jours du discours d'Obama sur la réforme des programmes de surveillance américains. Ce programme effectif depuis 2008 permet de s'incruster dans un ordinateur, même s'il est déconnecté d'internet par une technologie de radio fréquences[xxv]. La NSA ne le qualifie pas d'offensif mais considère qu'il fait partie des tactiques pour se défendre contre les cyberattaques. En collaboration avec *l'United States Cyber Command*, les hackers du TAO l'ont utilisé avec succès en s'infiltrant dans l'espace logique des réseaux militaires russes et dans les systèmes utilisés par la police mexicaine, par les cartels de la drogue, par les institutions commerciales de l'Union européenne et parfois par les partenaires de la lutte contre le terrorisme comme l'Arabie saoudite, l'Inde et le Pakistan. Quantum est particulièrement utilisé contre les unités de l'armée chinoise, accusées de lancer régulièrement des attaques sur des cibles militaires ou industrielles américaines, tout particulièrement pour dérober des secrets ou enfreindre la propriété intellectuelle. Les États unis ne se privent pas de protester. Quantum servers correspond semble-t-il à un réseau de serveurs parallèles greffés sur les routeurs situés aux points clés de l'Internet et capables d'inspecter en profondeur les paquets IP. Ce type d'opération a par exemple visé le consortium de seize entreprises qui gère le câble informatique sous-marin SEA-ME-WE-4 traversant l'Europe, une série de pays de la Méditerranée, du Moyen-Orient, et de l'Asie. Il transite en particulier par des pays sensibles comme le Pakistan et l'Egypte. L'opérateur Orange, qui fait partie du consortium et utilise les équipements du câble SMW4, a subi, à son insu, des attaques qui ont nui à son image[xxvi]. Quantum Insert est un programme de redirection. Le TAO, utilise une technique qui consiste à réorienter des individus cibles vers de faux sites et ainsi pénétrer leurs ordinateurs afin d'y installer des chevaux de Troie. Cette technique a été utilisée par le GCHQ pour pirater l'OPEP et la société belge Belgacom.[xxvii] En cas de nécessité, le TAO peut recourir à toute une palette d'outils, que propose l'unité *Advanced or Access Network Technologies* (ANT) dans un catalogue de cinquante pages. Les prix s'étalent de zéro dollar à 250 mille dollars l'unité[xxviii]. L'ANT développe également des applications informatiques pour des tâches spécifiques. Tout peut être piégé, avec ou sans la complicité des fabricants : cartes mères, firmware des disques durs, routeurs, parefeu, etc. Il arrive aussi au TAO d'intercepter des ordinateurs vendus sur Internet et d'insérer un mouchard avant de les laisser partir pour la livraison finale[xxix]. La division TAO s'est également assurée un accès clan-

destin au trafic de données internes de Swift pour pallier l'accord passé avec l'Union européenne n'autorisant pas l'envoi de données en vrac[xxx].

En décembre 2012, un analyste de la NSA aurait déclaré « depuis quelque temps, le piratage des routeurs représentait un bon business pour nous et nos partenaires 5-eyes, mais d'autres nations ont aiguisé leurs compétences et rejoint la scène »[xxxi]. Opportunistes, les hackers de la NSA et de ses quatre partenaires Five Eyes exploitent pour leur propre compte le cyber espionnage mené par d'autres pays[xxxii]. En 2009, la NSA (apparemment l'équipe S31177, nom de code Transgression) retrace une attaque qui vient d'être menée sur le système du ministère de la défense américain. Elle identifie ainsi le centre de commandement en Chine et, dès lors, espionne à sa guise les systèmes de collecte SigInt adverses opérant par exemple à l'encontre des Nations unies. Cette manière de laisser le sale travail à d'autres services de renseignement et de capter leurs résultats a pour nom, *« Fourth Party Collection »*.

La NSA est une espionne insatiable. Son *Remote Operations Center* (ROC, nom de code S321) est responsable d'opérations clandestines. Il a pour slogan « vos données sont nos données, vos équipements sont nos équipements[xxxiii] » Il pirate des réseaux de botnets[xxxiv] lance des opérations à distance au moyen d'outils hyper agressifs. Par exemple, les systèmes Hammerstein et Hammerchant piègent les appels téléphoniques envoyés à travers les réseaux VPN (virtual Private Network) via Skype et autres logiciels Voice Over IP (VoIP). Foxacid ajoute des fonctionnalités après infection d'ordinateurs cibles. Le ROC est plus qu'habile pour effacer les traces de transfert des données volées vers ses machines. Il repère une cible et certains employés dont il pirate les téléphones portables. Il transforme ces derniers en mules involontaires (*unwitting data mules*). Rien n'est laissé au hasard.

La NSA a son propre moteur de recherche ICREACH. Il attaque diverses bases et fournit des milliards de métadonnées (appelants, appelés, émetteurs, destinataires de courriels, heures, dates, lieux). Les informations, partagées avec le FBI, la CIA et d'autres agences, servent à traquer les personnes, cartographier leurs réseaux, prédire leurs comportements, déceler leurs affiliations politiques et religieuses. Puissants mouchards, les algorithmes de la NSA retracent les contacts, les contacts des contacts. Toutefois la boulimie électronique se heurte à des problèmes de mémorisation et de traitement de données. De plus l'évolution des techniques de cryptologie entrave quelque peu ses activités intrusives.

A l'occasion de la sortie à l'automne 2016 du film « Snowden », réalisé par Oliver Stone, le site Intercept a plongé dans ses archives et recensé dans un tableau synthétique les articles consacrés aux programmes intrusifs identifiés par les noms de code[xxxv]. Tout cela est effrayant mais le

futur est encore plus terrifiant. L'Internet des objets (des milliards) est une opportunité pour la NSA qui prévoit d'exploiter le domaine de la santé et les objets biomédicaux connectés comme les pace makers[xxxvi]. Porteur d'espoir ou de confort pour les individus, le progrès technologique pourrait se transformer en cauchemar !

Les informations portées à la connaissance du public sont très majoritairement antérieures à 2013. Il est fort à parier qu'entre-temps, l'agence dont l'innovation est une des trois priorités affichées dans NSA21[xxxvii] a abandonné certains programmes, en a perfectionné d'inconnus et en a développé de nouveaux. Pourtant les attentats terroristes augmentent. Il serait légitime de juger cette surveillance totale contre productive et de se demander à quoi sert-elle réellement ? En fait, l'acquisition d'informations n'est pas la seule raison d'être de la NSA. Tous ces outils dont elle dispose sont supposés lui permettre d'aider les leaders nationaux et militaires, les politiciens et les autorités du monde judiciaire à comprendre qui sont les adversaires, où ils se nichent et quelles sont leurs capacités[xxxviii]. Or, les phénomènes criminels et terroristes, sont devenus tellement complexes et invasifs de nos sociétés que malgré tous ses moyens la NSA ne peut pas compter sur ses seules forces. La Maison Blanche lui a renouvelé sa confiance et elle aspire à mener à bien, dans la plus grande clandestinité, des missions régaliennes renforcées.

Guerres secrètes

Les outils de pointe de la NSA espionnent touts azimuts dans l'expectative de capter des traces de criminalité ou tout simplement d'hostilité tandis que des programmes d'avant garde se transforment en psychologues afin de repérer la propagande djihadiste sur les réseaux sociaux mais aussi de comprendre les techniques d'endoctrinement et les étapes de radicalisation de certaines personnes. Devant désormais composer avec des menaces transplantées sur les territoires domestiques, la NSA et ses partenaires sont engagés dans une course technologique capacitaire permanente sans pour autant cohabiter en toute harmonie. Plus obscures en sont les raisons.

Des collaborations opaques et compliquées

Depuis plus de deux décennies, la NSA noue des accords stratégiques avec le complexe militaro-industriel américain ou avec des firmes spécialisées dans les technologies numériques et électroniques. Les ramifications sont difficiles à déceler mais éclairantes. De nombreuses entreprises travaillant pour le département de la Défense fabriquent des équipements pour elle ou collaborent en matière d'innovation. L'agence sous-traite des activités de renseignement, de nature en partie clandestine, à de petites sociétés privées qui jouent le rôle d'intermédiaires avec les opérateurs télécoms ou les fournisseurs d'accès Internet. Certaines sont liées aux services SigInt is-

raéliens. En matière de *Data Mining* la NSA collabore avec des entreprises technologiquement innovantes qui concurrencent désormais Palantir Technologies, une firme créée avec l'aide d'IN-Q-Tel, société capital-risque de la CIA. Il serait d'ailleurs pertinent de connaître l'étendue des liens que la NSA entretient avec la CIA, dont la nouvelle direction de l'innovation digitale[xxxix] développe des solutions de pointe avec le secteur privé. Il est confirmé qu'In-Q-Tel continue d'investir dans des entreprises dont les technologies sophistiquées permettent de fouiller dans les réseaux sociaux et de surveiller internautes, groupes activistes, mouvements contestataires et terroristes[xl]. Endgame Systems basée à Atlanta vend à la NSA ses services de cartographie de tous les appareils connectés dans le monde avec des précisions sur leurs caractéristiques et leurs vulnérabilités. L'agence fait aussi appel à Vupen, start-up montpelliéraine installée au Luxembourg et à Singapour et qui possède des bureaux proches du quartier général desa cliente ! [xli].La NSA règne en souveraine sur un microcosme d'espions, de géants du complexe militaro-industriel ou de start-up High-tech où très souvent, d'anciens des services de renseignement occupent des postes clés. Des réseaux de connivence sont ainsi bâtis sur des liens personnels et des conjonctions d'intérêts. De plus, une unité spéciale conjointe (Special Collection Service), le SCS associe les compétences clandestines de la CIA et les capacités SigInt de la NSA. Elle dispose de postes d'écoute, les « Eléments spéciaux d'interception » abrités dans les ambassades ou consulats américains, et développe avec des partenaires industriels des techniques d'interception sophistiquées et miniaturisées.

Sur le terrain de la contre prolifération d'armes de destruction massive, une cellule l'agence centrale de renseignement[xlii] Par ailleurs e renseignement SIGINT est fourni aux autres agences de renseignement, les clients. Vers 1989, la NSA aurait commencé à interagir avec les gardes-côtes (USCG)[xliii] dans ses missions de protection intérieure et policières y compris la lutte contre le terrorisme, la contrebande, le trafic de stupéfiants, la surveillance des bâtiments et flux maritimes privés internationaux. Ainsi en 2003, elle aurait aidé l'USCG et le GCHQ à traquer un cargo naviguant au large de la Floride et des côtes vénézuéliennes. Un bâtiment britannique a saisi 3 930 kilos de cocaïne pure dont la vente dans la ville de New York aurait pu rapporté 196,5 millions de dollars.[xliv] La NSA combine les écoutes de numéros à surveiller, les images radars et infrarouge des satellites espions, savamment analysées par des photo - interprètes. Il demeure toutefois difficile d'estimer le rôle précis de l'agence dans la lutte contre le terrorisme et la criminalité[xlv]. Le rapport d'enquête sur les attentats du 11 Septembre 2001 avait évoqué l'insuffisance de collaboration entre la NSA, la CIA et le FBI. Quinze ans plus tard, les relations occultes entre les agences de renseignement américaines, la Maison Blanche, le Congrès et les géants de l'Internet paraissent toujours compliquées. Début 2016, Le FBI demande

à Apple de débloquer l'iPhone 5c de Syed Rizwan Farook, l'un des terroristes impliqué dans le massacre de San Bernardino en décembre 2015, en créant un firmware qui désactiverait les mesures de sécurité d'iOS. La firme de Cupertino refuse de concevoir ce type d'outil arguant que les criminels pourraient l'exploiter et que cela nuirait à la sécurité de tous les appareils[xlvi]. Eddy Cue, patron des services Internet d'Apple et fils d'immigrés cubains, se montre de plus très soucieux de libertés civiques et de démocratie. Il estime aussi que le gouvernement qui a perdu, durant les dernières années, « cinq millions d'empreintes digitales, celles de ses propres employés, des centaines de millions de numéros de cartes de crédit, et plus encore » devrait utiliser des téléphones mieux sécurisés pour renforcer la protection des données. Le 16 février, le FBI obtient une injonction d'un tribunal californien obligeant Apple à apporter son aide. Tim Cook, furieux d'être informé par la presse réagit par une lettre ouverte. Soutenue par une grande partie de la Silicon Valley et par des organisations de défense des libertés civiles, il devient le héraut de la vie privée, défenseur du chiffrement car les téléphones sont de dangereux mouchards[xlvii].Tim Cook, favorable au chiffrement ne veut pas faire la loi ni s'y soustraire mais il souhaite forcer le dialogue et que le Congrès légifère sur la question. La première audition prévue le 1 mars sur les questions de chiffrement a été ajournée, car le FBI a entretemps réussi à faire débloquer l'iPhone en recourant soi-disant aux services payants d'une entreprise israélienne Cellebrite ou plutôt en achetant, un peu moins d'un million de dollars, à des hackers professionnels la faille qui lui a permis de contourner la sécurité. Le bureau fédéral aurait décidé de ne pas transmettre l'information sur cette vulnérabilité à Apple ! Deux ans auparavant, Michael Daniel, coordinateur de la cybersécurité auprès de Barack Obama, avait déclaré : « Divulguer une vulnérabilité peut vouloir dire que nous renonçons à la possibilité de collecter des informations cruciales qui pourraient contrecarrer une attaque terroriste, arrêter le vol de la propriété intellectuelle de notre pays, ou même permettre de découvrir des vulnérabilités plus dangereuses qui sont utilisées par les hackers ou d'autres adversaires pour exploiter nos réseaux »[xlviii].

Appuyée par Ashton Carter, secrétaire à la défense dont elle dépend, la NSA privilégie officiellement le renforcement du chiffrement[xlix]. On peut s'interroger sur son rôle dans cette bataille. James Comey aurait prétendu sans plus de précision devant un comité judiciaire de la Chambre que d'autres agences et la NSA avaient été sollicitées pour débloquer le téléphone. Est-elle intervenue en coulisses ? Pourquoi aurait-elle refusé, elle la grande spécialiste ? Peu probable - bien que possible - qu'elle ait tenté sans résultat. Peut-être n'a-t-elle pas voulu aider pour ne pas faire état de ses capacités au risque d'amenuiser la confiance des utilisateurs ou de pousser Apple à renforcer la sécurité. Elle ne tiendrait pas à témoigner dans une affaire criminelle devant la cour. Autre hypothèse, l'aide ne rentre

pas dans le cadre de ses missions et elle n'était pas autorisée à aider. Mais on le sait, la NSA a une large conception de ce qui relève du renseignement étranger et elle procède au renseignement domestique. Aucune loi n'interdirait à la NSA d'apporter une assistance technique. L'Amiral Mike Rogers a déclaré à Yahoo News que la NSA avait récupéré les enregistrements de métadonnées du téléphone de Farook mais pas le contenu. Enfin tout simplement, le FBI ne voulait pas de l'aide de la NSA. En contraignant Apple il veut initier un précédent et garantir les investigations futures[l]. Le FBI est sur un registre de facilitation d'enquête au détriment de la sécurité. Selon Edward Snowden, les allégations du FBI sont une imposture car il aurait été techniquement possible de débloquer le téléphone[li]. Obliger Apple à devenir un bras armé de ses pratiques d'investigation n'a aucun bien fondé juridique et menace les principes fondamentaux du droit privé, de la sécurité et de la transparence qui sous-tendent la conception d'Internet. Ce dangereux précédent pourrait à l'avenir contraindre les firmes à créer, concevoir et remodeler leurs systèmes pour permettre aux forces de l'ordre d'accéder aux données.

Plus sombre histoire encore. La NSA aurait trempé secrètement dans de sales opérations. En octobre 2003, un numéro de la lettre interne de la direction SigInt (SID) proposait une opportunité en termes de vacances d'emploi, une affectation à Guantánamo pour quatre-vingt-dix jours, en tant qu'officier de liaison (NSA LNO) ![lii] Les missions : collaborer avec les interrogateurs (DoD, CIA, FBI) afin d'évaluer et d'exploiter les informations soutirées aux détenus. Mais aussi fournir des informations sensibles collectées par la NSA pour assister les équipes conjointes de la base (Joint Task Force Guantanamo, JTF-GTMO). Un homme en poste, par ailleurs ravi d'avoir pu s'adonner à divers sports ou activités marines, a confirmé qu'il devait fournir du renseignement en vue des interrogatoires, formuler des questions et des stratégies, observer et participer aux séances. Or, certains agents du FBI auraient dénoncé des techniques de torture outrepassant les pratiques du bureau d'investigation. Des analystes de la NSA, spécialisés dans le contre terrorisme auraient participé aux interrogatoires et aux enquêtes qui ont été menées afin de découvrir d'hypothétiques armes de destruction massive possédées par le régime de Saddam Hussein. Ils auraient notamment eu des expériences de renseignement sur le terrain à la prison d'Abu Ghraib[liii]

La survenue d'évènements retentissants tendrait à prouver les difficultés que rencontrent les agences de renseignement pour agir dans la complémentarité et la concertation. Les échanges d'informations pâtissent de barrières de souveraineté, difficiles à estimer, et du souci de protéger les sources et les méthodes. Les forces de police européennes et autres collaborent pour mener des investigations post attentats dans le cadre de l'anti-terrorisme et de la lutte contre la criminalité organisée (trafics financiers, d'armes, etc.). Mais en amont,

les États auraient tendance à ne partager que les données brutes, et encore avec difficultés. Cela relève plus du volontarisme et du consentement que de la règle et de l'automatisme. Seuls quelques initiés sont informés de la nature de la collaboration de la NSA avec différents services nationaux de renseignement. Depuis la guerre froide, les Allemands entretiennent une collaboration étroite avec les Américains qui s'est renforcée après le 11 septembre et dont ils sont particulièrement dépendants. La Chancelière Angela Merkel, préoccupée par la montée des phénomènes extrémistes, souhaitait toutefois que l'Allemagne bénéficie des conditions accordées aux pays de second rang (Five Eyes). L'administration Obama aurait décliné sa demande. Par contre, en mars 2016, une alliance sur le point de se concrétiser entre les services français et britanniques laisse envisager possible le rêve, longtemps caressé par Paris de devenir le sixième membre de ce « club »[liv]. Washington a toujours repoussé une proposition d'accord de coopération bilatérale. En 2010, le français Bernard Bajolet, coordinateur national du renseignement (actuel patron de la DGSE) et Dennis Blair, son homologue américain avaient envisagé un pacte de non - espionnage, sur le modèle du *gentlemen's agreement* entre Washington et Londres mais la Maison Blanche ne voulant pas se priver d'espionner l'Hexagone, avait écarté Dennis Blair de son poste deux mois plus tard[lv]. En tant que directeur national du renseignement celui-ci jugeait avisé de « se servir de l'expérience accumulée dans les zones de guerre… »[lvi]. Il proposait de créer davantage « de centres de renseignement conjoints afin de faire circuler l'information encore plus vite ». Il fallait « faire plus pour accélérer les opérations conduites ensemble contre des ennemis communs »[lvii].

Depuis les attentats de Paris et Bruxelles, la NSA et le GCHQ britannique accumulent une masse considérable de communications électroniques et cherchent à en extraire des messages signifiants échangés par les terroristes[lviii]. Faisant suite aux attentats de Paris et de Saint Denis qui ont fait 130 morts en novembre 2015 et après quatre mois de fouilles infructueuses, les Belges ont demandé à la NSA de surveiller tous les téléphones présents à l'enterrement d'un des kamikazes, Chakib Akrouh, mort lors de l'explosion de sa ceinture piégée au cours de l'assaut mené à Saint Denis le 18 novembre, et enterré en mars 2016. Selon le responsable de la sûreté de l'État belge, la NSA a des capacités inégalées, ce qui a permis de s'emparer de toutes les informations mémorisées par les dits téléphones et de mettre la main sur Abdeslam[lix].

Confrontés au renforcement et à l'hybridation de menaces diffuses, les services de renseignement et de police, doivent pouvoir maintenir une longueur d'avance. L'Union européenne a adopté le 6 avril 2016 une communication conjointe relative à la lutte contre les menaces hybrides (*Joint Communication On Countering Hybrid Threats*) dans le but d'activer une réponse coordonnée au niveau européen[lx]. Aux États-Unis,

James Clapper prônerait lui aussi un renseignement plus intégré[lxi]. Ces initiatives et ces intentions déboucheront-elles sur des résultats efficients en matière de renseignement mais aussi de contre renseignement et de protection des infrastructures sensibles ?

Une cyber combattante hostile à la divulgation de ses secrets

Sur fond de coalitions secrètes, certaines entreprises mues par intérêt national et/ou lucratif développent et commercialisent des technologies qui facilitent le cyber renseignement et les cyber attaques, d'autres transmettent à leurs gouvernements des informations recueillies auprès de leurs clients, fournissent des technologies numériques vectrices de mouvements insurrectionnels et contestataires voire hébergent et assistent des hackers, services de renseignement ou mouvances criminelles tandis qu'inversement les plus naïves deviennent des proies faciles[lxii].

Investie conformément à la directive de sécurité nationale NSD42 d'une mission d'Information Assurance, la NSA joue un rôle leader dans la protection des systèmes qui traitent des informations classifiées ainsi que des systèmes sensibles utilisés par les militaires ou les agences de renseignement. Elle œuvre à créer un environnement cyber dynamique et sécurisé, cela en s'appuyant sur différents partenaires gouvernementaux, industriels et académiques[lxiii]. Certains jugent paradoxal que l'agence soit chargée à la fois d'espionner et de protéger les données, systèmes et infrastructures sensibles. D'un côté, elle a intérêt à favoriser l'introduction de portes dérobées (*backdoors*) ou de vulnérabilités dans les logiciels, et prône une cryptologie affaiblie pour pouvoir plus facilement pirater les systèmes étrangers ou simplement ciblés. De l'autre, elle semble privilégier une cryptologie renforcée pour éviter l'utilisation de failles par des hackers malveillants.

Début 2016, une initiative est presque passée inaperçue. Dans un souci d'efficacité, de coordination et d'agilité, Michael Rogers a décidé de concrétiser l'initiative NSA21. Les services opérationnels de la direction du renseignement des signaux (SID) qui espionnent les cibles étrangères et ceux de la direction Information Assurance (IAD) qui conçoivent des technologies sécurisés et protègent contre les tentatives intrusives et d'espionnage ont fusionné au sein d'une direction des opérations[lxiv]. Il prend ainsi le risque de mélanger deux cultures qui vont devoir apprendre à se faire confiance et à échanger des idées et des techniques[lxv]. Les relations ave les firmes privées de la cybersécurité vont devenir plus compliquées car le renforcement des capacités en matière de renseignement technique pourrait les inquiéter. Jusque là, l'IAD aidait à identifier les vulnérabilités dans les logiciels. Il est indéniable que la NSA est désormais engagée dans une posture cyber offensive de sécurité nationale. Toujours est-il que cette restructuration rendra plus opaque la répartition des dépenses entre moyens of-

fensifs et défensifs ! L'espionnage digital pose des défis permanents à la NSA. Certains chercheurs estiment sans en avoir la preuve tangible qu'elle aurait cassé un algorithme clef du chiffrement des communications VPN. L'enjeu est à la hauteur du déchiffrement de la machine allemande Enigma pendant la seconde guerre mondiale mais réclame des investissements colossaux, qu'elle est en mesure de faire pour bénéficier d'une écoute passive estimée à 20% des connexions d'un million des plus grands sites « https »[lxvi]. La NSA surveille des pirates, des ONG, des associations telle Anonymous mais aussi les hackers qui opèrent pour le compte des États. Elle affine ses techniques de cyber réingénierie.[lxvii] Durant les dix dernières années elle a détecté de nombreuses attaques provenant de Russie et de Chine. Le bilan fait état de trente mille tentatives contre le ministère de la défense américain, mille six cents ordinateurs piratés, plus de cent millions de dollars de coûts de réparation.

La NSA communique peu sur ses capacités cyber par crainte de livrer des indices à tout adversaire qui pourraient alors concevoir des systèmes de défense. Ceux qui osent dénoncer le système font l'objet de menaces et d'intimidations[lxviii]. D'un certain point de vue, Edgar Snowden pourrait être considéré comme un messager au rôle potentiellement dissuasif. Ses révélations laissent mesurer l'énormité des capacités cyber américaines. Des discours officiels auraient-ils la même portée[lxix] ? Michael S. Rogers est bien conscient des pouvoirs des médias et s'efforce, tel un équilibriste, de justifier les activités de la NSA. Convié à une assemblée du club national de la Presse le 14 juillet 2016, il discute des défis auxquels la NSA est confrontée au quotidien pour maintenir la cybersécurité. En tant que militaire il sait que le pire apprentissage est de prendre connaissance de ce qu'il faut savoir lorsqu'on rentre en contact avec l'ennemi[lxx]. C'est une course permanente pour garder un temps d'avance.

Combien de temps la NSA pourra-t-elle juguler les critiques et les dénonciations ? Un groupe apparemment inconnu, les Shadow Brokers (courtiers de l'ombre) a publié le 13 août 2016, sur la plateforme d'hébergement de code informatique GitHub et sur le site de partage de textes Pastebin rapidement fermés, un message annonçant la mise à disposition de deux dossiers chiffrés faisant état des cyber armes[lxxi] utilisées par le groupe de hackers Equation Group qui serait une émanation de la NSA voire correspondrait à son unité secrète la TAO. Le mot de passe était fourni pour le premier. Le second a été promis via un système d'enchères en bit coins non restituables pour les perdants.[lxxii] Selon les informations fournies par la source, toujours non identifiée, la NSA exploiterait des failles installées dans des équipements de sécurité de réseaux, des pare-feu fabriqués par les entreprises Juniper, Cisco, et Fortinet (toutes trois américaines) et par le chinois Topsec. Les programmes datent de 2013. Quand a-t-elle découvert la brèche ? En 2013 un peu après les révélations de Snowden ou ap-

proximativement en même temps que le reste du monde. Si elle était au courant en 2013, pourquoi n'a-t-elle pas informé les firmes Fortinet et Cisco. Un des exploits malveillants ciblait le pare-feu Fortigate (nom de code Egregiousblunder) et ceux de Cisco (Extrabacon et Epic Banana, Bananaglee). Ces vulnérabilités susceptibles d'être exploitées par des pirates font encourir des risques aux services gouvernementaux et aux entreprises. Cisco a confirmé ne pas être au courant et ne pas avoir de patch. Si la NSA était au courant en 2013 cela signifierait une faiblesse dans la mission Information Assurance car Cisco équipe chaque année les systèmes gouvernementaux que la NSA est chargée de protéger[lxxiii]. Edward Snowden voit dans cette affaire un avertissement des Russes qui se cacheraient derrière les Shadow brokers afin de décourager une escalade géopolitique autour de l'affaire de piratage du parti démocrate. Faut-il imaginer une réaction de leur part à l'accusation portée par les Américains. Le mois précédent, des responsables démocrates, Hillary Clinton et des entreprises de sécurité avaient en effet accusé le renseignement russe d'être à l'origine du piratage des mails du Comité national démocrate (DNC). Publiés par Wikileaks juste avant la convention d'investiture à Philadelphie ceux-ci risquaient influencer le résultat des élections. Est-ce tout simplement l'action d'un ancien de la TAO car les outils utilisés par l'unité d'élite de la NSA sont « stockés sur un réseau à part qui n'est pas connecté à internet ». Wikileaks représenterait toujours une menace car l'organisation a annoncé qu'elle détenait une copie intacte de l'archive des armes numériques de la NSA et qu'elle la publierait en temps voulu.

Les hackers d'élite de la NSA scrutent le cyberespace pour détecter des indices d'intrusion mais parallèlement conçoivent des outils intrusifs délirants. Le modus operandi des espions du XXI siècle se résume en cinq étapes : reconnaissance du terrain en utilisant les réseaux sociaux et l'ingénierie sociale ; élaboration des stratégies d'attaque et de déploiement d'outils selon un plan d'action construit (souvent cela se résume à envoyer des courriels des cibles bien choisies) ; intrusion durable dans l'infrastructure de la cible ; compromission du système informatique et usurpation d'identités obtenues pour accéder aux données ; et enfin récupération discrète (ou masquée) d'un maximum d'informations ». Le malware espion Flame, extrêmement complexe, précis, puissant et sophistiqué aurait été élaboré en prélude à l'attaque Stuxnet. Il semblerait que les Etats-Unis aient été les premiers, à recourir à un acte que l'on pourrait qualifier, au risque de déplaire, de « cyberguerre ». En collaboration avec l'unité israélienne 8200[lxxiv], la NSA et la CIA ont conçu l'opération Olympic Games, ensemble de programmes de cyberattaques validés successivement par Georges W. Bush et Barack Obama. La principale opération consistait à introduire un malware, baptisé par la suite sous le nom de Stuxnet par la société de sécurité informatique russe Kaspersky Lab qui l'a découvert, dans les systèmes industriels SCADA qui comman-

daient les centrifugeuses des installations nucléaires iraniennes. Le but était de les rendre inopérationnelles, sans attirer l'attention sur les causes réelles. Un projet plus sensible Nitro Zeus n'aurait pas été mis en œuvre par crainte d'une escalade dans les attaques émanant des pays étrangers[lxxv].

Malgré la puissance de leurs moyens cyber, les États-Unis ne sont pas à l'abri d'actes destructeurs qui pourraient procéder par gradation. Le 11 octobre 2012, Leon Panetta, secrétaire de la Défense a exprimé ses inquiétudes face à une cyber - catastrophe. Une structure importante avec un niveau élevé de renseignement pourrait en être à l'origine. D'aucuns imaginent en première phase une guerre par l'information (utilisation de réseaux sociaux pour lancer des rumeurs et fomenter des protestations, attaques par dénis de service DDoS sur les sites institutionnels politiques, puis attaques de réseaux locaux vulnérables). En deuxième phase, ils appréhendent des attaques sur les installations vitales, le but étant de saturer les services de sécurité d'une part et de déstabiliser la société, pour alors lancer des actions offensives plus complexes et potentiellement mortelles.[lxxvi] Un Pearl Harbor informatique est régulièrement évoqué par les autorités souveraines. Embarqués, ou susceptibles de l'être, dans des batailles de plus ou moins forte intensité, les stratèges et les tacticiens de la NSA se préoccupent donc de tout type de cybermenaces : cyberespionnage, cybercriminalité, cyber propagande, tentatives de déstabilisation, sabotage et cyberterrorisme. Ils entendent rester maître du terrain en maintenant leur dominance informationnelle grâce à des partenaires de choix.

« Silence city »[lxxvii] s'efforce de maintenir le secret sur ses activités de renseignement et d'Information Assurance et plus encore sur ses expertises en matière de guerre du sens. Elle combat les phénomènes d'influence dangereux pour la sécurité nationale en peaufinant maints stratagèmes Elle procède sur Internet à des opérations cognitives et de sales ruses, tactiques offensives qui relèvent de la guerre par l'information[lxxviii]. Les hackers de la NSA et du GCHQ, ne se contentent pas seulement de surveiller YouTube, Twitter, Flickr, Facebook et les blogueurs (guerre pour), ou de propager des virus destructeurs tel *Ambassadors Reception* qui crypte l'ordinateur cible, efface les mails, bloque l'écran et l'accès à Internet (guerre contre). Ils attaquent des groupes comme les Anonymous avec les mêmes armes DDoS qu'il les accuse d'utiliser[lxxix], ils leurrent leurs cibles, jouent sur un registre sexe, par exemple pour attirer une personne à un rendez-vous où elle sera arrêtée. Ils compromettent des internautes sur les réseaux sociaux. Le Joint Threat Research Intelligence Group, unité clandestine du GCHQ, s'incruste dans les discussions en ligne, cherche à contrôler, infiltrer, manipuler et déformer. Parmi les tactiques les plus utilisées, cette unité, maître dans l'art de la déception, diffuse de fausses informations pour porter atteinte à la réputation des cibles[lxxx]. Des faux discours ou des faux blogs sont propagés sur le web par de soi-

disant victimes de la cible ou des informations négatives sont postées sur les forums. Les photos sont modifiées sur les réseaux sociaux. Des courriels et des textes sont envoyés à ses collègues, voisins, ou amis. Les opérations clandestines en ligne (OCA)[lxxxi] servent à créer un événement réel ou cyber et à discréditer une cible. Elles utilisent un large spectre dont les moyens 4D's (*Deny, Disrupt, Degrade, Deceive),* empêcher, perturber, dégrader, tromper). Les opérations informationnelles (Information Ops) ont pour but de déformer et d'influencer le contenu. Le contenant est attaqué par des perturbations techniques *(Technical Disruption)*. Le mensonge, l'analyse des réseaux humains, la contre-argumentation et autres techniques de manipulation sont la base de ces tentatives d'infiltration cognitives, qui s'inspirent de la psychologie et d'autres sciences sociales. Elles s'articulent autour des notions de "leaders", de confiance, d'obédience et de conformité. N'importe qui peut être visé par ces activités clandestines qui compromettent l'intégrité d'Internet. Pourquoi pas des firmes ? Un transparent intitulé « Discréditer une entreprise » et présenté lors de réunions des Fives Eyes en 2010 et 2012, mentionne : « stopper les affaires et ruiner les relations d'affaires » ! Les sociétés aux activités criminelles ne sont assurément pas les seules dans l'œil de mire ?

Rompue à l'art de se renseigner, d'opacifier et de tromper, la NSA développe désormais une politique de domination technologique et de dominance informationnelle basée sur une approche globale[lxxxii], soutenue par la Maison Blanche.

Des pouvoirs et des missions étendues

Les capacités démesurées de renseignement électromagnétique de la NSA bien que facilitées par la dominance Internet américaine[lxxxiii] sont néanmoins en partie menacées par les combats nationaux ou régionaux pour la souveraineté numérique. Lors d'une interview à Re/code, le Barak Obama a pris la défense de Google et Facebook aux prises avec les instances régulatrices européennes, qui selon lui défendent pour des raisons essentiellement commerciales des entreprises moins compétentes ! Lorsqu'il déclare « Internet nous appartient, nos entreprises l'ont créé, développé, perfectionné. Les autres ne peuvent pas nous concurrencer »[lxxxiv], cherche-t-il implicitement à défendre la puissance cyber américaine ou se serait-il laissé enrôler dans ce litige avec l'Europe par les Gafa qui mettent tout leur pouvoir d'influence au service de leurs ambitions politiques[lxxxv]. En cas de fragmentation et de bunkérisation d'Internet, la NSA serait contrainte de renforcer les opérations clandestines à hauts risques, menées par sa division des opérations spéciales. La NSA, on le sait, exerce une surveillance extrême sur la colonne vertébrale d'Internet. Pourtant elle reste silencieuse sur les attaques dénoncées par Bruce Schneier, expert en cybersécurité réputé, sur son blog « Quelqu'un est en train d'apprendre à détruire Internet »[lxxxvi]. Depuis quelques mois,

les entreprises critiques de l'Internet, telle VeriSign[lxxxvii], subissent des attaques sophistiquées régulières en déni de service, graduées en puissance et durée, comme si celles-ci testaient les défenses. Acte d'espionnage ou de renseignement mené par le cybercommandement d'un État qui affute ses armes en cas de cyberguerre ? Probable pour Schneier. L'agresseur non identifié pourrait fort bien être la Chine.

L'administration Obama a donné des pouvoirs élargis à la NSA pour traquer sur Internet les pirates informatiques travaillant pour des gouvernements étrangers. Toutefois, la difficulté d'attribuer l'origine des attaques numériques et de discriminer affaires d'État et criminalité soulève maintes questions en particulier sur le plan diplomatique[lxxxviii]. James Clapper s'est d'ailleurs déclaré plus préoccupé par la multiplication d'offensives numériques de « faible et moyenne intensité » que par une attaque d'envergure[lxxxix]. En avril 2015, les États-Unis accusent des pirates chinois d'avoir fomenté une intrusion informatique dans les systèmes de l'Office of Personnel Management (OPM). Ce réseau fédéral américain des ressources humaines de la fonction publique gère les effectifs du gouvernement et accrédite des milliers de fonctionnaires fédéraux chaque année. 4 millions d'employés, actuels et anciens, seraient concernés. Vol d'identité ou espionnage, le FBI fut chargé d'enquêter. Un an auparavant, une attaque contre l'OPM et deux sous-traitants avait été bloquée et attribuée à la Chine par un haut responsable américain. Suspectée, celle-ci constituerait ainsi une immense base de données en s'attaquant aux fichiers électroniques d'agences gouvernementales, d'hôpitaux et de compagnies d'assurances santé, telle Anthem ou de grands groupes comme le distributeur Target ou le studio de cinéma Sony Pictures Entertainment. Des boites de courrier électronique à la Maison Blanche et au département d'État, des courriels de Barak Obama auraient été pris pour cibles mais l'auteur serait la Russie. Le département de la justice a signalé en 2014 que cinq membres de l'armée chinoise s'étaient introduits dans les systèmes d'entreprises métallurgiques, d'installations nucléaires et d'entreprises du secteur de l'énergie solaire pour y voler des secrets d'affaires. L'administration Obama déclara ne pas pouvoir tolérer des actions étatiques qui cherchent à saboter des firmes américaines et à miner l'intégrité d'une compétition équitable. Cette menace contre la sécurité nationale et économique, s'élèverait à des dizaines de millions de dollars voire à plus d'une centaine[xc]. Les Chinois ne se privent pas pour accuser les États-Unis d'espionnage industriel.

La NSA adresserait des renseignements à la CIA, aux départements de la sécurité intérieure, d'État, du commerce, de l'Energie et du Trésor, à l'agence de renseignement de la Défense (DIA), à la Réserve fédérale et au commandement des forces américaines en Europe. Cet appareil d'État, transformé en machine de guerre économique, livrerait des informations de nature commerciale aux firmes états-uniennes. Les États-Unis nient s'adonner à ce genre de pratiques[xci]. D'ail-

leurs n'ont-ils pas initié un accord passé entre les Présidents Xi Jinping et Barack Obama en septembre 2015 qui stipule qu'aucun gouvernement ne mènera ou ne soutiendra en connaissance de cause la violation par voie cyber de la propriété intellectuelle, dont les secrets commerciaux et des affaires, avec l'intention de fournir un avantage compétitif à des firmes ou des secteurs commerciaux ». Cela ne signifie pas la fin d'un hacking réciproque Chaque nation va continuer à espionner pour des raisons politiques et militaires. Les États unis espionnent pour soutenir leurs politiques en matière de lutte contre la non-prolifération, de respect des sanctions, mais aussi de négociations commerciales et de traque contre les pratiques de corruption étrangère sans se priver, semble-t-il, de surveiller les technologies militaires étrangères sous prétexte de développer des contre-mesures. Ils fournissent cependant des informations à leurs entreprises pour les prévenir d'éventuelles attaques ou des tentatives d'espionnage suspectées à leur encontre. Sont particulièrement concernés celles des secteurs aéronautiques, de la défense de l'énergie et de haute technologie. La nuance entre informations économiques et informations commerciales telle qu'argumentée a du mal à convaincre les adversaires.[xcii]

En effet, une note de la NSA de 2012, intitulée « France, développements économiques » détaillent les besoins de renseignement (Information Needs, IN) et les éléments d'information essentiels à collecter (EEI). Cela concerne :

- Les pratiques commerciales et financières françaises ;
- Les relations économiques de Paris avec les États-Unis, avec d'autres pays ou avec les institutions financières internationales ;
- Les positions de l'Hexagone sur les agendas du G8 et du G20 ;
- Les grands contrats de 200 millions de dollars ou davantage dans les ventes à l'étranger et impliquant les entreprises françaises, faisabilités, négociation ;
- Les secteurs stratégiques (Télécommunications, énergie, transports, biotechnologies. Les entreprises du CAC 40, les opérateurs d'importance vitales (OIV), les firmes aéronautiques.

La France bénéficie depuis quelques années de moyens et de puissance techniques pour détecter et identifier les attaques. L'Élysée fut l'objet d'une attaque informatique en 2012 identifiée en tant que Quantum Attack par les services de Bernard Barbier, alors directeur technique de la DGSE. En avril 2013, celui-ci fut envoyé par la nouvelle présidence demander des comptes au directeur tout puissant de la NSA, Keith Alexander, (2005-2014). Contrarié, celui que l'on surnomme « Alexander, le Geek » aurait déclaré qu'il était déçu car il pensait que jamais on ne les détecterait tout en ajoutant « vous êtes quand même bons »[xciii].

La France réputée passive sur le plan cyberoffensif[xciv], s'est vu longtemps reprochée de se cantonner à la contre ingérence. Que se passe-t-il vraiment ? La loi relative au renseignement du 24 juillet 2015 autorise les ser-

vices de renseignement à agir pour la promotion des intérêts économiques et industriels de la nation ». Reste à en attendre la concrétisation, au bénéfice des entreprises françaises et du développement économique. Faut-il encore une volonté politique à l'écoute des renseignements qui lui sont rapportés !

Où placer le curseur entre légitime et illégitime, entre désinformation et réalité des pratiques ? Les Américains sont pragmatiques : *business is business*. Tandis que la NSA s'arrime à une ambition panoptique d'espionnage planétaire de tous les réseaux, de tous les cerveaux électroniques et humains et alors que les menaces augmentent en intensité et complexité, la confiance des citoyens dans les services de renseignement technique risque encore de s'émousser, non pas tant pour ce qu'ils font, mais pour ce qu'ils ne disent pas.

Possibles ou évitables ?

Les dérives de la NSA sont à prendre au sérieux mais pas uniquement au regard des droits civiques et de la liberté privée. Elles se constatent amplement sur les échiquiers politique, diplomatique et économique où le renseignement apporte un avantage asymétrique.

Les risques humains

Cependant, plus que les machines et les institutions, ce sont les hommes, leurs attitudes et leurs comportements qu'il faut diaboliser car ils sont facteurs de risque. Le principal est l'absence d'esprit critique. Souvent aux prises d'une angoissante impression d'impuissance et résignés par une surveillance en apparence indolore, ou motivés par des intérêts plus ou moins avouables, décideurs et individus se désintéressent du renseignement. Ils ne prennent pas suffisamment conscience de ce qu'il est en train d'advenir, ne perçoivent que ce que d'autres veulent bien laisser voir, et que ce qu'ils veulent bien voir. Ils se complaisent dans une ignorance profonde. Ils savent en partie mais ils ne cherchent pas à comprendre. « Qui peut les prendre pour cibles », « pour quoi faire », « dans quels buts » font partie des questions qu'ils ne se posent guère. Fatalistes, des citoyens acceptent que les affaires de l'État soient traitées à leur insu au nom de la sécurité nationale et se contentent d'informations qui ne peuvent leurs être dissimulées ou qui sont manipulées et diffusées intentionnellement. De surcroît, ils restent asservis à des machines, qui seront d'autant plus facilement instrumentalisées par des esprits malintentionnés. L'hacktiviste Okhin, bien connu des services de renseignement, regrette la peur et le manque d'apprentissage éclairé de la navigation sur Internet. Il déplore que les individus, effrayés par les discours alarmants des médias de masse et des réseaux sociaux, soient devenus « pas prudents mais paranoïaques ». « Tout le monde a perdu de vue le modèle de menace », ne cesse-t-il de répéter[xcv]. La NSA joue sur la raison d'État et la sécurité nationale. Elle est d'autant

plus puissante que la peur prolifère. Toutefois, imprudence ou inconscience, certains opposants à des régimes oppressifs prennent le risque de trop communiquer sur les réseaux sociaux car ils ignorent les capacités réelles des logiciels espions[xcvi] tandis que des personnalités politiques auraient tendance à ne pas respecter les consignes d'usage de la messagerie électronique[xcvii]. Peu médiatisé, un malaise survenu au ministère des affaires étrangères français n'a sûrement pas échappée à l'œil vigilant de la NSA[xcviii].

Les services de renseignement technique se positionnent avant tout sur un registre « tout savoir, tout collecter. En l'absence de réels contre-pouvoirs ou d'une régulation suffisante, ils opèrent à l'abri du « secret défense » et rompent « avec les principes sacrés de l'égalité des armes, de loyauté de la preuve et de la publicité des débats »[xcix]. Or, le culte de l'opacité favorise les dérives du pouvoir, dangereuses à plusieurs titres.

En effet, tout président des États-Unis a le pouvoir d'étendre ceux de la NSA par de nouveaux ordres exécutifs ou par des directives imposant aux agences fédérales d'ajuster leur politique interne. Dans la directive présidentielle PPD-28 du 17 janvier 2014[c], Barak Obama rappelle les objectifs assignés aux activités SigInt qui recouvre la *foreign Intelligence* et la *counterintelligence*, telles que définies dans l'Executive Order 12333, signée en décembre 1981 par Ronald Reagan[ci]. Le concept de renseignement étranger désigne toutes les informations relatives aux capacités, aux intentions ou aux activités de puissances, d'organisations ou de personnes étrangères ou de terroristes internationaux. Ce texte constitue la base légale justifiant l'acquisition de quantités colossales de données en dehors du territoire américain, ainsi que le recueil des listes de contacts et des carnets d'adresses de logiciels de messagerie électronique et de conversations instantanées. Le discours, en partie équivoque sur les fins économiques et commerciales, enjoint de respecter les droits privés et les libertés civiles. La collecte SigInt ne doit pas être menée contre des personnes à des fins discriminatoire, raciste, sexiste ou religieuse. Or, l'affaire Snowden a alerté sur certaines dérives dans un pays se disant démocratique, dérives qui pourraient empirer suite à un changement de gouvernement. Une agence de renseignement régalienne peut être instrumentalisée par l'exécutif, dès lors en mesure d'exercer une surveillance totalitaire d'une profondeur inégalée. En effet beaucoup plus efficaces que les caméras, les technologies sémantiques conçues par les plus grands experts en neurosciences, mathématiques, linguistique et informatique explorent les données collectées en masse (les fameuses *big data*), profilent les individus, analysent leurs comportements, leurs modes de pensée, et en déduisent des attitudes futures. Au service d'une dictature ou d'un gouvernement répressif, elles sont attentatoires aux libertés et au droit d'exister. Des dérives sont d'ores et déjà constatées dans certains pays (Corée du Nord, Tadjikistan, Arabie Saoudite, Iran, Chine, etc.).

Pour Donald Trump, la démocratie et la transparence ont rendu les États-Unis trop faciles à déchiffrer par leurs ennemis. Ses positions irraisonnées en matière de politique étrangère inquièteraient les militaires qui, selon le général Michael Hayden, auraient peut-être le devoir de refuser d'exécuter les ordres présidentiels[cii]. Les hauts gradés de la NSA auraient-ils un tel esprit de rébellion ? Tant qu'il est encore temps, Barak Obama devrait admettre les erreurs de sa propre administration - qui a cependant marqué certaines avancées en matière de justice et d'égalité civique -, et accorder sa clémence présidentielle aux lanceurs d'alerte, accusés sous le coup de la loi *Espionage Act* d'avoir divulgué des informations sensibles[ciii]. Il couperait ainsi l'herbe sous le pied au candidat républicain qui devenu président, risquerait depuis le bureau ovale ordonner une politique répressive en prétendant ne pas être le premier[civ].

Un service de renseignement doit rester aussi peu politisé que possible. La NSA, qui relève du département de la Défense et fait partie des 17 agences dirigées par le DNI, doit composer avec le Congrès, le bureau de surveillance de la vie privée et des libertés civiles, et le Département de la Justice. Certes, mais les personnages qui représentent ces entités, leur personnalité, leurs convictions, leur versatilité et leurs réseaux influencent l'équilibre du système. Ils demeurent susceptibles de se laisser circonvenir par les services de renseignement. Investi d'un pouvoir extraordinaire, le directeur de la NSA doit être choisi avec circonspection. Ce serait apparemment le cas de l'amiral Mike Rogers qui est chargé - rappelons le - de répondre aux besoins SigInt du gouvernement américain et des autorités militaires, de garantir la protection des systèmes d'information et des infrastructures sensibles, et qui a autorité sur tout le spectre des opérations militaires cyber, défensives et offensives. « Rogers est l'homme le plus apte qui soit pour nous projeter dans le futur cybernétique » a déclaré l'ex amiral Gary Rouhead qui lui avait confié en 2011 le cyber commandement de la 10e flotte des États-Unis. Imaginons que tous ses pouvoirs incombent à l'avenir à un haut gradé qui se révèlerait encore plus monarque et démoniaque que le prédécesseur de Rogers, Keith Alexander. Surnommé « l'empereur » ou « Keith the Geek », et favori de Donald Rumsfeld, alors secrétaire à la Défense de l'administration G.W. Bush, il avait usé de toute son influence pour mettre en pratique une politique systématique et indiscriminée de collecte d'informations. Qu'adviendrait-il si le futur nominé devenait incontrôlable ?

Une agence de renseignement technique encourt également la folie scientifique de ses ingénieurs, chercheurs et cryptologues susceptibles de s'enfermer dans une course en avant pouvant devenir immaîtrisable au point de franchir un jour le seuil de la « singularité technologique »[cv]. Dans l'immédiat, ces hommes détiennent des pouvoirs certains car les évolutions en intelligence artificielle, en robotique, et en physique quantique sont fulgurantes. Brillants

concepteurs, ils tentent d'éviter de se laisser distancés par les avancées technologiques et par l'inventivité de pirates ou mercenaires étatiques hostiles, de blacks hackers opérant pour leur propre compte ou au nom d'entités criminelles voire terroristes. Ivres de leur puissance ils œuvrent à la protection des infrastructures sensibles, toutes dépendantes de l'électronique et du numérique et dont l'atteinte aurait pour conséquences d'incommensurables ravages. Or aucune organisation n'est à l'abri de la trahison d'un des siens. L'appât de l'argent, un chantage, un ego démesuré, une idéologie peut faire basculer dans la trahison ou l'acte de sabotage. A souhaiter que les tests de sélection soient fiables et les attributions du « droit à en connaître » constamment revisitées y compris pour les employés des firmes sous-traitantes.

En apparence, l'affaire Snowden a refroidi les relations entre la Silicon Valley et la NSA. Brouille temporaire car l'exécutif ne peut pas se passer des géants High-Tech. Mais où et quand s'arrêtera la collusion ? Certains acteurs du numérique manifestent déjà leur mégalomanie. Un démoniaque à la tête d'une trans-entité aurait des facilités pour imposer insidieusement sa vision du monde. Google est déjà passé outre les injonctions de l'État français. Lors de son lancement, Geoportail a été sommé de masquer diverses zones sensibles classées secret-Défense (bases navales, sites d'interception de la DGSE à Domme en Dordogne et Mutzig dans le Bas-Rhin, etc.) ou d'en empêcher une interprétation utile. Mais le géant Google Earth les a mis à disposition de la planète avec une fine résolution. La Direction de la Protection et de la Sécurité de la Défense (DPSD), notamment chargée de les protéger n'a pas pu opposer d'interdiction à une société américaine privée[cvi]. Les conseillers techniques ou projets, et les lobbystes de Google participent à de fréquentes réunions à la Maison Blanche. Les mouvements de personnel réciproques entre la firme et les services gouvernementaux sont prouvés. Les relations de proximité sont toutefois opaques. Éric Schmidt, président de Google/Alphabet est un supporteur enthousiaste d'Obama et du parti démocrate qu'il finance confortablement. Google est doublement poursuivi par l'Union européenne pour abus de position dominante et de violation des règles de concurrence de l'UE, mais a échappé aux États-Unis à une sanction, annulée par une commission présidentielle. Jusqu'où ira l'emprise de ce géant dont les tendances monopolistiques désillusionnent les pionniers libertaires, fans de créativité sur Internet ? Son moteur de recherche est conçu sur un principe méritocratique. Présent sur divers fronts d'innovations, il est en train de mettre au point avec Sony et Samsung des lentilles de contact capables de prendre des photos[cvii] !

Ces réflexions laissent percevoir quelques uns des dangers d'instrumentalisation du renseignement technique, y compris dans le secteur privé, et la nécessité de déceler avec précocité des déviances humaines, exacerbées par la puissance technologique.

Des décideurs au fait des questions de renseignement

Qui que soit le chef d'orchestre, la raison d'État ne justifie en aucun cas qu'un service de renseignement espionne avec un degré de sophistication poussé à l'extrême en s'affranchissant de toute règle. Les Européens s'insurgent contre les pratiques jugées liberticides de la NSA mais réalisent-ils qu'elle n'est pas l'unique entité à redouter. D'autres agences de renseignement violent les communications personnelles et professionnelles mais surtout des secrets afin de favoriser des intérêts nationaux. Les Chinois, les Russes, les Israéliens, etc. rivalisent avec les Américains. Or, les questions de renseignement[cviii] ayant indéniablement un caractère stratégique, surtout avec l'explosion des conflictualités dans le cyberespace, le renseignement d'État ou d'entreprise devrait être perçu comme des armes incontournables dont la responsabilité n'est pas à mettre entre les mains de n'importe qui. Décideurs politiques et dirigeants, à l'exception des inconscients, des têtes brûlées ou de ceux qui font une confiance excessive à leur seule intuition savent que l'anticipation, l'intelligence et la capacité à se projeter dans la peau de l'adversaire sont des principes stratégiques fondamentaux. En l'occurrence, ils sont en droit d'exiger un renseignement de qualité pour mieux comprendre les situations[cix]. Cela implique d'accorder une attention particulière aux services de renseignement et de sécurité, de leur attribuer des ressources conséquentes, et d'accepter d'écouter les « porteurs de mauvaises nouvelles » plutôt que les flatteurs. Obama a demandé que les divergences d'analyse entre les agences lui soient remontées en toute transparence[cx]. Pourtant, les hauts responsables militaires du commandement central des États-Unis (CentCom) auraient présenté à la présidence une vision optimiste de la situation à propos de la menace ISIS. Deux analystes du Centcom affirment avoir été licenciés à cause de leurs rapports concernant les groupes rebelles soutenus par Washington en Syrie. Ils y avaient exprimé leur scepticisme sur les capacités de ces hommes et leur faible attachement aux objectifs américains[cxi]. Un programme d'un montant de cinq cents millions de dollars destiné à entraîner et armer cinq mille rebelles syriens pour combattre Daech a été arrêté en octobre 2015. Seul cinq soldats syriens en auraient bénéficié et nombreuses furent les désertions et offensives d'autres groupes. Cela peut être apprécié comme une vaste plaisanterie péchant par défaut d'une vue systémique du problème. En 1986, Robert Baer, ex cadre arabisant de la CIA, fait allusion à ce problème de politisation du renseignement lorsqu'il évoque une discussion avec Milt Bearden responsable de haut rang de l'agence, officiant à Khartoum. Suivant son bon sens, il avait déclaré : « Kadhafi était complètement dingue, mais les Frères musulmans au pouvoir à Tripoli, ce serait bien pire. La Lybie sombrant dans l'intégrisme islamiste, cela signifiait une déstabilisation en chaîne des voisins, à commencer par l'Algérie et l'Égypte. ». Mais son interlocuteur, décrit comme ayant un flair politique aiguisé,

l'avait stoppé net en ironisant « si Gengis Khan sortait de sa tombe et déclarait qu'il veut supprimer Kadhafi, le gouvernement américain le soutiendrait. Alors, oubliez tout ça ».[cxii] Malheureusement, maints décideurs auraient tendance à ne pas tenir compte du renseignement qui leurs permettrait de mieux appréhender la réalité et l'évolution possible des situations.

Les analystes savent qu'il n'existe aucune boule de cristal permettant de se prémunir contre le risque d'attentat ou autre acte malveillant. Scrupuleusement, les meilleurs d'entre eux s'efforcent de détecter les signes avant coureurs généralement perceptibles dans le temps long. Ils raisonnent grâce à leur expertise plus en termes de causes que de symptômes, si possible en toute neutralité. Ils ont assurément la capacité de poser des questions simples (qui, quoi, où, quand, comment ? quoi si ?) de s'interroger sur les vulnérabilités, de tenir compte des contextes et de changer de lunettes en se mettant dans la peau des autres (amis, ennemis)[cxiii]. Les protagonistes de la surveillance (hommes politiques, directeurs de services de renseignement, hommes de loi, dirigeants de firmes High Tech) gagneraient à bâtir des stratégies non liberticides en recherchant eux - aussi des réponses réalistes à certaines questions. « Que faut-il chercher à éviter ? » aiderait à définir la condition minimale d'un bon équilibre entre transparence et secret, entre sécurité et protection de la vie privée et des libertés civiles. « Que faut-il chercher à réaliser ? » déterminerait les objectifs atteignables de stratégie nationale et de fourniture du renseignement utile. « Que faut-il chercher à réaliser, ou à éviter dans le cadre d'une alliance ? » permettrait par exemple de fixer le cadre et les limites d'une coopération interétatique ou inter agences en matière de renseignement. « Dans quoi ne faut-il pas s'engager ? » obligerait à déterminer les actions impensables et les valeurs éthiques à ne pas transgresser[cxiv]. Concrètement les populations tireraient un avantage à réfléchir de même et à se focaliser davantage sur une exigence de résultat. Mieux tirer partie de l'information concerne aussi bien les services de renseignement que les médias et les citoyens. Cela implique de sortir d'un état cataleptique où les « impétrants, ceux qui éclairent, « sont renvoyés à leurs gazettes littéraires, leurs revues scientifiques et leurs laboratoires »[cxv].

Des citoyens conscients des réels dangers et à l'imaginaire constructif

L'imaginaire paranoïaque peut se complaire dans un déballage d'informations, révélatrices d'une dominance effrayante. Celle que l'on surnomme « No Such Agency », ne parvient plus à tout dissimuler bien que les informations dévoilées datent quelque peu. L'imaginaire constructif, conscient que les vrais secrets, ceux du temps en devenir, ceux des programmes en cours, ceux des collusions clandestines actuelles restent inviolés, adopterait plutôt une attitude proactive d'intelligence du risque visant à protéger ce qui doit l'être. Les citoyens apprécieraient une efficience de la part de

leurs services de renseignement nationaux mais aussi la garantie d'une protection des libertés individuelles et le respect de la vie privée. Confrontés aux abus des services de renseignement étrangers, ils devraient s'attendre à une position ferme de leur gouvernement. Or, les protestations sont souvent frileuses et occasionnelles car les besoins d'échanges de renseignement pour lutter contre le terrorisme et la criminalité organisée dictent les ententes et favorisent de clandestines compromissions sur la scène diplomatique. D'autres intérêts croisés, souvent économiques ou financiers, restent la plupart du temps opaques.

Les individus se laisseraient-ils condamnés à constater et déplorer passivement une surveillance massive, indiscriminée et permanente ? Il serait pourtant légitime de revendiquer une plus grande transparence de la part de l'exécutif en posant certaines questions : « A quoi sert réellement cette surveillance ? », « Quels usages sont fait des données ? », « Pourquoi les programmes de surveillance des communications sont-ils secrets ? », « Combien coûtent-ils ? », « Qu'ont-ils réellement permis ? ». Il ne s'agit pas de s'insurger avec excès contre les activités de renseignement mais de se mobiliser pour qu'elles soient ciblées avec pertinence, limitées dans le temps et mieux contrôlées, afin d'en atténuer les effets pervers. Au milieu d'une suspicion générale, lors du festival des nouvelles technologies South by Southwest en mars 2014, Snowden et Christopher Soghoian, chercheur informatique et militant membre de l'Union américaine des libertés civiles, ont préconisé l'instauration de nouveaux organes de supervision. Ceux-ci auraient pour mission de surveiller le Congrès américain qui néglige son travail de contrôle et couvre les mensonges des directeurs d'agence tels James Clapper[cxvi].

Pour Snowden, « la communauté qui construit Internet » représente « les pompiers qui peuvent le sauver » et le grand public doit s'organiser pour se protéger en ligne. Considérant qu'il faut rendre la surveillance de masse plus chère et moins pratique pour la NSA », il incite « les gens, qu'ils soient journalistes ou citoyens » à utiliser les technologies de chiffrement. Certes, mais le pompier agit dans une logique réactive. Une attitude proactive des « surveillés » consisterait à se faire respecter en tant que contre-pouvoir afin d'obtenir la garantie d'une juste équilibre entre liberté et sécurité. Aucun service de renseignement ne devrait être redéfini en marge de tout débat démocratique. Dans des contextes hostiles de plus en plus mouvants et chaotiques, il serait cependant irréaliste de remettre en question l'existence des services de renseignement et de contre renseignement. Il demeure par conséquent irraisonnable de ne pas se tenir informé des risques encourus, des stratégies et techniques de sécurité.

Reste-t-il une quelconque liberté

L'existence de la NSA est désormais connue. Elle continue d'apporter une large

contribution aux armées américaines, avec des moyens renforcés sur le terrain et dans le cyberespace. Habiles parleurs, les hauts gradés qui la dirige en font régulièrement état dans des discours dithyrambiques Espionne sur les scènes diplomatiques et économico - financières, elle renseigne le gouvernement américain et tous ceux qui interviennent pour défendre ou promouvoir les intérêts de sécurité nationale. Fortement critiquée depuis 2013, elle compose avec le bruit médiatique et une acrimonie généralisée. Paradoxalement certains sujets comme l'espionnage économique sont peu couverts. Le risque est pourtant énorme pour les nations étrangères qui perdent les appels d'offres, les marchés et voient filer leurs entreprises de pointe sous la coupe de leurs adversaires. Obnubilée par une course en avant technologique qu'elle entend dominer elle recherche une dominance informationnelle absolue. La NSA est une institution qui doit rendre des comptes à des autorités. Elle est dirigée par des hommes qui fixent des règles appliquées par du personnel militaire ou civil. Elle a des missions et des préoccupations spécifiques, sa propre organisation, des relations de proximité et de multiples réseaux via les personnes qu'elle emploie. Si elle attire des milliers d'employés heureux de servir leur patrie, elle a aussi ses détracteurs domestiques et étrangers. Elle infiltre, infecte, détruit des systèmes d'information, manipulent des cibles sur les réseaux sociaux. Au nom de la raison d'État et de la sécurité nationale, elle espionne les gouvernements, les administrations, les entreprises, les institutions financières ou culturelles ou scientifiques. Des affaires d'État sont ainsi manigancées avec un temps d'avance au détriment de cibles crédules. Des négociations internationales tournent à l'avantage des États-Unis, des normes sont imposées, des marchés se perdent, des technologies sensibles ou des savoir-faire passent aux mains de l'adversaire, le chômage augmente...

L'omnipotence et l'omniscience de la NSA ne sont toutefois que chimères. Les faits ont prouvé que malgré tous les moyens qu'elle déploie, elle est incapable de traiter à temps toutes les données et métadonnées collectées en masse. Les carences dans l'élaboration du renseignement sont principalement dues au manque d'analystes compétents et de linguistes spécialisés dans les langues rares. De plus, certains renseignements ne s'obtiennent que par des contacts humains - agents intermédiaires, traitres et espions à la solde d'officiers traitants.

L'agence continuera à être diabolisée, en écho aux révélations des lanceurs d'alerte qui ont eu accès directement ou indirectement à des secrets que les autres ignorent et qui se sont exposés pour informer l'opinion à l'échelle planétaire. La querelle intense au nom de la démocratie et des libertés citoyennes a des fondements légitimes mais elle occulte des risques plus insidieux, ceux générés par les velléités politiques, militaires, économiques et scientifiques des Américains qui ne sont pas prêts à abandonner leur hégémonie sur la

scène internationale et au cœur de l'infosphère où conspirent de redoutables infocapitalistes? Les relations État/entreprise sont soupçonnées très fortes (NSA et Google, la CIA pratique du renseignement Open Source sur les réseaux sociaux SocMInt grâce au balayage des plateformes Twitter et Facebook, etc.). Les géants des technologies numériques et des nouveaux médias naviguent selon leurs intérêts dans les eaux troubles de la diplomatie, de la politique, de la défense, de la privatisation militaire, des tractations commerciales et de la propriété intellectuelle. Ils sont maîtres dans l'art des guerres informationnelles. Ils manipulent et profilent en toute quiétude des internautes, plus troublés par le traitement des données effectué par le gouvernement, tout en leur faisant croire à leurs libertés et à leur sécurité numérique L'engouement pour la course aux Pokemons est la preuve de comportements addictifs insouciants qui font la joie de ceux dont le métier est d'engranger et de revendre des milliards de données personnelles. Un rapport de la commission commerce du Sénat américain dénonce de nombreuses compagnies qui vendent des fichiers à des firmes ou des produits financiers à hauts risques à des populations à bas revenus. D'autres proposent des noms de victimes de viol ou contaminé par le HIV (79 dollars les 1000 noms). D'autres encore vendent des données privées aux cyber criminels spécialisés dans la fraude et le vol d'identité. Ces entreprises sont peu contrôlées contrairement à la NSA qui doit rendre des comptes au Congrès et aux autorités judiciaires[cxvii].

Ne serait-il pas temps de combler un « vide stratégique », de s'extraire de la dictature de l'immédiat et du culte exagéré du calcul et des technologies. Cela sous-entend de discriminer avec intelligence et raison les offres surabondantes d'information, de jeux et de services, de ne pas se laisser influencer par des discours éphémères inscrits dans un show journalistique à visée économique. En bref, il s'agirait de « mieux tirer partie de l'information » et de « sortir d'un état cataleptique où les impétrants, ceux qui éclairent, « sont renvoyés à leurs gazettes littéraires, leurs revues scientifiques et leurs laboratoires »[cxviii].

Les débats risquent d'être passionnées car les questions de renseignement interfèrent avec la Raison d'État. Tandis que les GAFA étendent leur influence politique et financière, la NSA, placée sous les projecteurs malgré elle, alimente une contre offensive menée par la commission renseignement de la Chambre juste avant la première du film « Snowden ». Le lanceur d'alertes qui est devenu l'expert le plus qualifié et le commentateur le plus en vue pour parler des opérations de la NSA aurait-il exagéré et gonflé l'évaluation de ses performances en trafiquant son curriculum vitae. Steven Bay, l'homme qui a embauché Snowden sous contrat avec la société Booz Allen Hamilton à Hawai prétend qu'il n'a pas eu accès au programme Prism. « C'est un gars intelligent... Il avait de l'expérience mais il n'était pas un analyste senior... il ne comprenait pas les programmes. Il ne comprenait pas le système global ». Ayant échoué au test in-

terne d'habilitation FAA 702, il ne pouvait pas avoir accès aux programmes de surveillance régis par cet article de loi. Cantonné dans un rôle subalterne, il ne pouvait, selon son recruteur comprendre ni les programmes ni le système global. « Il n'a pas compris le régime de surveillance et de contrôle juridique mis en place pour éviter l'espionnage des citoyens américains, qui est illégal ».[cxix] Mécontent de son échec, Snowden se serait plaint de questions pièges et n'aurait pas repassé l'épreuve d'habilitation. Cet accès refusé, il ne pouvait pas comprendre « ni la supervision, ni les règles concernant leur utilisation, ni la manière de traiter ces informations ». Snowden jure qu'il connaissait « les bons et les mauvais côtés de ces systèmes ». Il avait donc connaissance des programmes. Selon ses dires, il aurait été autorisé à télécharger de l'information dans le cadre d'un programme Heartbeat approuvé par deux niveaux de direction, sorte d'index qu'il établissait à partir des nombreuses opérations de surveillance que la NSA effectuait. Même s'il n'avait pas accès aux informations obtenues par ces programmes, certains éléments 702 étaient déclassifiés et l'amendement de 2008 de la loi FISA qui avait conduit à la création de cet article avait suscité des débats publics entre les responsables du renseignement, les législateurs et les défenseurs des libertés civiles. La NSA n'aurait pas installé d'équipements ni institué de règles qui l'auraient aidé à détecter les agissements de Snowden. L'extraction physique des fichiers ne nécessitait pas les compétences d'un pirate informatique super pointu. Snowden aurait également eu accès dans le cadre de ses activités de contre espionnage à des listes d'ordinateurs que la NSA aurait piraté dans le monde entier. Bernard Barbier, ancien directeur technique de la DGSE reconnaît que Snowden s'est comporté comme un traitre envers son pays, mais « il a montré que l'espionnage entre alliés existait et que le matériel était piraté par les Américains comme celui vendu par l'entreprise US Cisco » Il a favorisé la prise de conscience d'une dépendance technologique[cxx]. Reste à agir en adoptant quelques principes de base. S'imposer en priorité la règle du secret en identifiant ce qui ne doit pas être connu des autres et dont la divulgation serait porteuse de préjudices pour soi-même ou une entité, se déconnecter tout en renouant avec d'anciennes pratiques de communication et de transmission des informations ne sont pas des initiatives décalées. Participer aux débats et se rendre aux urnes, deux libertés accordées dans les démocraties, peuvent contribuer à éviter que se façonne un monde que l'on ne désire pas. Le principal ennemi n'est-il pas nous-mêmes ?

Notes

[i] Auteure de *NSA, National Security Agency : l'histoire de la plus secrète des agences de renseignement*, Paris, Tallandier, 2016, 509 p.

[ii] Martin Untersinger, « Des chercheurs relient le « cybercasse » de 81 millions de dollars aux pirates de Sony Pictures », *Le Monde*, 30 mai 2016.

[iii] Clin d'œil au conte jubilatoire « Mali, ô Mali d'Eric Orsenna, Editions Stock, 2014. Les services secrets français font appel aux « grandes oreilles de madame Bâ Marguerite pour traquer djihadistes et bandits au Mali.

[iv] La politique hégémonique et la volonté interventionniste musclée de l'entourage néoconservateur de G.W. Bush ont appelé à la vengeance et à une « guerre juste et préventive », « une guerre totale au terrorisme ». Les capacités du renseignement technique, devenu une priorité, ont augmenté considérablement. Le gouvernement américain céda à la douce illusion qu'engranger des informations suffit à faire basculer l'équilibre des forces à son profit.

[v] Steven D'Alfonso (membre de la Red Cell Team, experts dans le domaine de la contreintelligence chez IBM) « The Convergence of Organized Crime Groupes and Terrorist Organizations, *Banking an&t Financial Services*, 4 septembre 2014, Https://securityintelligence.com.

[vi] Créée en 1994, la division SOD est un centre de coordination des opérations multi-agences conduit par la DEA avec la participation des agences fédérales, du département de la défense, de la communauté du renseignement. Elle a pour mission de lutter contre les trafics de drogue et le narco terrorisme. Elle établit des stratégies et conçoit des opérations afin de démanteler les organisations internationales trafiquantes en attaquant leurs systèmes de commande et de contrôle des communications. L'*El Paso Intelligence Center*, créé en 1974 à La DEA lutte contre les trafics de drogue et la contrebande le long de la frontière sud-ouest. Le *Bulk Cash Smuggling Center* s'occupe de la contrebande et des trafics d'espèces. Sont également évoqués le *National Export Enforcement Coordination Center*, le *Cyber Crimes Center.*

[vii] National Security Council. Strategy to Combat Transnational Organizzd Crime : Enhance Intelligence and Information Sharing, https://www.whitehouse.gov

[viii] « The National intelligence Priority Framwork, (NPIF) », *electrospaces.blogspot.fr*, 19 mai 2016 ; grille d'avril 2013 présentée en format pdf sur members.efn.org.

[ix] Le programme Overhead espionne les communications au sol, sur réseaux mobiles voire Wifi.

[x] DNI (Digital Network Intelligence) : intelligence des réseaux digitaux

[xi] « (S//SI) New Release: The Fornsat plan », *NSA-SID Today*, 3 juin 2003, *theintercept.com*, 16 mai 2016.

[xii] TS//SI), « Target Development from Scratch: The Russian Tambov Crime Syndicate », *SIDToday*, 5 mai 2003, TheIntercept.com.

[xiii]Deux cartes respectivement datées de 2002 et 2012 signalent les stations américaines les plus importantes : à Sugar Grove (Timberline) et à Yakima (Jackknife) aux Etats-Unis ; à Geraldton (Stellar) en Australie - Darwin (Shoal Bay) ainsi que Pine Gap qui seraient encore opérationnelles ont disparu de la carte **2012 – ;** à Waihopai (IronSand) en Nouvelle Zélande ; à Harrogate (Moonpenny) et à Bude (Carboy) en Grande Bretagne à Misawa (Ladylove) au Japon ; en Thailande près de Khon Kaen (Lemonwood ou Indra) ; Cyprus (Sounder) ; à Oman près de Seeb (Snick). Sabana Seca (Coraline) aurait fermé en 2004. C'est probablement le cas de Nairobi (Scapel). Bad Aibling (Garlick) a été fermée en 2004 mais le BND Allemand continue de coopérer via des activités Sigint conjointes (Joint SigInt Actity, JSA) confiées au centre des communications situé à Mangfall Barracks. Il existerait en outre une quarantaine de stations régionales (SCS) exploités conjointement par la NSA et la CIA dont une à Brazilia et une à New Delhi en Inde « NSA's global interception network », 3 décembre 2013 (màj 17 juillet 2014), electrospaces. blogspot.fr.

[xiv] David Rosenberg, *Inside Pine Gap : The Spy Who Come in from the Desert*, Hardie Grant Books, 2011.

[xv] Gordon Corera, « Spying scandal : will the 'five eyes' club open up ?, *bbc.com*, 29 octobre 2013.

[xvi] Connu aussi sous le nom de code « room 641A » date de 2003. Tempora est l'équivalent pour le Royaume-Uni et Rampart système en coopération via certains pays européens.

[xvii] Optic Nerve (GCHQ) par exemple collecte les photos à partir des chats de Yahoo et surveille les webcams. Ces données sont utilisées pour la reconnaissance faciale,

[xviii] Wellspring par exemple est une banque anthropométrique d'empreintes de visage as alimentée chaque jour par des millions de photos interceptées à parti des communications numériques, des vidéoconférences, des réseaux sociaux ou de passeports et permis de conduire circulant sur le Net. Elle est utilisée dans la lutte contre le terrorisme.

[xix] ACIDWASH en Afghanistan, DUSKPALLET vise les GSM au Kenya, EVENINGWEASEL (wifi mexicain). SOMALGET permet de monitorer les systèmes de télécommunication d'un pays via le plus souvent des entreprises américaines implantées localement et de stocker les informations durant une trentaine de jours.

[xx] « Skynet, Angry Birds, Smurfs... les drôles de noms des programmes-espions de la NSA », *l'Obs*, 21 octobre 2015.

[xxi] « NSA, il est temps de faire le (premier) point », *Reflets.info*, 30 juillet 2014.

[xxii] Ryan Gallagher, Glenn Greenwald, « How The NSA plans to infect millions of computers with malware », *The Intercept*, 12 mars 2014.
[xxiii] Quantum-Insert, Quantumbot pirate les botnets, Quantumdns, Quantumsquirrel, Quantumsky empêche les cibles d'accéder à certains sites, Quantumcopper corrompt les déchargements de fichiers, Quantumhand (faux serveur Facebook), etc.
[xxiv] «The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics », *The Intercept*, 12 mars 2014.
[xxv] Ce procédé fonctionne par des ondes radio transmises depuis un petit circuit électrique ou depuis une carte USB installée clandestinement dans la machine par un espion, un fabricant voire un utilisateur ignorant du piège. Les ondes sont captées par une station relais de la taille d'une mallette distante parfois de plusieurs kilomètres et relayées vers la NSA qui peut alors installer un malware dans la machine à des fins d'espionnage ou de cyberattaques. Cf. E. Sanger, Thom Shanker, « NSA Radio Pathway Into Computers », *New York Times*, 14 janvier 2014.
[xxvi] « TAO, l'unité d'élite de la NSA qui pénètre dans tous les systèmes (MAJ) », *01net,* 30 décembre 2013.
[xxvii] « La NSA a piraté le câble sous-marin géré par Orange », *journaldugeek*, 30 decembre 2013.
[xxviii] Jacob Appelbaum, « Shopping for Spy Gear: Catalog Advertises NSA Toolbox », *Spiegel Online International*, 29 décembre 2013.
[xxix]Jacob Appelbaum, Laura Poitas, Marcel Rosenbach, Christian Stöcker, jörg Schindlerand Holger Stark, « Inside TAO : Documents Reveal Top NSA Hacking Unit', *Spiegel Online International*, 29 décembre 2013.
[xxx] « Follow the Money: NSA Spies on International Payments », *Spiegel Online International*, 15 septembre 2013.
[xxxi] Ryan Gallagher and Glenn Greenwald, « How the NSA plans to infect « millions of computers with malware », *The Intercept*, 3 décembre 2014.
[xxxii] Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Leif Ryge, Hilmar Schmundt, Michel Sontheimer, « The Digital Arms Race: NSA Preps America for Future Battle », *Spiegel Online International,* 17 janvier 2015.
[xxxiii] « *Your data is our data, your equipement is our equipment* » (ROC)[xxxiv].
[xxxv] Réseau d'attaque formé de machines compromises et pilotables à distance en simultanée. Un botnet sert à l'émission de spam, à l'implantation de programmes malveillants ou indésirables, à la réalisation d'attaques en déni de service distribué (DDoS), au camouflage de sites frauduleux, etc. Cf Glossaire des menaces, www.clusif.asso.fr.
[xxxvi] Jenna McLaughlin, « New film tells the story of Edward Snowden ; Here Are the Surveillance Programs He Helped Expose », *The Intercept*, 16 septembre 2016.
[xxxvii] Jenna McLaughlin, « NSA Looking to Exploit Internet of Things, Including Biomedica Devices, Officials Says », *Theintercept.com*, 10 juin 2016.
[xxxviii] La campagne NSA21 vise à renforcer l'agence dans son rôle de leader mondial en matière de rebnseignment d'eorigine électromagnétique et d'information Assurande dans les dix prochaines années et au delà. Les trois objectifs prioritaires sont le personnel, l'intégration et l'innovation. L'organigramme a été simplifié pour plus d'efficacité. Voir NSA21, nsa.gov.
[xxxix] *Understanding the Threat*, nsa.gov, 3 mai 2016.
[xl] Greg Miller, Cia plans major reorganization and a focus on digital espionnage, *Washington Post*, 6 mars 2015.
[xli] L'agence avait déjà investi par exemple dans Visible Technologies (gestion de la réputation), Netbase (analyse de réseaux sociaux), Recorded Future (prédiction d'évènements). « The CIA is Investing in Firms That Mine Your Tweets and Instagram Photos », *theintercept.com*, 14 avril 2016. Geofeedia, outil de géolocalisation des tags sur Twitter et Instagram, permet de surveiller les évènements tels que les protestations d'activistes en temps réel. Dunami, technologie de PATHAR, est utilisée par le FBI pour cartographier des réseaux, des centres d'influence et des signes de radicalisation. TransVoyant, créé par Denis Groseclose ancien vice-président de Lockheed Martin surveille également Twitter mais a servi à l'armée américaine en Afghanistan pour intégrer des données en provenance de satellites, de radars, d'avions de reconnaissance et de drones. Dataminr analyse aussi les tendances sur les réseaux sociaux.
[xlii] Claude Delesse, *NSA, National Security Agency*, Éditions Tallandier, Paris, 2016, p. 229-234.
[xliii] « S//SI)Reshaping the World : The Counterproliferation SIGINT Cell », *SidToday*, 3 novembre 2003.

[xliv] Les gardes-côtes sont partenaires de la direction SigInt de la NSA et sont une unité des services de cryptologie dépendant du Central Security Service (CSS) commandés par la NSA.
[xlv] Coast Guard Account manager, « SID Support to the US Coast Guard », SIDtoday, 8 avril 2003. Theintercept.com.
[xlvi] Les forces de l'ordre des États américains disposent désormais de logiciels (Stingrays, Troggerfish, Wolfpack Gossamer,...) qui permettent de localiser des personnes et d'écouter leurs conversations. Depuis 2015 l'obtention d'un mandat est requise mais il existe de nombreuses exceptions au nom de la sécurité nationale et de l'urgence. Christophe-Cécil Garnier, « Comme la NSA, les forces de polices peuvent écouter vos appels, slate.fr, 30 octobre 2015.
[xlvii] Mickaël Bazoge, « Craig Federighi ne veut pas créer un logiciel que les criminels pourraient exploiter », *macg.co*, 7 mars 2016.
[xlviii] Stephane Moussie, « Tim Cook en Une de Time : le chiffrement est une chose formidable », *macg.co* 17 mars 2016. D'autres firmes font aussi de la résistance. Elles optent de plus en plus pour le « *Privacy by design*[rlir]» et conçoivent des technologies hautement cryptées. WhatsApp a affirmé ne pas disposer des messages de ses utilisateurs qui sont chiffrés et stockés sur ses serveurs...
[l]Guillaume Champeau, « FBI vs Apple : la faille aurait été fournie par des hackers chasseurs de primes », *Numerama.com*, 13 avril 2016 d'après Ellen nakashima, « FBI paid Professional hackers onte-time fee to crack San bernardino iPhone », *The Washington Post*, 12 avril 2016.
[li] « Eddy Cue : « Les ingénieurs d'Apple travaillent contre les criminels », *macg.co*, 10 mars 2016.st
[lii] Jenna McLaughlin, « NSA is Mysteriously Absent From FBI-Apple Fight », *The Intercept*, 3 mars 2016
[liii] James McLaughlin, « Snowden : FBI Claim That only Apple Can Unlock Phone Is « Bullshit », *The Intercep*t, 8 mars 2016.Voir aussi Brian Barrett, « Tech Giants agree : the FBI 's case against apple is a joke », *Wired*, 3 mars 2016.
[liv] Si l'on en croit un des documents subtilisés par Edward Snowden et relayés par the Intercept en mai 2016. Voir : Cora Currier, « NSA closely involved in Guantánamo interrogations, documents show », *SidToday*, october 2003 et *theintercept.com*, 16 mai 2016.
[lv] Complexe pénitenciaire irakien situé à une trentaine de kilomètres de Bagdad, lieu de détention, de torture et d'exécution de prisonniers politiques sous Saddam Hussein fermé en 2002. Il fut rouvert par les américains en août 2003. « A unique Opportunity Awaits you « in Irak », *SidToday*, décembre 2003 et juin 2003.
[lvi] « Lune de miel douce-amère entre Paris et Londres », *Intelligence Online*, n° 756, 30 mars 2016. Les britanniques critiquent la compétence judiciaire et la culture policière de la DGSI qui seraient, selon eux source de malentendus avec les autres services de renseignement intérieur.
[lvii] Emmanuel Fansten, « Wikileaks : quand Sarkhozy jouait les VRP de Ricard aux États-Unis, *Libération*, 25 juin 2015.
[lviii] Il existe en Afghanistan des centres d'opérations communs ou des Américains, des Britanniques et des experts d'autres pays travaillent côte à côte.
[lix] David Dan, « Entretien avec Dennis Blair : les coulisses du renseignement américain », *Politique Internationale*, n°133, automne 2011.
[lx] Tom Rogan, « The Panama Papers Vindicate the NSA », *National Review*, 6 avril 2016.
[lxi] Abdeslam a été appréhendé après une fusillade dans la capitale belge le 18 mars. Cf. « La Belgique a fait appel à la NSA pour l'aider à trouver Salah Abdeslam », *buzzfeed.com*, 22 août 2016.
[lxii] Nato Cooperative Cyber Defence Centre of Excellence, « EU Policy on Fighting Hybrid Threats », *CCDCOE Incyder news*, 24 mai 2016, https://ccdcoe.org. Les menaces hybrides sont définies comme un mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (par exemple diplomatie, affaires militaires, économiques, technologiques)- qui peuvent être utilisées de manière coordonnées par un État ou des acteurs non gouvernementaux afin d'atteindre des objectifs spécifiques tout en restant en dessous du seuil d'une guerre formellement déclarée. Une guerre hybride est définie comme un type de guerre généralement présenté comme alliant guerre conventionnelle et non conventionnelle, guerre régulière et irrégulière, guerre de l'information et cyberguerre.
[lxiii] « Integrated Intelligence Key to Combatting Dynamic Threats », *The Cipherbrief*, 7 juillet 2016.
[lxiv] Nicolas Arpagian, « Les Entreprises complices et victimes de la cyberguerre », *Revue internationale et stratégique*, n°87, automne 2012

[lxv] nsa.gov.
[lxvi] Helen Nakashima, « National Security Agency plans major reorganization », *The Washington Post*, 2 février 2016.
[lxvii]Une direction des capacités et de la recherche est par ailleurs confirmée.
[lxviii] Reynald Fléchaux, « Comment la NSA a (probablement) cassé le chiffrement par VPN », Silicon.fr, 20 octobre 2015.
[lxix] Par exemple des programmes sont dédiés aux attaques iraniennes (nom de code Voyeur) ou françaises (Snowglobe). « Pay attention to that man behind the curtain: Discovering aliens on CNE infrastructure », CSEC Counter-CNE, Target Analytics thread SIDEV Conference NSA-June 2010 ; Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maghun, Laura Poitras, Marcel Rosenbach, Leif Ryge, Hilmar Schmundt and Michael Sontheimer, "NSA prepares America for Future Battle", *Spiegelonline*, 17 janvier 2015.
[lxx] En 2013, John Crane enquêteur spécialisé dans les informations fournies par des lanceurs d'alerte travaillant pour le Pentagone, où il a été responsable de la cellule dédiée jusqu'en 2002, a été poussé à la démission par sa hiérarchie après une longue procédure. Thomas Drake très critique vis-à-vis de Trailblazer s'était adressé à lui. La NSA et le Pentagone ont échoué à protéger leurs lanceurs d'alerte », *Le Monde*, 23 mai 2016.
[lxxi] FARRELL Henry, The political science of cybersecurity IV: How Edward Snowden helps U.S. deterrence, *The Washington Post*, 12 mars 2014.
[lxxii]« NSA Chief Mike S. Rogers discussed the continuing cyber sécurity challenges facing the US and the world at the National Press Club Luncheon on July 14, 2016 », *noelstjohn.smugmug.com*, 14 juillet 2016.
[lxxiii] 280 MB d'outils offensifs top secrets incluant des exploits zéro day et des implants.
[lxxiv] Le message s'est propagé sur Tumblr, site rapidement fermé de même que Github. Cf. Amaelle Guitton, La NSA dans le viseur des « Shadow Brokers » ? *Libération*, 17 aout 2016 ; Damien Bancal, Shadow Brokers : les hackers de la NSA piratés ? zataz.fr, 14 août 2016.
[lxxv] Nicolas Weaver, « Nick Asks the NSA : Shadow Brokers and the Leaking Ship », *Lawfareblog.com*, 24 août 2016.
[lxxvi] Unité israélienne responsable du renseignement d'origine électromagnétique et du déchiffrement de codes.
[lxxvii] Suite à l'affaire Stuxnet, des attaques ont ciblé les installations énergétiques ou sensibles au Moyen-Orient, en Cisjordanie, en Iran, et au Liban.
[lxxviii] Pierre Alonso, *Les Peurs des cyberdéfenseurs*, *owni.fr*, 30 octobre 2012.
[lxxix] aussi surnommée « SigInt City », « No such Agency » ou « Not Say Anything »
[lxxx] Troisième catégorie de guerres informationnelles, parfaitement maîtrisées par la NSA et l'agence de renseignement électromagnétique britannique.
[lxxxi] Déni de service distribué
[lxxxii]Glenn Greenwald, « How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations », *The Intercept*, 24 février 2014.
[lxxxiii]*Online Covert Action.*
[lxxxiv] Les questions de sécurité extérieure interfèrent avec les préoccupations intérieures que celles-ci soient d'ordre politique, militaire, économique, technique, scientifique ou idéologique.
[lxxxv] Les infrastructures d'Internet sont implantées pour la majorité sur le territoire américain et les acteurs qui pèsent dans le monde digital sont pour la plupart des firmes estampillées U.S. Le transfert de compétence de la gestion technique Internet de l'Iana à l'Icann, organisation de droit californien dont la gouvernance s'émancipe de la tutelle des États-Unis en devenant multipartite à partir du 1er octobre 2016, a largement été soutenu par le géants du Net (Google, Facebook, Amazon, Twitter) qui souhaitent « un Internet global, interopérable et stable. Garant de la sécurité économique et nationale, ce modèle préservera selon eux les intérêts américains. Jacques Cheminat, « Icann : derniers raouts avant l'émancipation américaine, *silicon.fr,* 30 septembre 2016 ; « Internet : Facebook, Google et Twitter soutiennent l'Icann », *Silicon.fr*, 13 septembre 2016.
[lxxxvi] David Dayen, « The Androïd administration : Googles Remarkably Close Relationship With the Obama White House, in Two Charts », *TheIntercept*, 22 avril 2016 ; Kara Swisher, « Obama The Re/code Interview, *recode.net*, février 2016.

[lxxxvii] Google, Amazon, Facebook, Apple, etc. Une entreprise de type GAFA est une entreprise qui, grâce à une habile combinaison de zéros et de uns, parvient à créer de la valeur, notamment en bénéficiant d'investissements d'autres entreprises, de contributions d'utilisateurs et d'infrastructures financées par les Etats ou les pouvoirs publics ». Laurent Calixte, « Les Gafa Apple, Google, Amazon, Facebook sont-ils devenus des partis politiques », *medium.com*, 30 août 2016.
[lxxxviii] Xavier de La Porte, « Quelqu'un se prépare à détruire Internet », *franculture.fr* (la vie numérique), 15 septembre 2016 ; Bruce Schneier, *Someone is Learning How to Take Down the Internet*, 13 septembre 2016, https://www.schneier.com.
[lxxxix] Société américaine (État de Virginie) exploite une vaste infrastructure réseau comprenant notamment deux des treize serveurs racines du DNS, gère le registre officiel pour les noms de domaines.com.,.net,. name et d'autres encore. Elle propose aussi plusieurs services de sécurité.
[xc] Charlie Savage, « Hunting for Hackers, N.S.A Secretly Expands Internet Spying at U.S. Border », The New York Times 4 juin 2015.
[xci] « États-Unis : les données informatiques de 4 millions de fonctionnaires piratées, *Le Figaro*, 5 juin 2015, Ellen Nakashima, « Chinese breach data of 4 millions federal workers », *The Washington Post*, 4 juin 2015.
[xcii] Ellen Nakashima, Ibid.
[xciii] James Andrew Lewis, « The US Really Does Want to Constrain Commercial Espionage : Why does Nobody Believe It », *lawfareblog.com*, 1 juillet 2016
[xciv] *Ibid*.
[xcv] Jacques Follorou, « Les confessions d'un maître de l'espionnage, *Le Monde*, 4 septembre 2016 ; p. 10.
[xcvi] Lors d'une conférence face à des élèves de l'école d'ingénieurs Centrale, Supélec, Nicolas Barbier en toute transparence a confirmé la responsabilité de la France derrière une attaque informatique mondiale détectée par les services canadiens, cf Ibid.
[xcvii] Amaelle Guiton, « Cryptographie et surveillance, les revers de la paranoïa, *rue89.nouvelobs.com*, 4 janvier 2015.
[xcviii] Les services de sécurité du gouvernement Kadhafi avaient acheté à la société française Amesys un programme du nom d'Eagle qui leur permettait de traquer et de cibler en temps réel les opposants libyens à travers les messageries. Ils étaient arrêtés et torturés pour avouer ceux que les bourreaux savaient déjà ! La direction d'Amesys était t-elle ignorante, soupçonneuse ou consciente de cette criminelle curiosité ?
[xcix] Preuve est faite toutefois que la violation des courriels et des communications sur les réseaux sociaux s'est poursuivie après la chute de Khadafi dans une Libye en plein chaos.
[c] Hillary Clinton par exemple a été accusée d'avoir évoqué des questions confidentielles via sa messagerie personnelle.
[ci] Le 10 mars, le magazine féministe Causette publie sur son site les courriels échangés entre des diplomates qui s'étaient concertés sur l'opportunité de remettre en toute discrétion la Légion d'honneur à Mohammed Ben Nayef, futur roi d'Arabie Saoudite et actuel ministre de l'Intérieur, le 4 mars à l'Elysée. Les médias français ne devaient pas être avertis, le planning présidentiel ne devait pas mentionner l'événement. Pour cause, l'ONU, le Parlement européen, et certains pays venaient de condamner le Royaume pour avoir exécuté des dizaines d'opposants et bafoué les droits des femmes. Ils lui reprochaient en fait de diriger une coalition arabo-sunnite au Yémen pour combattre la rébellion chiite houthiste et de bombarder sans distinction des civils, femmes et enfants. La France vend son âme pour rattraper un contrat de vente d'armes qui avait été convenu le 4 novembre 2014 avec le roi Abdallah, décédé deux mois plus tard.
[cii] Aucun des diplomates ne s'est rappelé que des écrits non cryptés laissent de dangereuses traces. Les médias saoudiens, l'AFP et le Front national ont relaté à leur manière l'évènement, mais la source amont à l'origine de l'indiscrétion demeure inconnue. Les hauts fonctionnaires craignaient sûrement plus l'opinion publique qu'une intrusion dans leur messagerie ! « Remise de la Légion d'Honneur ; chronologie d'une dissimulation », *Causette*, avril 2016, p. 28-29 ; « Comment la France vend son âme et des armes », *Ibid*., pp 30-31.
[ciii] Médiapart sous la direction de Fabrice Arfi, *La République sur écoute : chroniques d'une France sous surveillance*, DonQuichotte éditions, 2015, p. 13-14.
[civ] White House - Signals Intelligence Activities, *Presidential Policy Directive/PPD-28*, 17 janvier 2014.

[cv] De manière générale, les priorités du renseignement sont définies par le Président des États-Unis en concertation avec la Maison Blanche et les agences de renseignement. Le directeur national du renseignement, placé sous l'autorité et le contrôle direct du président, définit tous les quatre ou cinq ans les missions stratégiques de renseignement en conformité avec la stratégie de sécurité nationale.
[cvi] Peter Holley, « Former CIA Director : Military may refuse to follow Trump's orders if he becomes président », *The Washington Post*, 28 février 2016.
[cvii] Selon le journaliste Peter Maas, Edward Snowden a été tellement diabolisé que le pardon réclamé par l'Aclu, l'Human Rights Watch, Amnesty International, le Guardian, le New York Times, The Intercept et diverses personnalités relèverait d'un extrême courage de la part d'un Président en fin de mandat. Le cas de Chelsea Manning est pour raison identique encore plus délicat. Mais Obama pourrait accorder sa clémence et réhabiliter l'honneur de Stephen Kim, John Kiriakou et Jeffrey Sterling, Thomas Drake. Ex-agent de la CIA, Jeffrey Sterling , a été condamné en mai 2015 à quarante deux mois de prison ferme pour avoir fourni au journaliste, James Risen des informations classifiées relatives aux questions nucléaires. Stephen Kim, ancien du département d'État, a écopé de treize mois de prison ferme pour avoir transmis des informations relevant de la « défense nationale » au journaliste James Rosen de Fox News. John Kiriakou, ancien de la CIA, a été condamné à trente mois d'emprisonnement en janvier 2013 pour avoir divulgué au New York Times le nom d'un agent secret de la CIA. Thomas Drake, ancien cadre supérieur de la NSA a été poursuivi pour avoir dénoncé le programme de collecte de données « au filet » démentiel Trailblazer mis en place par M. Hayden. Ruiné, il travaille désormais dans un Appelstore.
[cviii] Peter Maas, « Why Obama should pardon all leakers and whistleblowers - not just Edward Snowden », *Theintercept.com*, 19 septembre 2016.
[cix] Point de non retour du progrès technique, et de son éventuel changement de régime, quand il cessera d'être conduit par les hommes pour être conduit par les machines.
[cx] Philippe Cohen-Grillet, « Vue imprenable sur les « sites interdits » de la défense, *Paris Match*, 11 mars 2016.
[cxi] « David Dayen, « The Androïd administration », *op. cit.* et *Culture Geek*, 5 mai 2016, bfmtv.com
[cxii] Pourtant les questions de renseignement ne sont qu'épisodiquement évoqués dans la littérature française des relations internationales et des affaires
[cxiii] Ces principes transférables en entreprise incitent les dirigeants à s'appuyer sur des services d'intelligence économique et de risk management en exigeant d'eux de fortes compétences et des capacités d'analyse renforcées.
[cxiv] « One of the things I insisted on the day I walked into the Oval Office was that I don't want intelligence shaded by politics. I don't want it shaded by a desire to tell a feel-good story » : Michael D. Shear, « Obama Orders Inquiry Into intelligence on ISIS », *New-York Times*, 22 novembre 2015. ; David J. Karl, « Connecting the Dots in Obama's Intelligence Scandal », *the Diplomat.com*, 19 décembre 2015.
[cxv] Shane Harris, Nancy A. Youssef, « Intel Analysts: We Were Forced Out For Telling The Truth About Obama's ISIS War », *Thedailybeast.com*, 4 avril 2016.Gregory Hooker responsable des analyses sur laa situation en Irak et identifié comme leader du mouvement d'objections a été transfé au Royaume-Uni.
[cxvi] Robert Baer, *La Chute de la CIA : les mémoires d'un guerrier de l'ombre sur les fronts de l'islamisme*, Folio document, 2003, p. 136-137, Trad. de l'américain par Daniel Roche, *See No Evil*, 2001.
[cxvii] Claude Delesse, « Renseignement, contre-intelligence et intelligence économique : des questions convergentes », in Gérald Arboit (Dir), *Pour une école française du renseignement*, Ellipses, CF2R, Paris, 2014, p. 137-166 »,
[cxviii] Adapté de Henri Kissinger, *L'Ordre du Monde*, Fayard, Paris, 2014.
[cxix] Philippe Baumard, *Le Vide stratégique*, Paris, CNRS Éditions, 2012, p. 17-18.
[cxx] Luc Vinogradoff, « Edward Snowden : « La NSA met le feu à Internet, vous êtes les pompiers qui peuvent le sauver », *Le Monde*, 10 mars 2016.
[cxxi] John Mclaughlin (directeur adjoint et directeur intérimaire de la CIA de 2000 à 2004), « Is the new Patriot Act making US safer ? », 21 juin 2015, ozy.com ; Marc Lowenthal and Ronald Marks, *Is U.S. Intelligence analysis as good as it gets ?, warontherocks.com*, 25 octobre 2015.
[cxxii] Philippe Baumard, *Le Vide stratégique*, Paris, CNRS Éditions, 2012, p. 17-18.
[cxxiii] Shane Harris (correspondant de Daily News sur les questions de sécurité nationale américaine), « D'Edward Snowden ou de celui qui l'a recruté à la NSA, lequel des 2 ment ? En voyant le biopic d'Oliver Stone, la réponse vous perturbera peut-être », *The Daily Best*, 20 septembre 2016, atlantico.fr.
[cxxiv] Jacques Follorou, *Op. cit.*

Note de lecture

NSA, l'histoire de la plus secrète des agences de renseignement

Claude Delesse - Tallandier - 2016

À l'heure où l'Amérique est bousculée par la volonté populaire d'un changement profond, ceux qui suivent les questions de renseignement doivent se poser des questions sur l'instrumentalisation possible de l'agence nationale de sécurité américaine, la NSA, dont les abus et dérives ont été largement exposés par les médias et les réseaux sociaux depuis 2013[1].

« *NSA, l'histoire de la plus secrète des agences de renseignement* » permet de plonger dans l'univers fascinant et inquiétant du renseignement d'origine électromagnétique (*SigInt*) ; et de mieux percevoir les missions, le fonctionnement, les rouages, les collusions et alliances, les dérives et préoccupations de cette institution créée en 1952 sous la présidence Truman.

Replacées dans les contextes historiques tant internationaux qu'étatsunien, les actions de cette agence de l'ombre, surnommée « *No Says Anything* » ou « *No Such Agency* », sont décrites au fil du temps. De son émergence aux luttes contre les phénomènes terroristes et contre la criminalité organisée, elle a connu maintes crises et supporté divers conflits tels que les guerre de Corée, du Vietnam, d'Afghanistan et d'Irak. Service régalien et instrument de souveraineté depuis des décennies, 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. Dirigée par un haut gradé militaire secondé par un civil, elle fait partie des dix-sept agences de renseignement américaines. « Défendre la nation et sécuriser le futur, telles sont ses missions. Concrètement, il lui incombe d'une part d'« Intercepter, collecter – y compris par tous les moyens clandestins – et déchiffrer les transmissions étrangères d'origines électromagnétiques ».

D'autre part il lui faut protéger l'information et les systèmes vitaux de sécurité nationale (*Information assurance*). Espionne insatiable et cryptologue hors pair, elle est obnubilée par la domination technologique, la maîtrise de l'information et la dominance informationnelle, enjeux fondamentaux de suprématie et quête permanente menée avec la complicité du complexe militaro-industriel et des firmes *High-tech*. Mais, demeurer à la pointe des capacités de détection ne garantit pas forcément le traitement à temps des signaux collectés et la compréhension des menaces. La NSA fortement critiquée pourrait-elle gagner en efficience grâce aux experts (mathématiciens, linguistes,

hackers, *managers*, etc.) attirés par patriotisme ou par goût des défis technologiques ?

Le texte, très documenté, se situe hors de toute polémique mais propose toutefois des pistes de réflexion plus que jamais cruciales. Il est uniquement construit à partir de sources ouvertes. Articulé autour de quatre parties, il est entremêlé d'anecdotes et évoque quelques traits de personnalité des hauts gradés qui ont dirigé l'agence (une biographie complémentaire figure en annexe). Une première partie consacrée à l'histoire de la NSA remonte bien avant la deuxième guerre mondiale, couvre la période de la guerre froide puis la transformation des menaces jusqu'aux attentats du 11 Septembre 2001. Les deux parties suivantes sont consacrées à la description du fonctionnement de la NSA et à ses dérives, difficilement contrebalancées par la pseudo vigilance du Congrès et du département de la justice voire par les médias souvent accusés d'allégeance au pouvoir exécutif, à quelques exceptions près.

Depuis la fin des années quatre-vingt-dix, on est au courant de l'existence d'« Échelon », perçu comme un réseau planétaire d'interception des télécommunications orchestré par la NSA en collaboration avec les agences *SigInt* britannique, canadienne, australienne et néo-zélandaise : GCHQ, CSTC, ASD, GCSB. Néanmoins, nous n'avons qu'une connaissance partielle des programmes démentiels mis en œuvre aux titres d'une surveillance planétaire, totalitaire, indiscriminée et des luttes cyber. Ces dernières s'inscrivent dans les guerres du futur : guerre économique, guerre technologique, guerres de l'information, cyberguerre. La NSA a fort à faire face à de redoutables adversaires, au premier rang desquels figurent la Chine et la Russie.

Le *tsunami* médiatique et la résonance qui a submergé les réseaux sociaux consécutivement aux révélations de 2013 auraient tendance à s'essouffler. Pourtant une plus grande vigilance serait de mise. « Que fait la NSA » ?, « Que deviennent nos données ? », « Comment sont-elles traitées et stockées ? », « À qui servent-elles ? » doivent demeurer des questions ouvertes, livrées à la curiosité d'académiques, déplorablement peu nombreux, de quelques journalistes pugnaces et d'esprits ou d'associations libertaires qui défendent les droits privés, les libertés civiles et d'expression. Autant rappeler que la maîtrise du secret est la quintessence des services de renseignement.

Or, celle-ci risquerait s'accentuer dans les mois à venir sous pression de la Maison Blanche rendant ainsi l'équilibre entre libertés et sécurité encore plus difficile, ce qui ne pourrait qu'accentuer le différend entre la société civile et l'État américain. Et, que faut-il craindre quand les géants *High-Tech*, les maîtres du *Data mining* et des *Big data* interfèrent au nom de leurs sacro-saints intérêts et de leurs ambitions lucratives ? La NSA a la peau dure. Ses dirigeants sauront-ils ou pourront-ils raison garder et fournir uniquement le renseignement utile pour protéger le monde de demain ? Avec le risque d'échouer, comme en 2001…

Note

[1] Cf : Quelques pistes de réponses : Jenna McLaughlin, Zaid Jlani, « We Asked NSA's Privacy Officer if U.S. Spying Powers are Safe With Donald Trump. Here's What she Said », TheIntercept.com, 24 mars 2016.

Démons et merveilles du « prédictif » : une bonne fois pour toutes...

Xavier RAUFER

Notre monde physique est balisé et connu – mais l'autre, le numérique ?

La seconde guerre mondiale s'achève et Paul Valéry pré-voit ainsi le monde à venir : «Toute la terre habitable a été de nos jours reconnue, relevée, partagée entre les nations. L'ère des terrains vagues, des territoires libres, des lieux qui ne sont à personne, donc l'ère de libre expansion est close. Plus de roc qui ne porte un drapeau ; plus de vides sur la carte ; plus de région hors des douanes et hors des lois ; plus une tribu dont les affaires n'engendrent quelque dossier et ne dépende, par les maléfices de l'écriture, de divers humanistes lointains dans leurs bureaux. *Le temps du monde fini commence* (...) Le monde auquel nous commençons d'appartenir, hommes et nations, n'est qu'une figure semblable du monde qui nous était familier. Le système des causes qui commande le sort de chacun de nous, s'étendant désormais à la totalité du globe, le fait résonner tout entier à chaque ébranlement ; *il n'y a plus de questions finies pour être finies sur un point.*»

En d'autres termes, Valéry décrit un «*Nomos* de la terre» l'ordre spatial de la Grèce antique réinventé par Carl Schmitt : «Le *Nomos* règle, pour tous les citoyens de la ville, le partage de ce qui leur est destiné»[1] ; telle est l'œuvre de Némésis, déesse qui répartit entre les dieux et les hommes.

Le monde fini de Valéry dure quarante ans : dès 1985, l'ordre planétaire se fragmente et le *Nomos* tourne au *Chaos,* quand apparaissent les «zones grises» au Sud du monde. Encore n'est-ce rien à côté de ce qui attend la Terre - car peu après, apparaît un continent (numérique) vierge et inconnu, le cybermonde.

Et quel continent ! Ecoutons son chantre, John Perry Barlow, président de la *Electronic Frontier Foundation* (et parolier du groupe de rock californien les *Grateful Dead)* : «Un continent si vaste qu'il pourrait

être illimité... Un monde nouveau que toute notre avidité n'épuisera sans doute jamais ; offrant plus d'opportunités qu'il n'y aura jamais d'entrepreneurs pour les exploiter ; un lieu où les malfaiteurs ne laissent nulles traces ; où, mille fois volés, les biens appartiennent toujours à leurs légitimes propriétaires... Où seuls les enfants se sentent vraiment chez eux...» («Déclaration d'indépendance du cyberespace», Davos, 1996).

Retour à aujourd'hui.

Frénétiquement, le présent cybermonde cherche à se comprendre lui-même. Il est vrai que ce monde-là exige de l'ordre : ses concepteurs, architectes et opérateurs viennent d'un milieu mathématique stable, ordonné et prédictible, où 2+2 font toujours 4 ; depuis toujours, le calculable est d'ailleurs leur refuge face au chaos du monde.

Notre «société de l'information» (car reposant sur l'informatique) se sait toujours incapable de maîtriser (modéliser) l'incertitude, l'à-venir. Mais elle éprouve l'urgent besoin d'annoncer (au moins) qu'elle le pourra bientôt ; que cette invention est imminente. Rien de neuf sous le soleil : dans cette société nerveuse et fragile, tout autant qu'à l'âge d'Aristote, l'angoisse de l'homme tient toujours à ce qu'il ne connait pas, ne peut connaître, l'heure de sa propre mort.

Même fictivement, cette société doit donc prétendre qu'elle surmontera l'angoisse humaine de l'avenir ; qu'elle maîtrisera demain l'in-calculable. D'où son obsession de la modélisation, de l'intégrale compréhension du monde. Chaque jour, le cyber-tam-tam annonce ainsi une nouvelle «solution» prédictive... l'état de santé... la finance... la toxicomanie... la police... nous verrons cela plus bas ce que vaut ce «solutionnisme».

En attendant, le *Big data* est la panacée ! Détecter et analyser les signaux émis par les hommes... Découvrir et exposer les *patterns* (modèles) inconnus : il y a tant de données inexploitées, partant desquelles élaborer ces modèles inédits. Tout analyser, tout corréler, tirer du sens de tout : telle est la présente ivresse du cybermonde. Elle est compréhensible : le champ de la prédiction ne grandit-il pas à mesure qu'on exploite de nouvelles bases documentaires, elles-mêmes toujours plus interconnectées ? Les limites à l'analyse prédictive ? On ne les voit pas.

D'où vient ce tam-tam prédictif ? De Silicon Valley

Quand elle se protège, la «société de l'information» se rue systématiquement sur des défauts et failles des systèmes numériques, sans trop s'interroger sur le système lui même. Dans une culture d'ingénieurs, le système est bon s'il fonctionne bien. Nul besoin de s'interroger sur ses fins dernières ; d'aller voir derrière le décor. Or bien sûr, les origines et finalités du cybermonde proviennent de la fort suspecte «Silicon Valley». Toutes deux méritent qu'on y aille

voir de près ; faute de quoi, on posera *ad vitam æternam* des rustines sur le pneu crevé - sans chercher qui a répandu des clous sur la route.

Or dès l'origine, Silicon Valley fréquente - avec délices - des espions, des mafieux, des fraudeurs - on l'a même créée pour ça : «Silicon Valley a grandi comme une filiale de l'armée et du renseignement des Etats-Unis» (cf. Malcomson, bibliographie). On verra plus bas que même des icônes du cybermonde ont trempé là-dedans.

Cela, les agents du système l'admettent eux-mêmes : « S'ils travaillent dur à inventer nos futures technologies, nombre d'entrepreneurs de Silicon Valley négligent les risques sociaux, légaux, éthiques et sécuritaires que leurs créations font courir à la société… Les développeurs de Facebook ont longtemps eu comme slogan 'Foncez et cassez tout au passage' (*move fast and break things*), devise affichée au siège de la société… Marc Zuckerberg renchérissant : «si vous ne cassez jamais rien, vous ne foncez pas assez»[2].

Et les mafieux ? Ils sont là dès la décennie 1970. Alors, les réseaux d'ordinateurs communiquent par les lignes téléphoniques existantes, grâce à une gamme de tons sonores (chuintements caverneux familiers aux usagers des premiers modems) Vite, de jeunes aveugles apprennent le sens et l'usage de ces tons - donc les failles du système : ces proto-*hackers* communiquent ainsi gratuitement entre eux, mais peuvent aussi écouter les échanges des autres. Ils s'associent alors à des *Geeks* pour fabriquer de primitifs modems et ouvrir à des clients cet univers en marge. Vendues une centaine de dollars, ces «petites boîtes bleues» piratent le système téléphonique Bell qui en vaut, lui, des centaines de milliards.

Qui fabrique ces petites boîtes bleues ? Dans les garages d'anonymes villas californiennes ou dans des clubs libertaires nommés «*People' computer company*» ou «*Homebrew computing club*», de juvéniles et chevelus post-Hippies ; parmi eux, Steve Wozniak et Steve Jobs, futurs fondateurs d'Apple (Wozniak l'avoue, 4/10/1984, dans un discours à la *Colorado School of Mines*). Qui sont les principaux clients des «petites boîtes bleues» ? Les mafieux de Las Vegas («When Vegas mobsters bought blue boxes from phone freaks», *Esquire*, cf. bibliographie).

Pour conclure sur ce point, mieux vaut garder en mémoire qu'outre ces douteuses fréquentations, que «Silicon Valley» qualifierait sans doute d'erreurs de jeunesses [3], la «Vallée» possède aussi, aujourd'hui encore, sa propre idéologie libertarienne *bottom-up*, auto-organisation d'individus, d'actions et de marchés, qu'elle juge bien supérieure aux vieilles régulations paternalistes *top-down*, avec leurs contraignants cadres, catégories et conventions. Le «gouvernement algorithmique» dont rêve «Silicon Valley» est fondé sur l'exploitation des justes données du *Big data*, sur ce que chaque individu fait en

réalité ; donc, dit-»elle», moins paternaliste, injuste et déformant que nos actuelles institutions.

Ce cyber-pouvoir est défini - de façon plutôt inquiétante - par Mme Antoinette Rouvroy, chercheuse en philosophie du droit à l'Université de Namur *(Mediapart, 25/05/15, bibliographie)* : «Nourri essentiellement de données brutes, signaux infra personnels et a-signifiants mais quantifiables ; opérant par configuration anticipative des possibles plutôt que par règlementation des conduites ; et ne s'adressant aux individus que par voie d'alertes provoquant des réflexes, plutôt qu'en s'appuyant sur leurs capacités d'entendement et de volonté». En bon français : de la manipulation à grande échelle.

Silicon Valley, des sommets du lyrisme utopique à la froide réalité du fric

Chers ingénieurs, journalistes et politiciens, ne croyez pas à la neutralité du système numérique (soi-disant voué au bien de l'humanité) rayonnant depuis la Silicon Valley. Ne croyez pas ces cyber-évangélistes et leur chatoyant «solutionnisme». Car la superstructure de Silicon Valley n'est finalement qu'un copier-coller de la bourgeoisie, dont Karl Marx a ainsi défini le rôle historique : « Partout où elle a conquis le pouvoir, elle a foulé aux pieds les relations féodales, patriarcales et idylliques... Elle a noyé les frissons sacrés de l'extase religieuse, de l'enthousiasme chevaleresque, de la sentimentalité petite-bourgeoise dans les eaux glacées du calcul égoïste» *(Manifeste du Parti communiste)*.

Et ce qu'elle propage en prétendant lutter contre le paternalisme d'hier n'est rien d'autre que son paternalisme à elle, celui qu'elle imposera demain : «bons» comportements, modes vertueuses, bienséance, hygiénisme, etc.

Retour à aujourd'hui : tout mesurer, tout contrôler, tout prévoir par *le Big data* ? Difficile et surtout, dangereux. Creusons. Sous les grandes proclamations, on trouve : domination, prédation, exploitation, aliénation, opacité. L'addiction numérique, aussi ; la fascination pour les écrans et les algorithmes - tout sauf neutres et perpétuant plutôt les inégalités sociales - on le verra plus bas. Enfin, une idéologie vide de politique, un idéal d'administration *high-tech*, de gestion anonyme et un management d'autant plus féroce qu'il affecte d'être *cool*.

Concluons en citant Michael Brenner, l'un des rares intellectuels américains à toujours «*think out of the box*» (*cf. bibliographie*) : «Oubliez les slogans *(de Silicon Valley, Ndl'a)* et leurs utopies inouïes ; oubliez le culte de l'électronique *high-tech* ; oubliez les fascinantes nouvelles frontières. En fin de compte, le seul étalon du succès, de la réputation, du statut social - et des plaisirs que procurent l'argent et l'amour - sont prosaïquement : le fric et les *stock-options*».

Silicon Valley dit «prédire» – mais qu'est-ce que la prédiction ?

«Prédire» est le maître-mot de Silicon Valley. Et policer la cité est clairement stratégique. Mais qu'est-ce que prédire en matière stratégique ? Tout remonte à la seule grande bataille navale de la première guerre mondiale, celle du Jutland[4]. Au bilan, la *Royal Navy* constate que son artillerie n'a mis que 3% de coups au but. Pour préciser les futurs tirs («*fire control program*»), la *Navy* forme des calculateurs. Ces premiers «*computers*» humains (de là provient le mot) doivent pré-voir, anticiper les mouvements des navires ennemis, en intégrant l'inertie temporelle, du moment où l'obus (ou la torpille) est tiré à celui où il touche sa cible.

Même problème lors de la seconde guerre mondiale. Encore neutre en 1940, Washington veut cependant aider la Grande-Bretagne lors du «Blitz» ; il ne peut livrer des armes - mais fournir de la matière grise aux amis est licite. La science balistique américaine optimisera donc l'artillerie anti-aérienne britannique lors de la bataille de Londres. Pour cela, des statisticiens doivent anticiper l'évolution des bombardiers (vols en zigzag, décrochements, etc.) ; prédire leurs mouvements, pour tirer à coup sûr. Dans un champ d'action donné (d'où vient et où évolue l'avion), ils doivent deviner un comportement (où cet avion va).

Solution théorique : *l'anti-aircraft predictor model*. Un système de tir automatique couple des canons anti-aériens à des radars (qui existent déjà). Un ultra-rapide processus probabiliste (le «prédicteur») fournit des données pertinentes (partant de ce que montre le radar) ; le tir «anticipe» donc les mouvements de l'avion et l'abat, sinon à tout coup, mais bien plus sûrement qu'avant.

Norbert Wiener, mathématicien de génie et pionnier de la cybernétique, relève le défi. Sa mission (en anglais) : imaginer «*the mathematics of predicting the movements of hostile airplanes according to probability*»[5]. Avec son collègue Julian Bigelow, ils tentent de modéliser un ensemble de comportements, humains et mécaniques : que se passe-t-il quand un pilote veut éviter des tirs de DCA ? Peut-on comprendre et modéliser les fort complexes interactions homme-machine qui soudain s'opèrent ? La logique opérationnelle de l'esprit du pilote visé est à chaque fois différente, bien sûr. Mais, estime Wiener, l'esprit humain sous tension tend à agir répétitivement et est donc prévisible.

Une machine est donc construite pour stocker et croiser des données sur les possibles figures aériennes du bombardier en vol, les réactions du pilote et les modalités du tir, afin d'obtenir l'anticipation voulue. Le premier «*computer*» - non plus humain, mais *mécanique* - est né. Notons que comme son ancêtre biologique post-Jut-

land, il lui est assigné d'anticiper *à temps* un comportement humain.

D'une seconde à l'autre, la prédiction de la machine est étonnante de précision - mais inutile, car les obus des canons anti-aériens mettent 20 secondes à atteindre l'altitude du bombardier en vol. La prédiction exigée est donc à 20 secondes. Et là, échec irrémédiable. C'est impossible, quelle que soit la puissance de calcul asservie à cette fin. Norbert Wiener abandonne le projet *anti-aircraft predictor model* en janvier 1943.

Depuis et pour l'essentiel, on en est là. La prédiction *réelle* se heurte encore et toujours à la barrière du temps. Nous parlons ici de la *vraie* prédiction : pas de l'hypothèse hasardeuse qu'un individu fera ceci demain, du fait qu'il a fait cela hier. Genre *Amazon* : «ceux qui ont acheté tel livre ont aussi aimé...». Cela n'est en rien de la prédiction mais (en anglais) du «*wishful thinking*».

D'ores et déjà, ces rappels historiques montrent l'audace de prétendre «prédire» un crime, action complexe et d'usage secrète, soudaine ou bien ourdie de longue date et impliquant deux humains minimum - voire bien plus.

Prédire en puisant dans le Big data ?

«Silicon Valley» balaie ces objections en affirmant qu'aujourd'hui, tout a changé, du fait du *Big data*. Le progrès technologique a doté l'humanité d'un immense, peut être d'un illimité, vivier de données susceptibles de multiples réutilisations, sans rapport avec leur collecte initiale. L'informatique permet de capter, conserver et traiter ces données, puis d'y repérer des corrélations.

Ce stock disponible, dit «Silicon Valley», est un nouveau, et décisif, facteur de production ; c'est la matière première de demain. «Les algorithmes permettront de faire des prédictions sur la dangerosité des personnes ou leur probabilité de commettre un acte particulier, à partir des *Big data* et des corrélations que l'on peut y trouver», dit ainsi un thuriféraire de la *data science*. Nous y voilà.

Sont-elles précises, ces corrélations ? Non, mais leur multitude compense leur flou. Les prévisions faites à partir de ces données sont elles valides ? Pas forcément, mais dans la *data science*, les erreurs servent : dans un domaine précis de recherche, chaque nouvelle vague de calcul intègre et corrige les fautes précédentes. Ici, disent les *Data Scientists*, pas de corrélations fallacieuses : plus ça va, et plus les prévisions sont précises.

Comme méthode, la modélisation prédictive par voie mathématique-informatique exige un indispensable outil : l'algorithme. La méthode plus l'outil produisent à leur tour le logiciel, qui les associe pour un projet, ou dans un champ, précis. Voyons maintenant si ces divers cyber-ustensiles sont fiables et solides.

Prédire en modélisant – mais qu'est-ce qu'un «modèle» ?

D'abord, écartons ce qu'à l'heure présente, nul logiciel, modèle ou algorithme ne peut accomplir : aucun de ces outils numériques ne peut comprendre, moins encore créer, un concept. Aujourd'hui, nul programmeur ne sait transcrire en code un sarcasme, de l'argot ou un propos cynique.

Venons-en au modèle : il représente abstraitement (dans un ordinateur ou dans sa tête) un processus qui part de ce qu'on sait déjà, puis «prédit» des réponses, ou réactions, à divers cas ou situations. Sorte de maquette facile à comprendre, elle permet d'inférer des faits situés dans l'à-venir. Fatalement, le modèle simplifie un réel infiniment plus complexe : la carte n'est pas plus le territoire que le logiciel n'est la vie vécue d'un être humain.

Qui plus est, les logiciels permettant la *data-science* ne sont pas des forces neutres et inexorables (comme le vent ou les marées) ; ils ne tombent pas du ciel, mais reposent sur les choix effectués par de faillibles êtres humains. Ces «modèles» qui toujours plus guident nos vies et génèrent une crainte religieuse - voire pratiquent l'intimidation mathématique - ne sont trop souvent qu'un ensemble codé de préjugés, de biais et d'incompréhensions. Loin d'éclairer la réalité, ils peuvent finir par l'incarner, suscitant un pseudo-réel qui - miracle ! - justifie les résultats obtenus : on parle alors de modèle autoreproducteur.

Pourquoi ? Tout modèle repose sur le choix humain, conscient ou non, des données à considérer ou rejeter ; *toujours,* un codeur décide de ce qu'on y inclut. Un modèle n'est pas une radiographie, mais porte les opinions, priorités et jugements de valeur de son concepteur, si honnête soit-il. Pour Cathy O'Neil *(cf. bibliographie)*, un modèle est «une opinion nichée dans un ensemble mathématique»

Comment ? Quand on élabore un modèle et que manquent les données exactes à coder sur ce qu'on recherche vraiment, on use de données proches, faisant fonction de… Dans le champ du stratégique ou de la justice, choisir ces ersatz est bien sûr fort politique, voire idéologique.

Concrètement : voici un logiciel aidant la justice à prédire les risques de récidive. Intégrant une masse d'informations sur l'environnement humain et géographique d'un individu, ce logiciel assume forcément que ces faits tirés de son passé seront répétitifs. Or comme codifier des données anciennes n'invente *en rien* le futur, chercher dans ces données *passées* des éléments d'un verdict ne «prédit» rien, mais projette ce passé dans l'avenir.

Pour quel résultat ? Rappel : avant le krach de 2008, tous les modèles d'anticipation des risques financiers assumaient que l'avenir de Wall Street ressemblerait à son passé :

on a vu le travail... Bienvenue dans la «face noire du *Big data*».

Modéliser exige des algorithmes – mais qu'est-ce ?

La capacité algorithmique, c'est la «possibilité de produire, à partir d'un ensemble de données, une fonction calculable permettant de comprendre, caractériser, expliquer ou *prédire* l'état courant ou *futur* des données capturées». On parle ainsi d'algorithmes, de modèles, de technologies *prédictifs*. (cf. *Archives de philosophie du droit*, bibliographie). En tout cas, cette suite d'opérations propose, selon diverses formulations :

- un moyen prouvable de résoudre un problème,
- une intermédiation sociale irréfutable entre un problème et une solution,
- ou encore, permet de résoudre de façon non-réfutable des problèmes communs.

Forcément, l'algorithme standardise et simplifie *(inconvénient)* mais à la vitesse électronique *(avantage)*. Toujours en apprentissage, il peut à tout instant produire une simulation «en information pure et parfaite, d'une situation réelle dont l'information est imparfaite et incomplète». Suivons cette étude des *Archives de la philosophie du droit* : «Les exceptions coûtent cher dans le code... La performance économique de la rente des MEAs *(Modèles Economiques Algorithmiques)* est directement dépendante des effets d'échelle et d'éventail que l'algorithme peut produire. C'est justement parce que ces MEAs peuvent s'absoudre des 'contextes' locaux, que leur avantage de coût absolu est si important.»

Décodeur : l'algorithme fonce dans le tas et rabote ce qui dépasse. Puisant sans cesse et à toute vitesse dans un flux immense et continu de corrélations associant des millions d'individus (grands nombres fournis par le *Big Data*), à des myriades de lieux, contacts, constantes et comportements, il élabore des modèles probabilistes affinés par apprentissage.

Exemple : pour une étude de consommation, l'algorithme créera et affinera (par voie statistique) des cibles commerciales, en calculant les traces qu'elles laissent sur Internet. D'où, disent les *Data Scientists*, sa capacité à *prédire* les comportements individuels tout comme les risques de sécurité. Aujourd'hui les algorithmes opèrent dans les domaines cruciaux de l'existence humaine : santé, amour, culture, finance, transports, etc. Ils dominent déjà :

- Le monde de la popularité (mesures d'audiences) ;
- Les classements de l'information (cyber-méritocratie) ;
- Les mesures de réputation (réseaux sociaux, personnes et produits) ;
- Le domaine des prédictions comportementales (études de consommation).

Mais ces algorithmes ne tombent pas de la lune et ne surgissent pas par génération spontanée : ils ont des créateurs (informaticiens, *data scientists*) et des commanditaires (les titans de la «Silicon Valley» qui en usent massivement). Bien plutôt, ces algorithmes sont (pour le moment) l'arme absolue de ces derniers, leur permettant, si besoin, de manipuler, contrôler et intimider ceux qu'ils veulent marginaliser ou de détruire («*disruption*»). Ainsi, disent les critiques, un algorithme n'est guère qu'une opinion formalisée par codage, transformée en processus automatisé de décision - pas la vérité du Bon Dieu.

Aujourd'hui, des algorithmes choisissent parmi les candidats à un emploi ; évaluent nos capacités de crédit et les risques de récidive de détenus. Est-ce sans risque ? On a vu que ces outils numériques n'étaient jamais neutres - mais sont-ils loyaux ? Là encore de forts doutes existent. N'en exposons qu'un, avant d'entrer dans le vif du sujet.

Récemment (*New York Times International*, 3/08/2016, *bibliographie*) des défenseurs des libertés civiques ont saisi la Cour suprême du Wisconsin : un audit du logiciel évaluant les risques de récidive des détenus révélait des verdicts biaisés en défaveur des Noirs dans 40% des cas ; les Afro-Américains se voyant constamment affecter un taux de récidive future deux fois supérieur aux Blancs.

Ce logiciel n'aidait pas la justice, il créait de la discrimination. La Cour suprême du Wisconsin a donc tranché : désormais, un algorithme ne décidera plus seul d'une mise en liberté provisoire ou d'un maintien en prison. Et ce logiciel devra afficher clairement son taux d'erreur réel. Mais dans le monde magique de l'Internet, qui a cette prudence ? Pas grand monde, on va le voir.

Police et justice «prédictives», vraiment ?

Il existe, nous chantent (en 2015) des médias naïfs ou manipulés, des logiciels portant sur la «criminalité prédictive» ; d'ores et déjà en Europe (Allemagne, Suisse) ces logiciels servent «à déterminer les risques de délits, les lieux d'infractions, le mode opératoire et le professionnalisme des auteurs d'infractions». Le tout, en mode conte de fées - voire publicité rédactionnelle : «Et si l'on pouvait prédire où et quand auront lieu les prochains crimes et délits ? Cela ressemble à un scénario hollywoodien mais aux Etats-Unis, c'est déjà la réalité. Cela s'appelle la police prédictive. Des scientifiques, des entreprises, établissent les futures cartes de la délinquance en utilisant des algorithmes, des formules mathématiques... Certaines villes vont même plus loin et disent prédire, non pas où auront lieu les crimes, mais qui va les commettre». *(TV News - 29/12/2015, bibliographie).*

Mieux ! Microsoft a développé un logiciel sachant «prédire le futur» et dire si un criminel récidivera dans les six mois. Il dit juste dans 91% des cas... Microsoft a beaucoup investi dans le développement des technologies prédictives. *(Business Insider, 17/12/2015, bibliographie)*

L'enthousiasme est contagieux : déjà, *Mediapart (20/05/2015, bibliographie)* a annoncé que le ministère français de l'intérieur se lance dans la police prédictive ; qu'il développe «un projet d'analyse et de prédiction de la criminalité», à partir d'une «démarche de renseignement criminel qui consiste, à partir d'une compréhension de la criminalité, à anticiper les phénomènes», tout cela, pour «prédire l'apparition des phénomènes criminels». Comment fonctionne ce «Predpol à la française» (*Big data* plus algorithmes prédictifs)? Le modèle est «basé sur les infractions constatées entre 2008 et 2013. S'il est validé et se vérifie sur les faits de 2014, nous le projetons sur l'année 2015».

Mais ces myopes journalistes et promoteurs du «Predpol à la française» ne semblent pas avoir repéré que la plupart des articles sur les technologies prédictives émanent d'une unique boîte de com' nommée «*Fusion*». Lisez les articles vantant la «police prédictive» : on y trouve des phrases comme «*according to a video discovered by Fusion*». Voyons ce que cette société américaine nous dit d'elle même (dans sa langue). Fusion produit du «*high impact digital advertising*» ; elle sait placer ses contenus «*within the heart of editorial content*»... «*We tell the most impactful stories... we create the most impactful conversations*» ajoute-t-elle, fière de rouler des journalistes trop pressés, se ruant sur des sujets tout prêts - et gratuits - sans s'étonner plus que cela du cadeau.

Avis à ces journalistes : qu'ils visitent le site de *Fusion* «*The media brand for a young, diverse and inclusive world*» ils y découvriront les habits neufs de la bonne vieille pub' rédactionnelle.

Après les miroirs aux alouettes médiatiques, le fond de l'affaire. En soulignant d'abord que l'idée de filtrer par voie de modélisation des millions de données sur de bénignes incivilités, permette de prévenir des crimes graves est, à ce jour, hautement hypothétique.

Voyons ce que disent de vrais experts ès-informatique. Ils sont moins fascinés que ces journalistes et politiciens qui, vivant trop souvent en symbiose, se contaminent les uns les autres. Ces experts observent que les logiciels de prédiction criminelle ne font qu'agréger et analyser des faits criminels passés puis calculent, heure par heure et géographiquement, où les crimes «doivent» se commettre ; ils les traduisent alors en «points chauds» (*hotspots*) sur la carte. Comme d'usage, Predpol & co. «prédisent» l'avenir à partir du passé.

Maintenant, souvenons-nous de ce nous avons dit du codage d'ersatz, faute de données pertinentes : si l'on code les seuls

crimes sérieux dans un logiciel Predpol ou analogue, on manque de grain à moudre, l'échantillon est trop réduit - donc peu ou pas de *hotspots* sur la carte. Il faut alors y inclure des délits, actes asociaux ou incivilités, selon une lecture biaisée de la fameuse théorie du «carreau cassé» de James Q. Wilson - en réalité bien plus subtile.

Selon cette simplette lecture, réprimer les délits permet de prévenir les crimes. Mais en fait, la standardisation étouffe statistiquement le logiciel : en principe créé pour cibler les crimes, il finit par ne «voir» que les incivilités.

Seconde critique : le côté bonneteau, «à tous les coups on gagne» ou prédiction auto-réalisatrice de Predpol & co :

- Predpol signale un *hotspot*, un policier s'y rend. Une infraction s'y commet, Predpol a raison. Pas d'infraction : Predpol a raison aussi, car le déplacement du policier l'a empêchée.

- Predpol signale un *hotspot* mais nul policier ne se rend sur les lieux : Ce policier apprend alors qu'une infraction s'y est commise : Predpol avait raison ! Rien n'arrive, rien n'est enregistré - Predpol n'avait pas tort.

Essai de Predpol à Oakland (Cal.) ville à majorité Noire. Les *hotspots* sont tous dans des quartiers noirs où les policiers passaient déjà leur temps. Predpol valide bêtement ce que la police fait déjà - mais «oublie» les quartiers blancs de la ville, où se consomme pourtant plus de drogue qu'ailleurs.

A Los Angeles, (2e force de police du pays, après New York City), quand les policiers arpentent les *hotspots* où ils allaient déjà avant, ceux-ci deviennent *encore* plus «chauds» ! (Prophétie auto-réalisatrice).

Troisième critique : Predpol réinvente l'eau chaude, prédit des banalités. Car tout policier sait que dans la criminalité des rues, le «gibier» s'adapte : quand la police multiplie les descentes dans un quartier ou sur un *hotspot*, le comportement des habitants et des criminels évolue. Or avant Predpol, les policiers n'agissaient pas au doigt mouillé. Et le fait d'être dirigés par des algorithmes les déresponsabilise, les démoralise. Comme ricane un cadre de la police de Burbank (Cal.) «Allez signaler à un gars qui pêche depuis vingt ans où il y a du poisson…».

Mêmes doutes sur la justice prédictive : les craintes s'accumulent sur la force normative de l'algorithme. Car si la justice d'un Etat de droit jauge la gravité du crime et les remords du malfaiteur ; le logiciel, lui, n'intègre *que* les données biographiques *passées* de celui dont il évalue le risque.

Quel destin pour un détenu à qui un logiciel «prédisant» la récidive (*automated risk assessment tool*), et non un juge, rejette la demande de libération conditionnelle ? Ne verra-t-il pas ses demandes sans cesse rejetées, hors de toute étude de son parcours

personnel ? Pire, la machine ne prendra-t-elle pas ce détenu comme variable d'ajustement de la population incarcérée ?

«Prédictif» : qu'est ce qui «marche» aujourd'hui ?

Les logiciels de type Predpol, pas trop : Richmond (Cal.) n'a pas renouvelé son contrat de trois ans, car la municipalité n'y voyait pas de baisse réelle des crimes sérieux. Burbank ne l'utilise plus car, disent les policiers locaux, ils n'ont pas besoin qu'un logiciel leur apprenne ce qu'ils savent déjà. Donc en Californie (où tout a commencé) le doute s'installe.

Les logiciels d'analyse des comportements anormaux («*Behavioral Recognition Systems*») semblent plus fiables car ici, considérer les précédents est pertinent. Un individu tourne autour d'un bâtiment et tente d'ouvrir les issues de secours... Dans une gare, un ivrogne titube trop près des rails... Des logiciels pré-curseurs peuvent «comprendre» de telles situations et ainsi, prévenir des intrusions ou des chutes sur la voie ferrée.

Voyons maintenant ces systèmes face à la menace terroriste. A ce jour, l'échec y est total. Depuis vingt ans, Washington dépense des fortunes à imaginer des «*watch lists*» efficaces de terroristes - pas de *futurs* terroristes, mais d'individus *déjà* actifs. Mais quels sont les symptômes d'un basculement dans la terreur ? Nul n'en sait rien - ni même d'abord, si ces symptômes existent. Or, quand gérer le présent est déjà si ardu, comment capter le futur ? Ce que la phénoménologie, discipline philosophique férue de temporalité, nomme le «domaine du possible» ?

Concrètement : comment repérer *à temps* Larossi Abballa[6] parmi dix mille «radicalisés» ? Aujourd'hui encore, le Renseignement intérieur français n'a pas grande compétence en matière d'anticipation (décèlement précoce). Certes Abballa multipliait les courriels inquiétants (*J'ai soif de sang... Dieu m'est témoin... Anéantissons les infidèles*) mais maints fanatiques disent de même, et parmi eux, sans doute y en a-t-il autant que de tels propos défoulent, que d'autres que cela excite.

A ce jour, le modèle antiterroriste prédictif est bel et bien hors de portée. Nul logiciel n'existe, qui permette de retrouver l'aiguille terroriste dans la meule de foin des radicalisés. De même, dans un domaine proche, n'a-t-on jamais pu concevoir un efficace système numérisé de prévention des suicides.

Pour conclure, élargissons notre propos. La prédiction stratégique est toujours fort difficile. Récemment, voici le «Brexit», que tous les bourgeois progressistes, tous les bobos libertaires d'Europe et alentours, qualifiaient de «crime». A la clôture du vote, 84% des parieurs des sites de jeux en ligne britanniques voyaient vaincre le «Remain».

Le «Brexit» a assommé la City de Londres, les politiciens et médias (désormais comme en France, un symbiotique hybride), plus les services spéciaux américains, fétichistes du *high-tech*. Lugubre, une agence de presse lamentait sa «difficulté à prévoir de tels chocs, même avec l'aide d'outils comme des algorithmes conçus pour sentir 'vibrer' média sociaux» *(Reuters, 25/06/2016, bibliographie*). Même les algorithmes n'y ont rien pu ! A qui se fier. Ce sera notre conclusion.

Sources de l'étude

• *Ouvrages (ordre alphabétique)*

Conway Flo & Siegelman Jim «Dark hero of the information age: in search of Robert Wiener», Basic Books, US, 2005

Goldsmith Jack & Wu Tim, «Who controls the Internet ? Illusions of a borderless world», Oxford University Press, London, 2006

Goodman Marc «Future crimes», Corgi Books - Penguin-Random, US, 2015

Malcomson Scott «Splinternet - how geopolitics and commerce are fragmenting the World Wide Web», OR Books, US, 2016

O'Neil Cathy «Weapons of math destruction», Allen Lane - Penguin Books, UK, 2016

Turner Fred «From counterculture to cyberculture», University of Chicago Press, US, 2008

Valéry Paul «Regards sur le monde actuel», Folio-Essais, 1994

Wiener Norbert «Cybernetics, or control and communication in the animal and the machine» Wiley, US, 1948

• *Médias, etc. (ordre généalogique)*

L'Expansion - 16/10/2016 «Big data, algorithmes : l'esprit porté par Silicon Valley est totalitaire»

Business Insider - 10/10/2016 «Crime prediction tool may be reinforcing discriminatory policy»

Le Parisien - 12/08/2016 (police prédictive) «Un usage de plus en plus répandu»

Michael Brenner (Blog) - 5/08/2016 «Silicon Valley: inferno / purgatorio / paradiso»

New York Times International - 3/08/2016 «Make algorithms accountable»

Reuters - 25/06/2016 «Brexit baffled punters, pundits and fund managers to the very end»

New York Times International - 22/06/2016 «Identifying future killers out of a sea of suspects»

New York Times International - 28/03/2016 «Studies fail to pinpoint who turns to terrorism»

TV News - 29/12/2015 «Les devins du crime aux Etats-Unis : reportage dans *Envoyé Spécial*»

Business Insider - 17/12/2015 «Microsoft is building an app that can predict criminal behavior»

Tech Insider - 15/12/2015 «Computer algorithms are now deciding wether prisoners get parole»

Libération - 10/10/2015 «En calculant nos traces, les algorithmes reproduisent les inégalités entre les individus»

Tech Insider - 19/08/2015 «Artificially intelligent security cameras are spotting crime before they happen»

New York Times International - 3/08/2016 «When algorithms are guilty of human biases»

Le Monde (Blogs) 27/06/2015 (Internet-Actu) «Police prédictive : la prédiction des banalités»

Mediapart - 25/05/2015 «Gendarmes et industriels imaginent un nouveau logiciel pour prédire le crime» *(même jour)* «L'algorithme n'est pas un système de prédiction mais d'intervention»

Institut Diderot, printemps 2015 «L'avenir des Big data»

Archives de philosophie du droit - (58) 2015 «L'algorithme et l'ordre public»

Science - 04/2014 - «The parable of Google flu: traps in the Big data analysis»

Esquire - 10/1971 «The secrets of the little blue box»

Notes

[1] Martin Heidegger & Eugen Fink «Héraclite, séminaire du semestre d'hiver 1966-1967», NRF Gallimard, 1973.
[2] Cf. Marc Goodman, fondateur du *Future crimes Institute* et professeur à la *Singularity University*, voir bibliographie.
[3] Auto-absolution américaine d'usage baptisée *colorful past*.
[4] Entre la *Grand Fleet* britannique et la *Hochseeflotte* allemande, 31 mai-1er juin 1916, 250 navires engagés ; 14 navires britanniques coulés, 11 allemands ; des milliers de morts ; pas de vainqueur décisif.
[5] Norbert Wiener «I am a mathematician», MIT Press, 1953.
[6] En juin 2016, il poignarde à mort, dans leur pavillon de Magnanville (Yvelines), deux policiers français sans liens directs avec l'antiterrorisme, puis est abattu par des forces d'intervention.

Géopolitique

Améliorer la sécurité des ouvrages hydrauliques dans le contexte sécuritaire actuel

Franck GALLAND

Le violence islamiste qui a frappé la France - et avant elle les Etats-Unis, le Royaume Uni, l'Espagne, la Belgique et une liste encore longue de pays victimes - a eu pour constante de causer terreur et désolation, en occasionnant le plus grand nombre de victimes et en frappant les esprits. C'est une guerre autant meurtrière que psychologique qui est imposée à nos démocraties. Elles n'ont pas choisi ce combat mais doivent pourtant s'y résoudre.

Pour ce faire, elles doivent réapprendre à se battre et à anticiper les coups qui continueront d'être portés sans relâche avant que le vent ne tourne définitivement en leur faveur. Car le combat n'a qu'une issue : une victoire sans concession contre l'obscurantisme et l'inhumanité. Il s'agit pour la France et ses consoeurs de *« vivre ou mourir »*, selon la devise que Théodose Morel avait donnée au maquis des Glières qu'il commandait.

En matière d'anticipation, vu le contexte actuel, il convient d'apporter un regard plus attentif à la protection des ouvrages hydrauliques.

Avant l'attaque de Pearl Harbour, en 1941, J. Edgar Hoover, écrivait qu'*« il a longtemps été reconnu que l'alimentation en eau représente un point de vulnérabilité particulier, offrant des opportunités d'attaque à un agent étranger »*[1]. Le directeur du FBI parlait naturellement à l'époque des menaces japonaises ou allemandes.

Cependant, la situation n'a guère changé depuis. Comme le soulignait en 2010 un rapport du *Congressional Research Service* dépendant du Congrès des Etats-Unis[2], les

ouvrages hydrauliques sont vulnérables et le resteront tant que des mesures spécifiques n'auront pas été mises en place pour leur protection.

Il n'est ici besoin de rappeler l'état de la menace qui n'a jamais été aussi élevé, ainsi que les tragédies qui en attestent ; celles du Bataclan, des terrasses, et de la promenade des Anglais, destinées à occasionner un maximum de victimes, de tout âge et de toute confession.

En revanche, afin d'anticiper le coup d'après, il est utile d'analyser la stratégie suivie par Daech en Irak et en Syrie, en matière d'occupation systématique des ouvrages hydrauliques et d'utilisation du chlore, réactif nécessaire au traitement de l'eau, comme arme de guerre.

Une prise d'otage systématique des ouvrages hydrauliques et l'utilisation du chlore comme arme de guerre

Sur l'Euphrate, en territoire syrien, l'armée islamique a d'abord ciblé le barrage de Baath qui alimente Raqqa et représente 60% de l'alimentation en eau de la Syrie, puis celui de Tabqa, le plus grand de Syrie. Cet ouvrage retient le Lac Assad, et fournit en eau et en électricité la ville d'Alep.

Il en a été de même sur le Tigre, avec le barrage *Saddam* tel qu'il fût appelé à l'époque, et qui est rapidement devenu une source de préoccupation majeure pour le Pentagone, dés sa saisie par l'Armée islamique, le 7 août 2014.

Outre son état de vieillissement avancé, cet ouvrage menace directement la ville de Mossoul, et ses 1,7 millions d'habitants, d'un véritable tsunami urbain en cas de rupture. Ce barrage est par ailleurs d'une importance stratégique, étant le plus important d'Irak et fournissant 45 % de l'électricité de ce pays. Il était donc essentiel que des bombardements ciblés interviennent le plus rapidement possible afin de chasser l'occupant et de redonner le contrôle de l'ouvrage aux peshmergas, ce qui fût fait à compter du 16 août 2014.

Mais au delà de ces ouvrages vitaux, citons également ceux de moindre importance en taille, mais qui peuvent devenir autant d'armes de destruction massive contre les populations situées en aval. Le barrage de Tharthar à Samarra sur le Tigre a ainsi été occupé par Daech d'avril 2014 à l'automne 2015. Celui de Ramadi et de Fallouja sur l'Euphrate le sont encore à l'heure où nous écrivons ces lignes[3].

Les écrits et les actes de Daech témoignent également d'un intérêt accru pour les infrastructures hydrauliques, mais pour d'autres raisons que la puissance qu'offre un barrage.

Sans aborder les problématiques d'empoisonnement d'eau potable qui rappellent le

temps des Croisades, où Saladin, en 1187, avait eu raison des chevaliers chrétiens en polluant systématiquement les puits sur leur chemin et en détruisant les villages maronites qui ravitaillaient les Croisés en eau, ce sont maintenant aux stocks de chlore de focaliser notre attention.

Entre 2006 et 2007, l'utilisation du chlore a clairement été l'une des stratégies déployées par Al Qaeda en Irak dans sa guerre asymétrique contre les forces de la coalition.

D'après les sources de presse de l'époque, citées dans un excellent article du Service de Santé des Armées[4], de janvier à début juillet 2007, la vingtaine d'attentats perpétrés au chlore auraient fait plus d'une centaine de morts et environ 800 blessés et/ou intoxiqués à des degrés très divers.

Ces attentats couplaient des bombonnes de chlore gazeux, gaz plus lourd que l'air, à un explosif puissant, de façon à libérer le toxique en tenant compte du sens du vent, comme durant la première guerre mondiale. Le 22 avril 1915 se déroulait en effet la première attaque chimique de l'Histoire. Elle eut lieu dans le secteur d'Ypres en Belgique et a été menée à partir de chlore, prenant par surprise 15 000 hommes des troupes alliées et provoquant 800 morts, ainsi que de très nombreux intoxiqués à vie souffrant de pathologies respiratoires.

Après le théâtre irakien, depuis le déclenchement du conflit syrien, force est de constater que le chlore gazeux est redevenu un outil de combat. L'Organisation pour l'Interdiction des Armes Chimiques (OIAC) a ainsi dénoncé à plusieurs reprises l'utilisation de ce gaz, utilisé à partir de barils largués par hélicoptères ou couplé à des explosifs.

L'Irak et la Syrie étant des laboratoires à ciel ouvert en matière de guérilla urbaine, notre analyse est qu'il est malheureusement à craindre que ce mode d'utilisation du chlore soit sous peu importé en Europe, comme l'a été la fabrication d'explosifs TATP utilisés au Stade de France, ou comme le seront dans un futur proche les voitures piégées (cf. tentatives récentes avec des bouteilles de gaz).

En réponse à ces nouvelles formes de menace

A la lecture de ces menaces avérées ou supposées, une démarche d'anticipation doit être urgemment mise en œuvre afin d'éviter tout effet de surprise et un désastre annoncé sur rien n'est entrepris.

La première des mesures à prendre viserait à renforcer la sécurité périmétrique des points sensibles des ouvrages hydrauliques (par exemple les salles de contrôle des turbines ou les vannes maîtresses) par de la technologie : détection d'approche périphérique par bornes infrarouge, protection périmétrique des bâtiments par radars de détection, camera mobile pour levée de doute...

Pour le chlore, ce sont les lieux de production et de stockage qui doivent être mieux protégés, tant chez les fournisseurs de réactifs que chez les opérateurs privés et publics en charge de la production et de la distribution d'eau potable. Des moyens technologiques comme ceux exposés plus haut, mais également purement techniques (par exemple une cage de protection les bombonnes de 49 kg) permettent d'y concourir.

Dissuasion, détection et retardement des intrus doivent ainsi devenir les maître-mots visant à atteindre une meilleure gouvernance en matière de sûreté des points vitaux, susceptibles de mettre en danger la vie des populations.

Par ailleurs, les forces de police et de gendarmerie, ainsi que les armées, ne pouvant qu'occasionnellement veiller physiquement à la sûreté de zones aussi étendues qu'isolées, il est nécessaire de renforcer leur dispositif. Dans ce domaine, il faut sans doute pouvoir s'inspirer d'expériences étrangères.

Celle des Etats-Unis est de ce point vue intéressante. Le *Bureau of Reclamation Police*, également appelé *Hoover Dam Police*, a été créé en 1931 pour la protection de ce barrage stratégique situé dans le Névada, à 37 kms de Las Vegas.

Depuis, ses fonctions n'ont pas changé. Elles se sont même vues confortées au lendemain du 11 septembre ; le barrage, ainsi que d'autres ouvrages hydrauliques essentiels d'Arizona et du Névada, étant protégés par du personnel compétent, doté d'outils à même de contrôler en temps réel véhicules et individus qui s'y rendent. Avant d'entrer en fonction, les personnels du *Bureau of Reclamation* passent 12 mois en formation spécialisée sur les ouvrages qu'ils ont à protéger. Ils savent ainsi ce qu'ils doivent surveiller en priorité.

Car le sujet, est bien là. Un ouvrage hydraulique, ou un site classé Seveso, ne doit pas être protégé comme un simple site industriel ou un vulgaire entrepôt. La sécurisation de ces ouvrages critiques, potentiellement dangereux en cas d'acte malveillant, réclame fiabilité, compétence et rigueur sur le « Quoi protéger ? » et le « Comment ? ».

D'où la nécessité de créer un corps de gendarmerie spécialisé sur le modèle du *Bureau of Reclamation*, ou d'adapter au cas des ouvrages hydrauliques et à d'autres sites critiques français, l'exemple de *la Civil Nuclear Constabulary* britannique.

Cette entité créée en avril 2005 a pour fonction d'assurer la sécurité des sites nucléaires civils britanniques, au sein de leur périmètre immédiat, mais également dans un rayon de 5 kms autour d'eux. Les membres de cette unité spécialisée ont, comme la police des transports du Royaume-Uni, les mêmes pouvoirs d'anticipation (capacité de renseignement) et de réponse (usage des armes) pour neutraliser tout adversaire suspecté ou déclaré.

Au delà de la création d'une police pour les ouvrages hydrauliques les plus critiques, il serait également utile de travailler à la possibilité d'associer à ce service de gendarmerie un groupe de précieux auxiliaires que peuvent par exemple être les agents techniques forestiers de l'ONF ; version moderne des anciens gardes des Eaux et des Forêts qui ont été remplacés en 1963. Agents assermentés, ils ont le pouvoir d'établir des procès verbaux et sont les représentants de la police de la nature et de l'environnement. Pourquoi dés lors ne pas leurs demander d'être également attentifs, lors de leurs patrouilles, à la sûreté des ouvrages hydrauliques, situés généralement en pleine forêt ou dans des parcs naturels ?

Au delà des gardes forestiers travaillant pour l'ONF, le même type de réflexion est à étendre aux agents techniques de l'environnement travaillant pour l'Office national de la chasse et de la faune sauvage, les parcs nationaux, ou encore de Conseil supérieur de la pêche.

Enfin, des agents privés de sûreté, spécialisés dans la protection des infrastructures critiques, constitués de personnels formés et compétents ayant quitté les Armées et les services de sécurité de l'Etat, apporteraient une ossature précieuse contribuant à la protection des grands barrages.

Les ouvrages hydrauliques présentant un risque particulier doivent également pouvoir faire l'objet de surveillances spécifiques qu'offrent maintenant de nouvelles technologies comme les drones terrestres et aériens, auxquels on peut ajouter les capteurs de qualité d'eau nouvelle génération, ou les cordes optiques assurant un contrôle préventif sur les bâtiments et ouvrages d'art.

Ainsi donc, c'est un savant dosage entre organisation et compétence humaine, associées à des innovations technologiques qui doivent désormais permettre de mieux protéger les ouvrages hydrauliques critiques face aux nouvelles formes de menaces que la France et l'Europe apprennent à connaître.

Notes

** Franck Galland, Spécialiste des questions sécuritaires liées aux ressources en eau, Franck Galland a été directeur de la sûreté de Suez Environnement et dirige Environmental Emergency & Security Services, (ES)², cabinet d'ingénierie-conseil qu'il a créé en 2010 et qui est spécialisé dans la résilience des villes et de leurs opérateurs de réseaux de vie (eau, énergie, télécom).*
Chercheur associé à la Fondation pour la Recherche Stratégique, son dernier ouvrage, paru en mars 2014 chez CNRS Editions, est intitulé «Le Grand Jeu. Chroniques géopolitiques de l'eau » (préface de Sir Richard Dearlove et de Miguel-Angel Moratinos).

[1] « Water Supply Facilities and National Defense, » J.E. Hoover, Journal of the American Water Works Association, vol. 33, no. 11 (1941).

[2] « Terrorism and Security Issues Facing the Water Infrastructure Sector », Claudia Copeland, Specialist in Resources and Environmental Policy, March 16, 2010.

[3] Cité en page 6 de l'étude « Water as Weapon : IS on the Euphrates and Tigris. The Systematic Instrumentalisation of Water Entails Conflicting IS Objectives », Tobias von Lossow, German Institute for International and Security Affairs, Janvier 2016.

[4] « Attentats au chlore en Irak : utilisation d'un toxique chimique en combat asymétrique ». P. Burnat, C. Renard, F. Dorandeu, C. Lefevre, C. Bodelot, F. Ceppa, F. Fontaine. Médecine & Armées. Revue du SSA. T.38. N°1. Février 2010.

Rubriques et chroniques

Antidiotiques

La prison

Philip DECKHARD

C'est un sujet tabou. Les personnes issues de l'immigration sont surreprésentées dans les prisons françaises. Mais en l'absence de statistiques ethniques, le sujet ne peut pas exister autrement qu'instrumentalisé par les uns ou tu par les autres. Personne ne conteste le phénomène, qui est ancien et n'est pas propre à la France. Mais l'aborder et l'étudier pour en comprendre les causes est mission impossible pour les chercheurs, alors qu'ils peuvent le faire, par exemple, au sujet des Noirs dans les prisons américaines. Est-ce la simple conséquence de conditions sociales, le produit d'un système judiciaire qui serait discriminatoire ? Est-ce, pour reprendre les théories d'un Eric Zemmour, le résultat d'une plus grande propension à la délinquance chez les personnes d'origine étrangère ?

Auteur : Jean-Baptiste Jacquin, « Pourquoi les enfants de l'immigration vont en prison ? », *Le Monde*, 21 octobre 2016.

Contexte : Le 8 octobre 2016, à Viry-Châtillon dans l'Essonne, non loin de la cité de la Grande Borne, haut lieu du crime, quatre policiers font l'objet d'une tentative d'assassinats par une bande d'une vingtaine de personnes munies de cocktails Molotov. L'un des policiers se retrouve dans le coma, très grièvement brûlé. L'émotion est grande. Cet acte criminel et les déclarations imprudentes du ministre de l'Intérieur (« des sauvageons ») déclenche quelques jours plus tard plusieurs semaines de manifestations de policiers, partout en France.

Antidote : Admirons le tour de passe-passe dialectique. Voilà un quotidien qui durant des décennies aura interdit d'aborder la question complexe de la sur criminalité des étrangers et des Français d'origine étrangère, et ce au au nom de la lutte contre le racisme et la xénophobie, puis qui soudain autorise d'en débattre, mais en canalisant le sujet dans des limites étroites, politique-

ment correctes. Avec pour témoins les habituels sociologues du déni du réel (Laurent Mucchielli, Sébastien Roché, Marwan Mohammed, etc.) qui au long de deux pleines pages ne développent qu'une seule thèse : les discriminations sont l'explication. Celles d'une part de l'action de la police et de la justice ; celles d'autre par de la société et des inégalités coupables. Après le déni du réel, son explication lénifiante. Toute autre thèse - culturaliste, politique, démographique, etc. - que celle de la discrimination, donc de l'excuse absolutoire, est ignorée ou plus exactement diabolisée d'emblée avec l'épouvantail Eric Zemmour. Comme disaient les moscovites du temps de l'Union soviétique : « Dans la *Pravda* (vérité) il n'y a pas d'*Izvestsia* (informations), et dans les *Izvestsia* il n'y pas de *Pravda* ».

* * *

Police (A toujours tort)

« Vos recherches montrent (d'ailleurs) que les poursuites pour outrage et rébellion se sont multipliées depuis les années 1990…

Entre 1974 et 2015, le nombre d'infractions à personnes dépositaires de l'autorité publique constatées - outrage, rébellion, violence - a quintuplé, passant de 11 000 à 57 000, quand la délinquance en général n'a pas doublé. Les condamnations pour ces faits sont passées de 10 000, au milieu des années 1990, à environ 18 000 dans les années récentes. Cette croissance procède principalement d'un durcissement délibéré de la réaction policière aux incidents, dans le cadre d'une conception répressive de l'action policière. Ce qui ne peut que contribuer à la détérioration des relations entre la police et les jeunes des quartiers «difficiles», qui sont les principaux auteurs de ces infractions.»

Auteur : René Lévy, sociologue et historien au Centre de recherches sociologiques sur le droit et les institutions pénales (CESDIP), unité mixte du CNRS en cotutelle avec le ministère de la justice et l'Université Versailles-Saint-Quentin-en-Yvelines, interview avec Julia Pascal, « les policiers se voient en éboueurs de la société », *Le Monde*, 25 octobre 2016.

Contexte : voir supra

Antidote : Dans ce contexte tendu, le quotidien *Le Monde* interviewe longuement et avec complaisance ce sociologue dont tout le propos consiste à expliquer que la police est conservatrice, violente, coupée de la population, raciste, etc., en résumé: seule fautive de ce qui lui arrive. La mauvaise foi et le manque de rigueur intellectuelle culminent quand il est question des violences faites aux policiers, aux pompiers et aux gendarmes. L'augmentation des « infractions à personnes dépositaires de l'autorité publique » (outrage, rébellion, violence) ne peut recevoir qu'une seule explication : le « durcissement délibéré de la réaction policière ». A une autre époque, il eut été ques-

tion de dénoncer les « provocations policières ». Autrement dit, si les policiers sont de plus en plus agressés verbalement et physiquement, la raison tient à leur comportement provocateur: une police brutale, toute tournée vers la seule répression, aux pratiques discriminatoires, harcelant les « jeunes », etc. Les policiers seraient donc seuls responsables de ce qu'ils subissent : « Qui sèmerait le vent récolterait la tempête ». L'affirmation est non seulement sans fondement mais choquante. Il s'agit d'une pure opinion militante manifestant un préjugé anti policier, et non d'un constat scientifique étayé par des faits. Par ailleurs, on notera *la perversité* du raisonnement : depuis quand la victime est-elle a priori et systématiquement responsable de ce qui lui arrive ? Ce *renversement de responsabilité* rappelle de biens tristes souvenirs. On croirait entendre les raisonnements malsains et machistes qui imputent parfois aux femmes violées le crime subi et ce en raison de leurs supposés accoutrements légers ou de leurs propos prétendument aguicheurs.

Le sociologue/militant évite d'évoquer une autre explication qui, plus conforme à la réalité, ne rentre pas toutefois dans son parti pris idéologique: les criminels et les délinquants sont devenus *objectivement* plus agressifs et moins craintifs. N'ayant plus peur de l'Etat et de la sanction pénale, ils sont devenus plus audacieux. Mais une telle grille de lecture est incompatible avec l'autre mantra du sociologisme selon lequel « le délinquant est une victime ».

Faits & Idées

Xavier RAUFER & Stéphane QUÉRÉ

Régulièrement dans «Sécurité Globale», nous donnons les chiffres et données récoltés ces derniers mois lors de notre revue de presse internationale ; faits vérifiés et recoupés dans le seul but d'enrichir le débat criminologique. Ces éléments couvrent tous les aspects et variantes du crime et du terrorisme. D'où l'objectif et le nom de cette chronique : donner aux lecteurs des *faits*, pour qu'ils aient (plus et mieux encore) des *idées*.

• Statistiques & données criminelles à l'échelle mondiale

Dans ce chapitre, les faits et données, recueillis à l'échelle mondiale ; au minimum, transcontinentale.

Terrorisme[1]

Selon les deux principales bases documentaires américaines consacrées au terrorisme, ce que ces bases documentaires qualifient de terrorisme (attentats, etc.) advient principalement (80% des faits par elles recensés) dans six pays : Afghanistan, Irak, Nigeria, Pakistan, Syrie, Yémen.

Selon l'une de ces bases («Global Terrorism Database») on compte ainsi mondialement les homicides d'origine terroriste :
2010 : 7 700 homicides
2014 : 43 600
2015 : 38 400

En sortant des statistiques deux attaques exceptionnelles (Oklahoma City, avril 1995 et 11 septembre 2001) le terrorisme n'a provoqué, ces trente dernières années, que moins de 50 morts par an aux Etats-Unis, soit moins que ceux causés par la foudre.

Trafic & exploitation des êtres humains[2]

A l'échelle du monde (estimations faites à l'échelle de 74% de la population mondiale) on estime que 45,8 millions de personnes vivraient en état d'esclavage moderne, dont 15% dans l'Afrique sub-saharienne. 68% de ces esclaves modernes vivent, ou sont découverts, dans dix pays : Bangladesh, Chine, Congo (rep. démocratique du), Corée du Nord, Inde, Indonésie, Nigeria, Pakistan, Ouzbékistan, Russie.

Par esclavage moderne, les auteurs du rapport entendent : prostitution et mendicité forcées, travail forcé (rural, artisanal, manuel, domestique), mariages forcés.

Deux estimations du rapport : il y aurait aux Etats-Unis 11 700 personnes vivant en état d'esclavage moderne ; et 17 500 aux Pays-Bas.

Pédophilie - selon une étude mondiale d'ECPAT (*End Children Prostitution, Pornography and Trafficking*), le profil du pédophile-type a changé : ce sont moins souvent des hommes blancs occidentaux, riches et d'âge mur, mais désormais des touristes asiatiques, des voyageurs d'affaires, des migrants, des travailleurs temporaires, des expatriés - voire des bénévoles employés par des ONG.

Les destinations du tourisme sexuel varient elles aussi : désormais, ce sont d'abord des pays pauvres et isolés d'Europe centrale et orientale, ou d'Amérique latine (Moldavie... Pérou, etc.).

Le nombre des enfants maltraités augmente, lui, depuis 20 ans.

Crimes à l'environnement[3]

Trafic d'ivoire, pillage de ressources naturelles, abattage illicite de forêts, pêcheries illicites, enfouissement de déchets toxiques, abattage de «viande de brousse» ; mines illicites et fraudes au crédit carbone : regroupées sous le nom de crimes à l'environnement, ces infractions ont généré un chiffre d'affaires compris entre 71 et 213 milliards USD en 2014, et entre 91 et 258 Milliards USD en 2015. Une augmentation de + 26% de 2012 à 2015, de 5% à 7% par an.

Contrefaçons[4]

(Statistiques sur 500 000 saisies douanières dans le monde, 2011-2013) Selon l'OCDE et l'Office de l'Union européenne pour la propriété intellectuelle, la valeur mondiale des importations de biens contrefaits était en 2013 de 461 milliards de USD, soit environ 2,5% du commerce mondial.

Pays les plus touchés par la contrefaçon, ces mêmes années : Etats-Unis, Italie, France, Suisse.

Pays producteurs de contrefaçons : Chine (63,2% des produits saisis) ; Turquie, 3,3%.

Dans l'UE, 5% des produits importés sont piratés ; valeur 85 milliards d'euros.

Dans le monde, les médicaments contrefaits représenteraient 10% de l'ensemble de la production médicamenteuse - jusque parfois 60% dans certains pays pauvres. Ils provoqueraient jusqu'à 800 000 morts par an.

Piraterie[5]

La piraterie diminue en haute mer, sauf dans le golfe de Guinée.

Asie du sud-est : au 1er trimestre 2015, 30 attaques de pirates, au 1er trimestre 2016, 6.

Monde : au premier trimestre 2015, 54 attaques de pirates, au 1er trimestre 2016, 37.

1er trimestre 2016 dans le golfe de Guinée : 10 attaques et 44 prises d'otages.

Fraudes, escroqueries, arnaques financières, etc.[6]

En 2015, selon l'ONG britannique Oxfam, le produit brut mondial a progressé de 3,1% ; mais sur terre la répartition de la richesse est toujours plus inégalitaire. Cette année-là, le patrimoine cumulé des 1% des plus grosses fortunes du globe dépasse celui des 99% restants.

Selon le FMI, la corruption représente en 2015 de 1500 à 2000 milliards de USD par an, soit près de 2% du produit brut mondial.

(Enquête Heuler-Hermes) En 2015, 93% des entreprises françaises ont connu au moins une tentative de fraude (77% en 2014). 20% de ces entreprises ont subi plus de 10 tentatives de fraude dans l'année. Les fraudes internes ont concerné 18% de ces entreprises. Sinon, il s'agit de fraudes «au président», provenant de fournisseurs, ou de cyber-crime (vol de données, etc.). 30% de ces entreprises n'ont pas réussi à toutes les déjouer. 46% des entreprises françaises n'ont pas de service antifraude et 68% d'entre elles, pas de plan d'urgence en cas de fraude.

• La criminalité, par continents

Dans ce chapitre, les faits et données, classés par continent (sauf l'Europe).

Statistiques & données criminelles, Amérique latine & Caraïbes[7]

8 des dix pays les plus meurtriers au monde, ceux où le taux d'homicides connu est le plus élevé, sont en Amérique latine ; de même, 47 des 50 villes les plus meurtrières du monde. Sur ce continent, on passe d'effarant sommets - San Salvador, capitale du Salvador, 188 homicides pour 100 000 habitants en 2014 (pays tout entier : 116/100 000), à La Serena-Coquimbo, au Chili, ville la plus sûre du continent où il n'y a presque pas d'homicides, dans un pays au taux fort européen de 3/100 000. Hausses et chutes brutales alternent :
Bogota, Colombie - 1995 : 59/100 000, 2013 : 17/100 000
Medellin, Colombie - 2002 : 179/100 000, 2014 : 27/100 000
Ciudad Juarez, Mexique - 2010 : 282/100 000, 2015 : 18/100 000

Amérique centrale[8]

En 2015, le taux d'homicides tend à baisser dans le pays ; les premières données disponibles montrent qu'on passe de 116/100 000 à 104/100 000. Ca semble se confirmer début 2016 :
Homicides en mars 2016 : 611
Avril : 353
Mai : 351
Juin : 331 (juin 2015 = 677)

Mais voilà qu'une scission advient au sein du fort meurtrier méga-gang «Barrio 18» entre nordistes et sudistes (Barrio Dies Y Ocho surenos), ce qui risque de relancer la tuerie. A voir.

Argentine[9]

Nulle statistique criminelle n'a été publiée dans ce pays, sous la présidence de Mme Cristina Kirchner. Ce sont donc les premières en huit ans.
Toutes infractions, de 2008 à 2015 : + 10%
Homicides : 2008 : 6/100 000 ; 2015 6,6/100 000 (stabilité)
Vols avec violence & à main armée : de 2008 à 2015 : + 9 %
Crimes sexuels : + 78% (changement des lois)
Saisies de cocaïne de 2008 à 2015 : 6 tonnes (- 42% sur 2014), 2008 : 12,2 t.

Brésil[10]

Corruption - en 2009, la banque (d'Etat) brésilienne BNDES a prêté, selon des critères largement clientélistes, 76 milliards de dollars à qui semblait bon à ses dirigeants - plus que ce que la Banque mondiale prêtait au monde entier, au même moment.

Homicides : à Rio de Janeiro, on a compté 2 100 homicides de janvier à mai, + 13% sur les mêmes mois de 2015. Ces dernières années il y a eu dans ce pays plus de 60 000 homicides volontaires par an - un Hiroshima tous les trois ans.

Colombie[11]

de 2006 à 2015, les milices paramilitaires colombiennes, soi-disant vouées à combattre les guérillas révolutionnaires type Farc, *Autodefesas Unidas de Colombia* (AUC), etc., ont fait 332 149 victimes, ainsi réparties :

- 322 504 personnes chassées de leur terres, de leurs maisons,
- 559 agressions sexuelles,
- 560 disparitions définitives,
- 8 194 homicides connus,
- 305 enlèvements,
- 147 cas de torture,
- 82 recrutements forcés.

Ce principalement dans les provinces d'Antioquia, Valle de Cauca, Cordoba, Narino, Choco.

Au premier trimestre 2016, 14 de ces milices étaient toujours actives en Colombie ; présentes dans 146 des 1 100 municipalités de Colombie, elles-mêmes réparties dans 22 des 32 provinces du pays.

Mexique[12]

En juillet 2016 le *Secrétariat exécutif du système national de sécurité publique* (SENSP) annonce pour le premier semestre 2016, 10 301 homicides connus (environ 57 par jour) ; + 15% sur le 1er semestre 2015 (8 979 homicides ; 9 502 homicides au 1er semestre de 2013, début de la présidence de Enrique Pena Nieto).

Taux d'homicides pour 2014 : 16,7/100 000, taux pour 2015 : 16,9/100000.

Un autre système de comptage des crimes (*Semaforo delictivo*) annonce 9 615 homicides pour le premier semestre de 2016 (+ 16% sur le 1er semestre 2015).

Sur ces 9 615 homicides, 5 413 sont dus au crime organisé. 6 homicides sur 10 sont commis à l'aide d'armes à feu.

De son côté encore, l'Institut national de la statistique mexicain annonce 20 525 homicides en 2015, soit un taux de 17/100 000 (20 010 homicides en 2014).

Homicides liés aux Cartels de la drogue : augmentation de + 15% au premier trimestre. Aux trois mêmes mois de 2015, 47% des homicides étaient attribués aux Cartels, on en est à 57% en 2016. Etats du Mexique avec le plus d'homicides :
- Colima : 17,7/100 000
- Guerrero : 14,5/100 000 (le plus d'homicides liés aux Cartels)
- Sinaloa : 8,3/100 000.

Selon *Semaforo delictivo* On compte en mars 2016 1725 homicides, 3158 de janvier-février, soit + 11% sur jan-fev. 2015. Comme on a compté en février 2016 55 homicides par jour dans le pays, le Secrétariat à la sécurité publique annonce que pour 2016, on risque d'atteindre 23 000 homicides, soit 20/100 000.

Enlèvements : en février 2016, les dépôts de plaintes de ce chef ont augmenté de + 13% sur février 2015 - et il y a pour ce crime un très fort chiffre noir.

Lutte anti-crime - en mai 2016, on apprend que les forces armées mexicaines (police, militaires) n'y vont pas vraiment avec le dos de la cuiller. La moyenne mondiale pour de tels affrontements (forces de l'ordre contre bandits) est de 4 blessés pour un mort. Au Mexique, c'est 8 morts pour un blessé - et on atteint 30 morts pour un blessé quand les Marines mexicains interviennent ! De 2007 à 2012 l'armée mexicaine a tué environ 3 000 bandits, et compte 158 morts dans ses rangs.

Pérou[13]

Selon *l'Observatorio naciolal de politica criminal*, on a recensé dans le pays, pour l'année 2015, 7,2/100000 homicides (5,4/100000 en 2011).

Statistiques & données criminelles, Amérique du Nord

Canada[14]

Pour la première fois depuis douze ans, la criminalité monte au Canada, en 2015. Infractions déclarées cette année-là par les services de police : + 1,9%, hors infractions routières, soit 70 000 de plus qu'en 2014. Notamment : tentative de meurtres : + 22% ; usages d'armes à feu et vols à main armée : + 22% aussi.

A Montréal, les infractions recensées ont tendance à baisser depuis dix ans (-2,5% en 2015). Mais il y a eu dans cette ville, l'an passé, 30 homicides (2 de plus qu'en 2014) et les tentatives d'assassinat y ont bondi de + 48%.

Etats-Unis[15]

Homicides - en 2015, hausse dans les grandes villes des Etats-Unis, après des années de baisse. Calcul sur les 65 plus grandes polices urbaines du pays : augmentation dans 44 d'entre elles, dont New York city,

Los Angeles et Chicago (mais baisse à Washington DC, Miami et Baltimore.

Homicides dans les 30 plus grandes métropoles des Etats-Unis (2015 sur 2014) : + 14,5% ; 50 plus grandes villes, + 17%.

Infractions en général dans les 30 plus grandes métropoles des Etats-Unis (2015 sur 2014) : - 0,1%, stabilité. Crimes violents, + 3,1% (homicides, vols à main armée, viols, etc.).

Chicago - janvier-mai : 240 homicides (+ 50% sur janvier-mai 2015) Mai 2016 : 66 homicides, 19 de plus qu'en mai 2015, 25 de plus qu'en mai 2014. Blessés par armes à feu janvier-mai 2015 : environ 1 200 ; janvier mai 2014, environ 800.

Los Angeles - janvier-février 2015 : 48 homicides (+ 27% sur 2014).

Miami en revanche - 1er trimestre 2015 : 25 homicides et 1er trim 2016 : 12 homicides.

New York city (rappel) - homicides de 2010 à 2015 : - 35%. Crimes violents dans les parcs et jardins de la ville : juillet 2014 - mars 2015 : 340 ; juillet 2015 - mars 2016 : 417, + 23%.

Controverses, le suicide - de 1999 à 2004, les suicides aux Etats-Unis ont augmenté de +24%. Suicides d'Amérindiens (1999-2014) : + 38% ; suicides de femmes + 89%. Ce, dans un pays où l'antiracisme et le féminisme sont (médiatiquement) toujours plus virulents. Etrange, non ? Enfin rapprochons les suicides des homicides : homicides en 2013 : ± 5/100000 ; suicides la même année ± 12/100 000.

Controverses - armes à feu, Noirs, police, etc. - A l'été 2016, paraît une étude d'un jeune professeur (afro-américain) d'économie et de statistiques à l'Université Harvard. Publiée par le réputé *National Bureau of Economic Research*, l'étude approfondie porte sur des données policières de : Austin, Dallas, Houston (Tex.), Los Angeles (Cal.), Orlando et Jacksonville (Fla.). Elle porte au total sur 1 332 tirs de la police (mortels, blessures) sur des civils, de 2000 à 2015. Une fiche détaillée est réalisée sur chacun de ces tirs.

Exemple : à Houston, Tex., la police a (de 2000 à 2015) procédé à 1,6 million d'interpellations, soit environ 290 par jour. Durant ces 15 ans, il y a eu à Houston 507 usage mortel d'armes à feu, soit environ 34 par an. Etc.

Ce qui ressort de l'étude. Lors d'une interpellation, les Noirs sont plus souvent sujets à de la coercition physique, jetés à terre ou aspergés de lacrymo, mais les policiers - quelle que soit leur race - sont plus enclins à ouvrir le feu, sans avoir eux-mêmes été directement attaqués, sur des Blancs (étude sur les 1 332 cas évoqués ci-dessus).

Tirs par la police, toujours - au premier semestre 2016, 510 individus ont été abattus par la police aux Etats-Unis (sur 320 millions

d'Américains). 95%, des hommes 123 Noirs (27,3% des morts ; 235 Blancs (52,3% des morts) ; 79 Hispaniques (17,6% des morts).

Policiers tués par armes à feu : janvier-juin 2016 : 67 ; janvier juin 2015 : 62 (+ 8%).

En juin 2016 paraît une étude du *Harvard Injury Research Center*, à partir des données du *Federal National Crime Victimization Survey*, portant sur 160 000 cas d'usage controversé d'armes à feu, de 2007 à 2011. Il en ressort que : 48% des propriétaires d'une arme à feu aux Etats-Unis déclarent l'avoir acquise pour se protéger (catégorie en augmentation de + 22% depuis 1999). Or sur les 160 000 cas envisagés, l'autodéfense prouvée représentait 127 cas, et 0,9% du total des crimes commis dans les cinq ans étudiés. Proportion très faible, donc.

Justice, race, crime - en juin 2016, une étude tirée du *Bureau of Justice Statistics* (*national prisoners statistics*, etc.) nous apprend que les prisons des Etats (pas les prisons *fédérales*) comptent quelque 1,3 million de détenus. Dans ces prisons, le taux d'incarcération des Noirs est 5,1 fois plus élevé que celui des blancs (Hispaniques, 1,4 fois plus). Ces prisonniers : Blancs, 35%; Noirs, 38%; Hispaniques, 17%. Rappel sur la population des Etats-Unis en général, par race : Blancs : 62% ; Noirs : 13% ; Hispaniques, 17%.

Dans 12 Etats,(Alabama, Caroline nord & sud, Delaware, Géorgie, Illinois, Louisiane, Maryland, Michigan, Mississippi, New Jersey, Virginie) plus de la moitié de la population pénale est Noire (Maryland : 72% d'hommes noirs dans les prisons).

Dans 11 Etats : 1 homme Noir de 18 ans et plus sur 20 est en prison ; Oklahoma, 1 homme Noir adulte sur 15.

Taux d'incarcération par race pour 100 000 habitants : Noirs, 1408/100000 ; Hispaniques, 378/100 000 ; Blancs, 275/100 000;

Par rapport à la drogue, sur l'ensemble des toxicomanes ayant été (au minimum) interpellés : Noirs, 13% des toxicomanes, 36% des interpellés pour possession, 46% des condamnés. Rappelons enfin que 62% des Noirs vivent dans les quartiers-ghettos des centre-ville, le plus souvent en familles instables, exposées à de hauts niveaux de criminalité.

Statistiques & données criminelles, Asie[16]

En avril, l'ONUDC donne une estimation prudente du chiffre d'affaires du crime organisé en Asie du Sud-Est : environ US$ 100 milliards par an. Dont : stupéfiants, environ $ 31 milliards par an ; contrefaçons, 30 milliards/an, trafic des êtres humains, 2 milliards/an.

Statistiques & données criminelles, Europe

Dans ce chapitre, les faits et données, classés par pays de l'Europe (sauf la France).

Généralités, Europe

Immigration, crime et terrorisme[17] - De l'été 2015 à l'été 2016, plusieurs sondages exposent l'inquiétude des Européens, à propos des conséquences négatives des présentes grandes vagues migratoires :

- *Eté 2015 :* pour la première fois depuis 2010, l'immigration devient le problème le plus cité par les citoyens, dans 20 des Etats-membres de l'UE, l'économie passant au second plan. Immigration au 1er plan : 38% des sondés (24% en novembre 2014), + 14 points en un semestre. Situation économique : 27% (moins 6 points). Chômage : 24% (moins 5 points). Finances publiques : 23% (moins deux points). Terrorisme : 17% (plus 6 points). Notons que cet Eurobaromètre date de mai 2015 - donc avant la grande vague migratoire de l'été.
- *Eté 2016 :* Sondage du Pew Research Center dans les pays suivants : Allemagne, Espagne, France, Grèce, Hongrie, Italie, Pays-Bas, Pologne, Royaume-Uni, Suède. Dans 8 de ces dix pays, une majorité (courte ou large) estime que l'afflux de migrants accroît le risque terroriste (moyenne : 59%). Quelques chiffres : Hongrie, 77% ; Pologne, 71% ; Italie, 69% ; Grèce, 65% ; Espagne, 50%.
- *Eté 2016 encore* : Selon Europol, le trafic intercontinental de migrants vers et dans l'Europe implique désormais environ 50 000 malfaiteurs divers, dont 10 000 identifiés au cours de l'année 2015 (6 400 nouveaux identifiés en 2014). Le chiffre d'affaires global de ce trafic est estimé à ± 6 milliards d'euros par an.

Fraudes de toutes natures [18] - En 2015, les fraudeurs ont dépouillé l'UE de 888,1 millions d'euros, selon L'Office de la Lutte Anti-Fraude (OLAF). En 2014, c'était 901 million d'euros. Pour l'essentiel, il s'agit de prêts frauduleux, de fraudes à la TVA, etc. De 2010 à 2014, l'UE a ainsi perdu 2,5 milliards d'euros.

Allemagne 1 : données criminelles générales[19]

Cambriolages : il y en a eu environ 160 000 en 2015, + 10% sur 2014. Les cambriolages sont au plus haut depuis 15 ans. «Beaucoup de cambrioleurs viennent d'Europe de l'Est et disparaissent par les frontières ouvertes» (Police fédérale). En 2015 à Hambourg, par exemple, on a recensé 5 200 cambriolages (+ 20% sur 2014). Dans cette seule ville, les cambriolages et tentatives ont causé un préjudice d'environ 20 millions d'euros.

En 2015 toujours, les vols à la tire ont augmenté de + 7%. En général, la criminalité constatée en Allemagne a atteint 6, 33 million d'infractions en 2015 (dont 40% de vols), + 4,1% sur 2014.

Criminalité financière - En avril 2016, le ministère des Finances annonce avoir détecté sur l'année 2015 de 15 000 à 28 000 transactions hors secteur financier (immobilier, ventes de voitures, marché de l'art) à but de blanchiment. Financier et non financier, le blanchiment total repéré atteint en 2015, 113 milliards d'euros. Une estimation précédente n'indiquait que 50 milliards d'euros.

«Mafia» russe - En Juillet, le ministère de l'Intérieur allemand avertit que le crime organisé russophone se répand dans le pays, actif dans les cambriolages et les vols de commerces. Dans les prisons allemandes, 10% des détenus parlent russe et y sont souvent recrutés par des gangs de leur pays. En Allemagne, la criminalité organisée russe a un effectif de 20 000 à 40 000 malfaiteurs. Beaucoup entrent dans le pays comme «demandeurs d'asile».

Vols dans les commerces - Une bande entre dans un commerce, un comparse distrait le vendeur, les autres pillent. 391 000 de ces vols en 2015, + 15% sur 2014. Préjudice global : 2,1 milliard d'euros en 2014. Objets les plus volés (où sont les «forçats de la faim ?») : parfums, lames de rasoir, cosmétiques, petite électronique. perte moyenne par vol : de 1 500 à 2 000 euros.

Allemagne 2 : crimes des migrants, crimes visant les migrants[20]

Le 5 février 2016, le chef du service de renseignement extérieur allemand (*Bundesamt für Verfassung Schutz*, Bureau de protection de la constitution, BFV), Hans-Georg Maassen, alerte : l'Etat islamique ont infiltré des terroristes en Europe parmi les environ 1 million de «réfugiés» ou «migrants» entrés en Allemagne en 2015.

En mai 2016, Holger Munch, chef de la police fédérale (*Bundes Kriminal Amt*, BKA) annonce la forte augmentation du nombre des auteurs étrangers identifiés de cambriolages, et la baisse d'auteurs allemands de ces mêmes infractions. Des étrangers, souvent Géorgiens, qui travaillent en bande. Un rapport du ministère de l'Intérieur du land du Nord-Rhein-Westphalie (où se trouve la ville de Cologne) annonce aussi l'augmentation du trafic de stupéfiants et des agressions sexuelles.

Juin 2016 : relevé des infractions de tout type commises par des migrants ou des clandestins, par rapport au total des infractions commises (69 000 connues) :
- Vols : 29% du total
- Faux documents & atteintes diverses à la propriété : 28%
- Coups et blessures, atteintes aux personnes : 23%
- Agressions sexuelles : 1,1%

En juin encore, le BKA annonce une baisse de 18% des infractions commises par des migrants ou clandestins en janvier-mars 2016 (par rapport au trimestre précédent). Les individus les plus souvent interpellés pour ces infractions sont issus d'Algérie, Géorgie, Maroc, Serbie, Tunisie.

Toujours en juin, le ministre fédéral de l'Intérieur annonce que, du fait de la crise migratoire, les infractions visant les migrants et clandestins ont été multipliées par 5. 2014 : 170 crimes visant ces migrants ; 2015, 894 crimes. Notamment : incendies d'asiles de réfugiés, 5 en 2014, 75 en 2015.

En juillet, le BKA publie un rapport de 50 pages sur les exactions commises pendant la nuit passée de la Saint Sylvestre. Le di-

recteur du BKA déclare : «Il y a un lien entre ce phénomène (les agressions) et la forte immigration, en particulier en 2015».

Ces agressions impliquent environ 2 000 hommes, pour 1 200 victimes féminines. Ont été authentifiées 642 agressions sexuelles pures et simples, et 239 accompagnées de vol. 650 de ces agressions ont eu lieu à Cologne, 400 à Hambourg, etc.

De janvier à juin 2016, 120 suspects ont été identifiés, la plupart Algériens et Marocains ; la moitié, vivant en Allemagne depuis moins d'un an. Plus de 600 plaintes ont été déposées dans la même période.

La criminalité organisée en Bulgarie[21]

Juin 2016 : le ministre de l'Intérieur déclare que ses services ont repéré et s'intéressent à 424 entités criminelles organisées opérant dans le pays.

La criminalité organisée en Grande-Bretagne[22]

En avril, le ministère de l'Intérieur britannique révèle qu'un commerce sur 5 (gros ou détail) a été victime d'un vol en 2015, 4,7 millions d'infractions, dont 72% de vols par des clients.

La Grande-Bretagne compte quatre régions : l'Angleterre, le Pays de Galles, l'Ecosse et l'Irlande du Nord. Les statistiques suivantes concernent l'Angleterre & l'Irlande du Nord, qui sont d'usage publiées ensemble.

Homicides : 573 (+ 56 en un an, + 11%)

Taux d'homicides en 2005 : 1,6/100 000

Taux d'homicides en 2015 : 1/100 000

Proportion de policiers en 2010 : 1 pour 386 habitants

Proportion de policiers en 2015 : 1 pour 452 habitants

Attaques à l'arme blanche : + 9%

Atteintes aux personnes (en général) : + 27%, *surtout du fait d'un changement dans le mode de calcul*. Cependant, de 2010 à 2015, les crimes violents ont diminué de 25%

6,4 millions d'infractions constatées (- 7% sur 2014)

La criminalité organisée aux Pays-Bas[23]

Avril 2016 - on apprend qu'en 2015, le monde de l'illicite (stupéfiants, prostitution illicite, jeux illicites) a injecté 2,7 milliards d'euros dans l'économie néerlandaise (2,6 milliards en 2014), soit 0,4 de cette économie. Là-dessus, les stupéfiants représentent 55% ; la prostitution, 21% ; les jeux illicites plus le piratage musical, etc., 9%.

Juin 2016 - En 2015, la police néerlandaise a interpellé 173810 adultes suspectés d'une quelconque infraction (107 sur 10 000), moins 12% sur 2014. Juvéniles de 12 à 18

ans : 22 490 en 2015. Ces suspects sont deux fois plus nombreux en ville qu'à la campagne.

La criminalité organisée en Suède[24]

En Suède, la pénalisation des clients des prostituées existe depuis 1999. Selon les autorités «la prostitution a diminué de moitié». Vraiment ? Dans la rue, oui. Mais sans doute n'y a-t-il pas une prostituée de moins, peut-être y en a-t-il en fait plus, car tout ou presque s'est déplacé (l'effet de déplacement, toujours...) sur Internet. Un policier suédois : «On ne peut tout contrôler... Il y a de nouvelles annonces tous les jours... On ne peut surveiller chaque jour toutes les annonces sur Internet».

Donc une prostitution plus discrète, mais toujours là, quoique invisible. En prime, le chien répressif suédois n'a pas de crocs : des peines de prison sont bien prévues - mais nul n'a jamais été incarcéré de ce chef. Pareil en Norvège, où la prostitution aurait «baissé de 25%». Avec les applications du téléphone portable, tout s'arrange hors racolage sur la voie publique. Dans les pays scandinaves, la situation est finalement pire pour les prostituées, livrées à leurs clients, toute confiance dans la police étant désormais abolie.

La criminalité organisée en France[25]

Trafic de cigarettes - en 2015, les taxes sur le tabac ont rapporté 14 milliards d'euros à l'Etat français. Selon une étude du géant de l'audit et du conseil KPMG, commandée par Philip Morris International, Imperial Tobacco, Japan Tobacco International et British American Tobacco, la France a été en 2015 la championne d'Europe de l'usage de cigarettes illégales devant la Pologne, le Royaume-Uni et l'Italie (cigarettes de contrebande et contrefaçon, trafic transfrontalier, achat à la sauvette, sur Internet, etc.). Cela représenterait 9 milliards de cigarettes en 2015, soit 14,6% de l'usage total (+ 1,2% depuis 2014).

61,5 milliards de cigarettes ont été achetées dans les réseaux officiels et 16 milliards de cigarettes fumées sans achat chez le buraliste (27% de la consommation) dont 14,6% de paquets illégaux et 12,5% de paquets acheté légalement hors de France.

Cambriolages - en mai 2016, une étude de l'ONDRP portant sur les années 2007-2014 et faite auprès de 130 000 familles, a permis de profiler la cible idéale pour les cambrioleurs. Dans les critères, la catégorie sociale est en tête, suivie de la nature du logis, les maisons isolées étant (bien sûr) plus à risque que les immeubles.

La cible idéale est ainsi un individu jeune, diplômé du supérieur, famille monoparentale, logis pavillonnaire proche d'une agglomération de plus de 100 000 habitants. Régions les plus à risque : Ile-de-France, Sud-Est. Les moins à risque : Nord-Pas-de-Calais (??), Ouest, Rhône-Alpes, Auvergne.

• Statistiques & données sur les stupéfiants et leur trafic

A l'échelle mondiale[26]

Selon ONUDC-World drug report 2016, 29 millions de personnes sont en état d'addiction à divers narcotiques, de par le monde (+ 2 millions sur 23014) ; 12 millions le sont de drogues qui s'injectent et 14% de ceux-ci sont séropositifs ou ont un sida déclaré. Plus largement, le même rapport de l'ONU indique qu'en 2014 et de par le monde, quelque 250 millions de personnes avaient usé au moins une fois d'une drogue illicite (ici, pas d'augmentation par rapport à une étude datant de 2010).

- *Cocaïne :* en Amérique latine, les cultures de coca ont progressé de 10% entre 2013 et 2014 ;

- *Opiacés :* le nombre de toxicomanes aux opiacés ou opioïdes (médicaments analgésiques, etc.) a cru de 17% de 2013 à 2014.

Economie de la cocaïne[27]

Voici la machine à profit de la cocaïne au long de la transformation de feuilles de coca en chlorhydrate de cocaïne :

- Colombie, Pérou Bolivie : le kilo de feuilles est vendu de 1,30 à 3 US Dollars le kilo.
- Selon la variété de coca, de 450 à 600 kilos de feuilles donnent un kilo de pâte-base. Donc pour produire un kilo de pâte-base, les narcos doivent acheter pour 600 à 800 US Dollars de feuilles.

I kilo de pâte-base, ou cocaïne base, donne un kilo de chlorhydrate de cocaïne. Au printemps 2016, 1 kg de chlorhydrate de cocaïne se vend :

- Dans la jungle andienne, US$ 2 200
- Dans un port de la région, US$ 5 500 à 8 000
- En Amérique centrale, US$ 10 000
- Au sud du Mexique, US$ 12 000
- A la frontière des Etats-Unis, US$ 16 000
- Aux Etats-Unis (selon l'Etat), de US$ 24 000 à 27000
- En Europe (selon le pays) de US$ 53 000 à 57 000
- En Australie, US$ 200 000.

Au départ de Colombie, la cocaïne est pure à 85%. En Grande-Bretagne, pure à 60% en gros, à 30% au détail.

Culture de la coca - de 2000 à 2014, les surfaces plantées en coca ont diminué de 40% en Amérique latine. Mais des progrès en génie génétique et techniques agricoles font que cette baisse n'est en fait que de 10%. Du fait de saisies plus importantes à l'international, la quantité de cocaïne disponible sur la marché mondial est cependant moindre. Nouveau : les cultures de coca recommencent à augmenter en 2014 en Colombie (2014, surfaces cultivées : + 39%, en 2015, + 42,5%).

Etats-Unis : la consommation baisse : en 2014, les surdoses mortelles de cocaïne ont diminué de - 34% et les admissions à l'hôpital de ce fait, de - 54%. Dans ce pays, 90% de la cocaïne arrive de Colombie.

Nouveaux marchés : la cocaïne conquiert à présent Israël, la Chine et l'Australie.

Europe[28]

Cannabis - dans le 21e rapport de L'Office européen des drogues et debla toxicomanie, on append que 1% des Européens en consomme tous les jours. Que la teneur en THC (principe intoxicant, Tétra Hydro Cannabinol) de l'herbe est en moyenne de 8 à 12% et de la résine, jusqu'à 18%.

Grande-Bretagne[29]

(Angleterre + Pays de Galles, CSEW, 2015-2016) en 2015, environ 725 000 individus, soit 2,2% de la population de ces provinces entre 16 et 59 ans, ont consommé régulièrement de la cocaïne-poudre, la 2e drogue du pays après le cannabis. De 16 à 24 ans : 4,4%.

2,7 millions d'individus en ont consommé au moins une fois dans l'année.

L'année précédente (2014-2015) : 16 à 59 ans : 2,3%, 16-24 ans : 4,8%.

Rappel pour 2008-2009 : 16 à 59 ans, 3% ; 16-24 ans, 6,5%.

Donc, baisse régulière.

Foyers riches *(revenus £ 50 000 et plus par an)* : 16 à 59 ans, 2014-15, 2,2% 2015-16, 3%.

(Angleterre + Pays de Galles, CSEW, 2015-2016) - Usage de drogues par les femmes :

Femmes ayant usé d'une drogue ou plusieurs, dans l'année précédente :
- 205-2016 : 5%, au plus bas depuis la fondation de la statistique en 1996. Pour 2003-2004, c'était 8,8%.

Usage d'un quelconque stupéfiant l'année précédente (femmes de 16 à 24 ans) :
- 2015-16 : 18% (1,1 million d'individus)
- 2014-2015 : 19,5%
- 2005-2006 : 25,2%.

«Croissant d'Or»[30]

Selon l'organe fédéral russe chargé de la lutte antidrogues, la production d'opium en Afghanistan a été multipliée par 40 depuis l'entrée (en octobre 2001) des Etats-Unis en Afghanistan, suite aux attentats du 11 septembre 2001. Dans ces 15 ans, les surfaces plantées en pavot sont passées de 131 000 hectares à 154 000 (+ 18%). Aujourd'hui encore, ce pays produit plus de 90% de l'opium mondial. A la fin de la décennie 2000, la vente d'opiacés contribuait pour 19% au PNB afghan (environ 2,3 milliards de US$).

43% des drogues fabriquées en Afghanistan sont exportées via le Pakistan. Désormais, une partie des profits de ce trafic va à l'Etat islamique.

Mexique[31]

Pour la première fois, le Mexique publie des données sur la culture du pavot à opium, voué à la production d'héroïne, dans le pays. Selon Mexico il y avait (entre juin 2014 & juin 2015) 24 800 hec-

tares plantés en pavot, ce qui fait du Mexique le 3e producteur mondial. Selon les Etats-Unis, ce serait 17 000 ha, + 59% sur 2013 et selon l'ONUDC, il y avait dans le pays, mais en 2009, 19 500 ha de pavot.

Toujours plus, les Cartels mexicains exportent aux Etats-Unis une puissante héroïne de synthèse nommée Fentanyl. La concentration du Fentanyl étant 40 fois celle de l'héroïne, 25 à 30 kilos de Fentanyl ont la puissance d'une tonne d'héroïne. On peut couper le Fentanyl bien plus que l'héroïne, ce qui le rend 20 fois plus profitable que cette dernière.

Héroïne : achat en gros US$ 6 000 en Colombie, revente en gros US$ 80 000 à Boston (par exemple).

Fentanyl : achat en Chine d'un kilo, US$ 5 000 ; après coupage = 20 kilo dans la rue ; vente au détail par grammes = US$ 1,5 million.

Aux Etats-Unis, le Fentanyl se consomme souvent sous forme d'un mélange avec de l'héroïne nommé «*Diablito*». En 2014, les Etats-Unis ont connu plus de 700 surdoses mortelles dues au Fentanyl.

Etats-Unis[32]

Chaque année, les Américains dépensent environ 65 milliards de dollars en stupéfiants. De 2000 à 2015, les surdoses mortelles d'opiacés + opioïdes (drogue et médicaments analgésiques) ont quadruplé. Le nombre d'héroïnomanes a doublé de 2005 à 2012.

Tout le dispositif anti-blanchiment mis en place aux Etats-Unis pour intercepter l'argent de la drogue, récupère US$ 1 milliard par ans (soit 1,5% du total). Donc 98,5% de cet argent reste aux Narcos - taux de taxation d'une extrême modestie...

Aux Etats Unis (2015) les surdoses mortelles d'opiacés + opioïdes sont désormais de 78 par jour, plus que du fait des accidents de la route ! On a compté en 2014 plus de 16 000 de ces surdoses mortelles.

En 2014, les Etats-Unis comptaient environ 500 000 Américains en état d'addiction aux opiacés + opioïdes 75% des toxicomanes ont commencé par prendre des analgésiques type Oxycontin, Hydrocodone, Méthadone, etc., et sont ensuite passés à l'héroïne ou au Fentanyl.

Aujourd'hui, en moyenne, une dose d'héroïne coûte moins cher aux Etats-Unis qu'un paquet de cigarettes (ces dernières : de 4,5 à 10 US$ le paquet).

La dernière étude sur le coût économique de l'épidémie d'opiacés + opioïdes date de 2007. Elle fournissait alors les résultats suivants :

- Total : US$ 193 milliards de dollars par an.
- Dont : US$ 120 milliards, perte de productivité... travail non exécuté...prix des désintoxications... Prison... morts précoces... US$ 11 milliards : coûts médi-

caux ; US$ 61 milliards : justice, police, victimes à défrayer, etc.

Afrique du Sud[33]

La route du sud prise par l'héroïne afghane pour s'exporter aboutit en Afrique du Sud ; on la nomme «*smack Track*» : Pakistan - Iran - Océan indien - Afrique de l'Est - Afrique du Sud. C'est un trafic surtout maritime qui voit, estiment les experts, environ 22 tonnes d'héroïne par an transiter par l'Afrique de l'Est (Mombasa, Dar es-Salaam). La consommation annuelle de cette partie de l'Afrique serait d'environ 2,5 tonnes d'héroïne par an, le principal consommateur régional étant la Tanzanie.

Notes

[1] *New York Times International* - 17/08/2016 «Terrorism's toll is rising in West but not around the world».
[2] The Global Slavery Index 2016 ; AFP - 12/052016 «Le tourisme pédophile progresse dans le monde, le profil des criminels change».
[3] *Al-Jazeera*, 5/06/2016 - «UN: rising environmental crime threatens our societies» ; *Reuters*, 4/06/2016 «The world's 4th most valuable criminal enterprise is growing at an alarming pace» ; ONUDC - 13/05/2014 «Wildlife crime worth USD 8-10 Billion annually, ranking alogside human trafficking, arms and drug dealing in terms of profit : UNODC chief».
[4] *The Conversation*, 7/04/2016 «Médicaments contrefaits, un crime mondial». OCDE - avril 2016 + *AFP*, 18/04/2016 «Le commerce mondial de contrefaçon pèse près de 500 milliards de dollars par an».
[5] *L'Express+Afp*, 27/04/16 «La piraterie diminue dans le monde, sauf au large du Nigeria».
[6] *Le Point*, 6/07/2016 «Quand les oubliés de la mondialisation se vengent dans les urnes» ; *Le Figaro*, 12/05/2016 «2 000 milliards de pots-de-vin versés chaque année dans le monde» ; *Le Figaro*, 15/04/2016 «Les tentatives de fraudes en entreprises ont explosé en 2015».
[7] *The Guardian* - 13/06/2016 «How to make Latin America's most violent cities safer»
[8] *AP* - 3/07/2016 «El Salvador, deadliest nation in 2015, sees lull in violence» ; *Vice News* - 5/06/2016 «The murder rate in the world's murder capital is finally dropping».
[9] *Insight Crime* - 27/04/2016 «Does reality match perception of rising crime in Argentina ?
[10] *New York Times International* - 5/08/2016 «No game : the Olympics, Rio and terror» ; *New York Times International* - 23/07/2016 «Immense wealth and corruption in Brazil».
[11] *Colombia Reports* - 29/04/2016 - «Colombia's post AUC paramilitaries left more than 320 000 victims».
[12] *Business Insider* - 27/07/2016 «Homicides are on the rise in Mexico after years of decline, and it's the result of a new criminal dynamics» ; *Insight Crime* - 27/07/2016 «Mexico's deteriorating homicide trends show no sign of abating» ; *AP* - 21/07/2016 «Homicides rise 15,4% in Mexico in first half of 2016» ; *New York Times International* - 28/05/2016 «Mexican military runs up body count in drug war» ; *Insight Crime* - 28/04/2016 «Figures show violence in Mexico rising and spreading» ; *Insight Crime* - 5/04/2016 «Rising homicide rate in Mexico wiping out recent gains».
[13] *Insight Crime* - 22/07/2016 «Peru's new homicide indes shows spiking violence in drug port».
[14] *Le Quotidien-Presse Canadienne* - 21/07/2016 «Criminalité en hausse au Canada» ; *Global News Canada* - 27/04/2016 «Overall crime down, but serious offenses up in Montreal».
[15] *New York Times International* - 17/08/2016 «Shadow of crime in New York» ; *Wall Street Journal* - 22/07/2016 «Fact checking Donald Trump's remarks on crime» ; *New York Times International* - 12/07 «Bias in Police shootings ? Study says no» ; *Le Monde* - 8/07/2016 «Qui sont les 510 personnes tuées par la police américaine en 2016 ?» ; *Foreign Policy* - 4/07/2016 «America's suicide epidemic has gotten worse» ; *Washington Post-WonkBlog* - 14/06/2016 «For every gun used in self-defense, six more are

used to commit a crime» ; *Daily Mail + AP* - 5/06/2016 «Murder, rape and other violent crimes have soared this year in major US cities» ; Juin 2016 - The Sentencing Project - Research and advocacy for reform - «The color of justice: racial and ethnic disparity in states prison» ; *Washington Post-WonkBlog* - 22/04/2016 «Last year's crime trends are still a puzzle, even with new data».

[16] *NNN-Bernama* - 25/04/2016 «Transnational organised crime value in Southeast Asia exceeds US$ 100 billion per year, UN.

[17] *Reuters* - 13/07/2016 «People smugglers have hit record level as criminal gangs cash in on Europe's refugee crisis». *AP* - 11/07/2016 «Survey : Europeans worry migrants may increase terror threat» ; *Washington Post* - 11/07/2016 «Anti muslim views rise across Europe» ; *AFP*, 1/08/2015 «L'immigration, principale préoccupation des Européens».

[18] *CITY AM* - 31/05/2016 «The European union lost over € 880m to fraud in 2015.

[19] *Deutsche Welle* - 10/07/16 «German federal police warn of Russian mafia spreading in Germany ; *The Local Deutsch* - Deutsche Welle - 21/06/2016 «Shoplifting on the rise in Germany» ; 21/04/2006 «Over € 100 billion laundered in Germany every year: report» ; *International Business Times* - 21/04/2016 «Money laundering reaches s 113 bn. in Germany, as organized crime flourishes» ; *Deutsche Welle* - 30/03/16 «Burglary rate in Germany hits 15-year high».

[20] *The Local Deutschland* - 11/07/2016 «2 000 men were involved in NYE sex crimes: police» ; *Le Figaro* - 11/07/2016 «Allemagne : un rapport révèle l'ampleur des agressions sexuelles du nouvel an» ; *Sputnik-Kommersant* - 29/06/2016 «Allemagne : le nombre de crimes contre les migrants explose» ; *The Local Deutschland* - 10/06/2016 «Why refugees are committing far less crimes» ; *The Local Deutschland* - 8/06/2016 «Crimes by migrants drop 20% in three months» ; *Daily Mail* - 18/05/2016 «Germany sees huge rise in number of burglaties carried out by migrants» ; *New York Times International* - 6/02/2016 «Germany says suspects entered EU as refugees».

[21] *Novinite* (Bulgarie) 23/06/2016 «Ministry of the Interior: 424 organised crime groups operate in Bulgaria».

[22] *Forecourt Trader UK* - 29/04/2016 «Retail has highest crime rate of all business sectors» ; *The Guardian* - 21/04/2016 «Murder rate in England and Wales rises 11%» ; *Sunday Express* - 21/04/2016 «Killings up 11% and rape cases hit highest rate since 2003, shock figures reveal» ; *Daily Mirror* - 21/04/2016 «Britain facing violent crime wave as stabbings and murders soar».

[23] *NL Times* - 22/06/2016 «Over 10% drop in adult crime suspects» ; *NL Times* - 05/04/2016 «Vice, crime, pumps over € 2,7 billion in Netherlands economy».

[24] *L'Express+ Afp* - 8/04/2016 «Europe du Nord : une prostitution moins visible mais toujours vivace» ; *France Info* - 14/02/2016 «En Suède, la prostitution s'est déplacée sur Internet».

[25] *20 Minutes* - 9/06/2016 «La France, plus grosse consommatrice de cigarettes illégales en Europe» ; *Le Figaro* - 19/05/2016 «Une étude dévoile le portrait-robot des victimes du cambriolages».

[26] *Business Insider* - 30/06/2016 «These maps show how dangerous illegal drugs travel» ; *Turkish weekly* - 23/06/2016 «UN: record 29 million people drug-dependent worldwide».

[27] *Business Insider - Stratfor* - 27/06/2016 «From Colombia to new York City: the narconomics of cocaine» ; *Insight Crime* - 24/06/2016 «Is the global cocaine trade in decline ?».

[28] *Le Point* - 1/06/2016 «L'ecstasy et l'héroïne font leur grand retour en Europe».

[29] *City AM* - 29/07/2016 «Rich Britons used the most cocaine last year since 2009» ; *BBC News* - 28/07/2016 «Drug use among women drops to 20-year low».

[30] *TeleSur* - 31/08/2016 «Afghan opium production 40 times higher since US-Nato invasion».

[31] *Insight Crime* - 23/06/2016 «Mexico publishes poppy cultivation data for first time» ; *New York Times international*, 10/06/2016 «Potent opioid is enrighing Mexican cartels, US says».

[32] *Fair Share Education Fund* - August 2016 - «Anonymity Overdose (Report) ten cases that connect opioid trafficking and related money laundering to anonymous shell companies» ; *Le Figaro* - 29/06/2016 «Etats-Unis : hausse des décès liés à l'héroïne».

[33] *Daily Maverick*, Afrique du Sud - 21/06/2016 «From Afghanistan to Africa : heroin trafficking in East Africa and the Indian Ocean».

Tribune Libre

Lutte contre la délinquance et le crime en banlieue : un cuisant échec

*Dave HOLDEN**

La loi de 2007 sur la prévention de la délinquance devait marquer un tournant dans la prise en compte et la perception de la problématique. Il ne s'agissait nullement de ressasser les causes de la délinquance à grands renforts de thèses et antithèses d'universitaires, politiques, professionnels et autres, mais bien de se concentrer sur les moyens et les actions. Neuf ans après, force est de constater l'échec global et la déception ambiante, notamment de beaucoup de maires.

Le texte de 2007 - et l'esprit même de la loi - reposait sur le maire comme pivot d'un dispositif local et partenarial ; un dispositif recentré sur le territoire sur lequel le maire disposait des outils juridiques pour réunir tous les acteurs locaux concernés par la délinquance. L'un de ces outils était le partage des informations, ou plus exactement du secret professionnel auquel trop d'institutions ou de structures étaient jusque là attachées (telles que la protection judiciaire de la jeunesse, l'aide sociale à l'enfance, la justice). Si bon nombre de partenaires y ont cru, si les initiatives locales sont pléthoriques et fort intéressantes, ce dispositif est un échec.

En premier lieu, toutes les institutions n'ont pas joué le jeu de l'échange et de la transparence, attachées à leurs préjugés et considérant leur domaine de compétence comme un pré carré non transmissible. Si le ministère de l'intérieur et les forces de l'ordre ont longtemps pratiqué l'opacité, ces dernières sont aujourd'hui les seuls partenaires quotidiens et transparents des mairies depuis 2007. Les procureurs sont trop peu nombreux à accepter que des données nominatives soient fournies par les services de police ou de gendarmerie dans les instances partenariales, sans parler de l'absence ré-

currente des magistrats à ces dernières. La protection judiciaire de la jeunesse comme l'aide sociale à l'enfance montrent la même réticence à partager le secret professionnel, montrant une méfiance non dissimulée à l'encontre de leurs interlocuteurs institutionnels, incluant même les travailleurs sociaux (assistantes sociales et psychologues) implantés dans les commissariats. Les bailleurs sociaux sont demandeurs de solutions toutes faites mais rechignent à utiliser l'arsenal juridique en leur possession, dans un contexte social interne complexe, notamment avec les gardiens d'immeubles.

Dans ces méandres partenariaux, les mairies et leurs services de prévention comme les associations, fourmillent d'initiatives et de volontarisme, souvent mort-nées ou bloquées par un partenariat non-abouti.

En second lieu, l'échange d'informations pour lutter contre la délinquance repose sur des constats précis et objectifs de la situation. Les statistiques de la délinquance sont indispensables - mais non exclusifs - pour obtenir une photographie d'un territoire. Or, depuis la création du service des statistiques du ministère de l'intérieur, les chefs de service territoriaux de la police et de la gendarmerie ont pour interdiction de communiquer ces données aux maires. Seul le dit service est habilité - autorisé - à leur fournir les chiffres ... qu'ils n'ont toujours pas reçu à ce jour. Les édiles municipaux sont ainsi dépendants de la qualité de leurs relations avec les forces de l'ordre qui leur distillent, au compte goûte et officieusement, des données chiffrées. D'autres font appel à des cabinets d'études qui leur facturent notamment des logiciels cartographiques qui ne seront pas alimentées par des données fiabilisées faute de transmission par le service statistique du ministère.

La fameuse coproduction de sécurité tant vantée depuis près de 15 ans - de la police de proximité à nos jours - n'est qu'illusion, faute de véritable politique pénale et de lutte contre la délinquance. Les initiatives locales sont nombreuses mais forment un patchwork disparate et dépendant des bonnes volontés, financées à grand coup de ressources du Fonds Interministériel de Prévention de la Délinquance (FIPD), sans véritable contrôle. Aucun enseignement n'est tiré de toutes ces expériences, aucune centralisation et étude réelle ne sont réalisées pour formaliser et généraliser les bonnes pratiques et surtout, conduire à une ligne de conduite et à une politique cohérente et efficace de lutte contre la délinquance. Il suffit de regarder le catalogue du Comité Interministériel de Prévention de la Délinquance (CIPD) pour constater l'hétérogénéité des domaines et actions éligibles à un financement : semblable à la Samaritaine, vous trouvez de tout au CIPD qui finance tout. Bien plus, une enquête du secrétariat général du CIPD réalisée en 2010 au titre du suivi des actions de prévention de la récidive, relevait que les deux champs d'actions les plus financés étaient les « art, culture, sport et loisirs » et « l'emploi et l'insertion professionnelle », et 31% du public bénéficiaire étaient des personnes incarcérées.

Les gouvernements se succèdent et seules les terminologies changent dans les circulaires et instructions ministérielles. Au patchwork des initiatives locales fait écho le mille-feuille des directives nationales, sans fil directeur et complété au gré de l'actualité, pour sembler répondre aux critiques potentielles d'immobilisme.

Ce constat est le même depuis au moins deux décennies et le contexte terroriste sur notre territoire n'a nullement réveillé les concepteurs. Si de nombreuses mesures ont été prises depuis le début de la vague d'attentats, elles ne le sont qu'en réaction et sur du court terme. Aucune démarche d'anticipation ou de pro-action n'avait été entreprise, et rien en ce sens ne semble changer. A la nécessité criante de créer en France un service spécifique anti-terroriste, le gouvernement, comme tous ceux avant, ne prennent que des mesurettes visant à répondre à la démocratie d'opinion et/ou à calmer des forces de l'ordre atterrées et épuisées.

Quid de la lutte contre la délinquance. Mêmes causes, même constat. Bien plus, le profil des auteurs des attentats est invariablement le même : des jeunes issus de la délinquance de droit commun vouant une haine féroce contre une société qui ne les aurait pas intégrés et contre les forces de l'ordre.

Les évènements dramatiques et la menace terroriste prégnante devraient mener les autorités à repenser l'ensemble de la politique pénale et ouvrir une réflexion sur les moyens à long terme à mettre en œuvre pour lutter contre ce fléau endémique et exponentiel de la délinquance, et plus particulièrement de la délinquance des mineurs.

Une lueur d'espoir sur un travail de fond était apparue en 2012 avec l'annonce d'une conférence gouvernementale de consensus sur la prévention de la récidive par le garde des sceaux Christiane Taubira. Après de nombreuses auditions et consultations, il en est ressorti un texte inutile : « les 12 recommandations pour une nouvelle politique publique de prévention de la récidive » relèvent de la rhétorique idéologique et sont vides de sens et de fond. Plusieurs mois d'auditions et de travaux pour aboutir à une réflexion avortée : « *1. la peine de prison, une peine parmi d'autres ; 2. Abandonner les peines automatiques ; 3. Instaurer une peine de probation ; 4. Mettre en œuvre la peine de probation ; 5. Sortir certaines infractions du champ de la prison ; 6. Permettre la réinsertion des récidivistes ; 7. rendre la prison digne des citoyens ; 8. Empêcher toute « sortie sèche » ; 9. permettre l'accès aux dispositifs de droit commun ; 10. Supprimer les mesures de sûreté ; 11. Conduire une évaluation raisonnée ; 12. Coordonner la recherche* ».

Des pans entiers de la problématique ont été éludés dès le départ et le jury s'est focalisé sur les alternatives à la prison. La prévention de la récidive n'a été abordée que sous l'angle des condamnés à une peine d'emprisonnement, et plus précisé-

ment des détenus. Ceux faisant l'objet plus largement d'une sanction pénale n'ont pas été pris en compte.

Bien plus, deux thèmes majeurs ont été écartés volontairement : la récidive-réitération des mineurs et l'exécution des peines.

Dans de nombreuses villes, si la part des mineurs auteurs est stable depuis 2013 après une hausse continue depuis les années 90, elle reste considérable et préoccupante. L'aveuglement de certains sociologues évoquant « une instrumentalisation politique et médiatique en matière de délinquance des mineurs » est particulièrement dangereux et explique en partie l'immobilisme, voire le blocage sur cette thématique. Les forces de l'ordre sont les premiers spectateurs d'un phénomène endémique. Dans certaines catégories d'infractions telles que les vols avec violences ou les coups et blessures, la part des mineurs mises en cause atteint plus de 40% dans les grandes agglomérations ou les banlieues. Comment ignorer et parler d'instrumentalisation à Marseille, Saint-Denis, Sarcelles où les vols avec violences dans la rue et les transports en commun sont devenus depuis plusieurs années le sport local de mineurs de plus en plus jeunes ? Ces mêmes villes et banlieues gangrénées par une délinquance définitivement installée que les responsables politiques et les autorités ne voient pas ou plus.

Ces villes et ces quartiers cumulant problèmes sociaux-économiques et insécurité que l'on regarde avec fatalisme, où on injecte des sommes astronomiques dans le cadre de l'ANRU (agence nationale de rénovation urbaine) notamment, sans tenter de régler les problèmes de fond. Ces quartiers où règnent une véritable omerta et un sentiment d'insécurité tellement fort que les habitants sont paralysés. Lorsque quotidiennement les cages d'escaliers et halls d'immeubles sont occupés par des groupes de jeunes filtrant les entrées (en contrôlant l'identité des personnes et interdisant l'accès aux non-résidents !), régulant les allées et venues des résidents en fonction de leur trafic (un jeune à l'entrée donne le feu vert pour rentrer dans l'immeuble ou descendre l'escalier selon qu'une transaction est en cours ou pas), vociférant jusque tard dans la nuit, installant chaises et tables sur un palier tel un stand, des gamins d'une dizaine d'années maillant le territoire d'un quartier pour siffler à l'arrivée d'un véhicule de police ou dotés de talkie-walkie contre un billet de 10 ou 20 euros... tant de situations réelles et nombreuses qui ne relèvent nullement d'une quelconque manipulation médiatico-politique.

Lorsque les résidents ont encore le courage ou la force d'en parler, ils décrivent un véritable calvaire quotidien auquel l'arsenal juridique ne sait pas répondre : la loi du 2 mars 2010 avait été annoncée comme LA solution aux troubles à l'ordre et à la tranquillité publics, en créant l'infraction d'occupation illicite dans les parties communes.

Source incommensurable d'espoir chez les habitants et les bailleurs, le texte s'est révélé inapplicable : d'une part, les éléments constitutifs de l'infraction sont rarement réunis et la simple présence génératrice d'insécurité (voire de peur) ne rentre pas dans les critères légaux. D'autre part, la nécessité d'identification précise d'une victime et de son dépôt de plainte démontre l'ignorance du législateur : comment obtenir un témoignage sur procès-verbal (qui ne peut être anonymisé) dans un climat de peur ? Bien plus, le texte est inadapté à la réalité en exigeant la matérialité d'une entrave, ce qui ne s'applique qu'à une infime partie des situations.

En pratique, rares sont les habitants qui acceptent de témoigner. Et lorsque les plus courageux déposent plainte, très peu de procédures judiciaires donnent lieu à des poursuites pénales : impossibilité d'apporter la preuve irréfragable, impossibilité d'individualiser la commission des faits (selon le principe d'imputabilité du droit pénal français), les éléments constitutifs de l'entrave non remplis, etc. Et pour les rares procédures qui ont passé tous les filtres et sont audiencées, les magistrats du siège sont absolument *non- conscients* du contexte et liés par des règles juridiques inadaptées.

Restent aux forces de l'ordre le recours à des moyens détournés peu ou pas coercitifs que sont par exemple les verbalisations pour tapage diurne ou nocturne, le dépôt d'immondices. Quant aux faits d'atteintes aux personnes (telles que les menaces) ou même les dégradations, faute d'auteurs nominativement désignés ou identifiés, l'impunité reste totale pour les fauteurs de troubles. Les habitants regardent quotidiennement le même manège sans que rien ne change : les forces de l'ordre viennent, contrôlent, repartent et les individus sont toujours là... comme le calvaire des habitants qui ne fait pas le poids face aux accusations de contrôles aux faciès et de harcèlement par les forces de l'ordre.

Quelle aberration de devoir expliquer pourquoi certains individus peuvent être contrôlés plusieurs fois dans une même journée alors qu'ils pourrissent la vie des habitants d'une cage d'escaliers au point que certains vivent reclus ou développent des symptômes dépressifs !

Le sentiment d'impunité - voire l'impunité purement factuelle - sans cesse alimenté a pour corollaire et conséquence un sentiment d'abandon très fort des habitants et à une omerta généralisée. Un exemple récent dans une banlieue parisienne dite difficile est celui d'habitants demandant au maire une rencontre ni dans leur quartier ni même en mairie afin de ne pas être vus en sa présence et désignés ainsi comme « balance ». De même, les courriers dans les commissariats se font de plus en plus rares puisque l'absence de résolution des problèmes décourage tout témoignage même anonyme.

Il faut participer à une réunion de quartier lorsque les habitants osent venir pour

constater cette désolation et cette détresse que ni les autorités administratives ou judiciaires ne soupçonnent ou comprennent. Fatalistes sur leur environnement dégradé, les habitants développent un sens inversé des priorités et ne focalisent plus que sur les questions de stationnements et enlèvements de véhicules, alors même que leur cage d'escalier est occupée par des vendeurs de stupéfiants.

Dernière trouvaille des technocrates pour rassurer la population dans ces quartiers : les adultes-relais. Réminiscence de 1999, ce programme créé par le comité interministériel des villes a « vocation à favoriser le lien social entre les habitants des quartiers prioritaires, les services publics et les institutions ». En théorie, l'adulte-relais, employé en CDD ou CDI, est censé être un médiateur social qui contribue à « renforcer le lien social et le règlement des conflits de la vie quotidienne ». En pratique, ce n'est autre que le système dit des grands frères dont on connaît les dérives.

Il existe un autre facteur d'impunité des mises en cause, celui engendré par les règles pénales : d'une part, celles relatives à l'exécution (défaillante) des peines défaites; d'autre part, celles relatives à la procédure même.

Le fonctionnement de nos appareils pénaux n'autorise pas de forts pourcentages d'élucidation des délits les plus couramment pratiqués et portés à la connaissance des services de police. Et quand le délinquant se fait prendre, seule une partie de ses actes est élucidée. Se pose alors la double question relative à la sanction pénale : la sanction prononcée est-elle adaptée à l'infraction, au contexte et à la personnalité de l'auteur ? Dans quel délai la sanction pénale va-t-elle intervenir pour produire ses effets vis-à-vis de l'auteur et de la victime ?

Sur le premier point, le panel de sanctions permet d'individualiser la réponse pénale. Cependant, le recours aux alternatives aux poursuites ne doit pas être utilisé comme un outil de désengorgement des tribunaux correctionnels. Si les parquets se targuent chaque année d'un taux de réponse pénale supérieur à 80%, la corrélation entre la sanction et l'infraction n'est pas précisée. Bon nombre de policiers peut quotidiennement donner des exemples de décisions inadaptées voire ineptes : le rappel à la loi en MJD pour l'auteur d'un vol avec violence, un SDF multi-réitérant convoqué devant le tribunal correctionnel, un mineur multi-réitérant de vols avec violences cumulant les mises en examen devant le juge pour enfant avec suivi socio-éducatif, etc.

Sur le second point, la charge de travail des tribunaux entraîne des délais de convocation devant les juridictions pénales à l'effet dévastateur sur la victime et l'auteur. Des convocations devant le tribunal correctionnel plus d'un an après sa notification renforcent le sentiment d'impunité (voire d'inexistence de l'infraction) de l'auteur. Que dire de l'impact pour la victime pour laquelle l'action des services de police et de

la justice est alors illisible et génère une défiance certaine.

Mais ces deux questions ne relèvent que du premier niveau de réponse pénale. La certitude pour le délinquant de voir la peine exécutée pour qu'elle produise le double effet dissuasif et protecteur n'est pas la réalité. C'est l'Union syndicale des magistrats qui a la première ouvert ce dossier grâce à un livre blanc publié en 2002 dénonçant une « justice virtuelle » dans laquelle 37% des peines de prison fermes prononcées restaient lettre morte. En réaction, le rapport de l'inspection générale des services judiciaires remis au Garde des Sceaux quelques mois plus tard a conclu à l'inexécution de près de 30% des peines de prison.

Qu'est devenue la procédure pénale en France ? Plus exactement, que signifie aujourd'hui procéder à une enquête judiciaire ? Sans exagération aucune, ce n'est plus que de la paperasse au détriment de l'investigation où la parole des policiers et gendarmes n'a presque plus de valeur juridique - malgré les règles inscrites dans le code de procédure pénale - et où la victime est reléguée en arrière plan.

De la loi contre la présomption d'innocence aux récentes directives européennes « *sur la simplification de la procédure* », le témoignage du professionnel comme celui de la victime n'a qu'une valeur probante réduite : faute d'éléments matériels de nature irréfragable (une vidéo par exemple), le témoignage est insuffisant et ne suffit plus à emporter l'imputabilité. En pratique, quotidiennement, comment expliquer à une victime, dont vous avez arraché le témoignage malgré ses peurs, que sa parole ou que le fait qu'elle reconnaisse formellement son auteur lors d'un tapissage (parade d'identification selon le terme juridique) ne suffise pas à contrecarrer les dénégations du mis en cause ? Comment rassurer une victime à laquelle vous avez encore arraché son accord pour être confrontée en audition à son auteur, et à laquelle vous devez expliquer que si elle souhaite être assistée par un avocat, elle doit faire les démarches seule (et à ses frais), contrairement au mise en cause ? Et à compter du 16 novembre 2016, en application d'une directive européenne transposée dans la loi du 3 juin 2016, il faudra expliquer à la victime que l'avocat du mise en cause pourra être présent, à côté de la victime, lors de la séance d'identification ?

Ce même texte qui ne comporte quasi exclusivement que des mesures renforçant les droits du mis en cause pendant l'enquête au mépris total de la victime. Exemple symptomatique : la possibilité pour le gardé à vue de s'entretenir pendant 30 minutes avec la personne et par le truchement de son choix. Nonobstant les contraintes pratiques et opérationnelles qu'une telle mesure engendre pour un service de police, nul besoin d'expliquer les conséquences sur le bon déroulement des investigations.

Tel est le tableau aujourd'hui : des victimes délaissées dans une procédure pénale qui

se complexifie, des peines peu exécutées, une récidive mal traitée, une délinquance des mineurs sous-estimée et des banlieues qui s'enferrent dans leur ghettoïsation faute de véritable politique de la ville. Simple constat de l'inefficacité des politiques menées depuis plus de deux décennies.

Les crédits de l'ANRU ou du FIPD ne font que cacher maladroitement la forêt. Quelle médiocrité et malhonnêteté intellectuelles que de penser encore aujourd'hui qu'injecter de l'argent - sans aucun contrôle d'autant plus - peut avoir une incidence sur la délinquance, la paupérisation de certaines populations et la communautarisation grandissante dans de nombreux quartiers déjà fragilisés. Sur ce dernier point, rares sont ceux qui dénoncent l'emprise des courants religieux sur le domaine scolaire et extra-scolaire. Il suffit seulement de vouloir regarder pour constater le développement exponentiel des associations, notamment musulmanes et affichées comme telles, qui assurent des missions d'enseignement et de soutien scolaire auxquels de plus en plus de parents - non musulmans et de classe dite moyenne - inscrivent leurs enfants. Intérêt idéologique ou religieux ? Non. Seulement une offre de qualité dispensée par des personnes diplômées qu'ils ne trouvent pas ailleurs : d'une part, ils ne rentrent pas dans les critères d'accès (ressources trop élevées pour les dispositifs locaux, ou pas assez pour les organismes privés) ; d'autre part, ces associations sont les rares à assurer un service de proximité et de qualité. Il y a quelques années on parlait de l'emprise des sectes dans le milieu de la formations professionnelle notamment, aujourd'hui, un même phénomène se développe dans l'éducation et le sport avec les associations cultuelles (mêmes causes, mêmes effets, mêmes processus).

Et dans ce marasme que nos autorités sont loin d'imaginer, les policiers sont (avec les municipalités) les derniers interlocuteurs et les seuls exécutoires de la population. La demande de sécurité et d'Etat ne semblent reposer que sur les épaules des forces de l'ordre, acculées et épuisées. Epuisées par des années d'empilement d'instructions sans cohérence. A ce titre, la direction de la sécurité publique en est le plus bel exemple par la vacuité des mesures prises au gré de l'actualité, des marottes des ministres ou de la haute hiérarchie : les plans anti-quelque chose pleuvent de toute part entraînant un nombre considérable d'opérations de contrôle/sécurisation/prévention. Si la présence policière sur le terrain garde évidemment son utilité - non quantifiable - en termes de délinquance, le mille-feuilles des plans et opérations conduit à l'auto - paralysie du système.

Il ne s'agit là que de pur affichage sans examen préalable et simple de la situation : ce qui existe déjà, ce qui fonctionne ou pas. Les zones de sécurité prioritaires (Z.S.P.) sont symptomatiques de ce besoin de surproduction bureaucratique. Présentées comme LA solution pour résoudre la délinquance dans les quartiers les plus difficiles, il s'agissait de créer une cohésion de tous

les partenaires concernés sur le dit territoire qui s'engageaient à y renforcer et concentrer leurs actions, moyens et efforts : le partenariat comme la recette miracle contre la délinquance à grands renforts de CRS ou de gendarmes mobiles.

C'est un échec pour plusieurs raisons. En premier lieu, si les expériences de 1999 avec la police de proximité et les contrats locaux de sécurité, puis de 2007 avec les contrats locaux de sécurité et de prévention de la délinquance (et de la radicalisation depuis peu) ont montré l'immobilisme du système, les ZSP de 2013 n'ont pas fait mieux puisqu'il n'y a toujours pas plus de véritable réflexion et refonte des politiques.

En second lieu, les ZSP n'ont rien changé, rien inventé sur les territoires concernés : la culture et la pratique du partenariat existaient bien avant, certes dépendant des bonnes volontés locales mais existant. Et les organisations déjà évoquées supra qui n'ont jamais joué le jeu du partenariat, n'ont pas modifié leur comportement depuis les ZSP.

S'agissant de la présence policière renforcée, les circonscriptions de police concernées ont reçu au début le renfort des forces mobiles. A ce jour, peu de ZSP en bénéficient encore, et les circonscriptions qui ne sont pas placées sous le feu des projecteurs (telle que Marseille) doivent continuer à faire et « innover » avec leurs propres effectifs.

Quel bilan ? Aucun. La situation ne s'est pas forcément aggravée mais aucune amélioration n'est intervenue et l'on maintient un dispositif contraignant faute d'oser le réformer : le mille-feuilles à la française de dispositifs et de lois qu'on empile sans jamais rien supprimer.

Un mille-feuilles qui dans la police est en train d'imploser. La plupart croit encore en leurs missions mais est épuisée, oscillant entre incompréhension et fatalisme. L'échec des politiques contre la délinquance est criant dans l'indifférence et l'ignorance générales.

Note

* Commissaire de police (sécurité publique) en région parisienne.

BULLETIN D'ABONNEMENT OU DE RÉABONNEMENT

Sécurité Globale

Bulletin d'abonnement ou de réabonnement

À retourner accompagné de votre règlement aux
Éditions ESKA – 12, rue du Quatre-Septembre, 75002 PARIS
Tél. : 01 42 86 55 65 – Fax : 01 42 60 45 35

http://www.eska.fr

M, Mme, Mlle _____ Prénom _____

Société/Institution _____

N° _____ Rue _____

Code postal _____ Ville _____

Pays _____

Adresse électronique _____

TARIFS D'ABONNEMENTS*

	France particulier	France société/ institution	Etranger particulier	Etranger société/ institution
1 an (2017)	❑ 109 €	❑ 138 €	❑ 133 €	❑ 164 €
2 ans (2017 et 2018)	❑ 196 €	❑ 245 €	❑ 235 €	❑ 293 €

* Abonnements souscrits à l'année civile (janvier à décembre).

❑ Je souscris un abonnement pour ❑ 1 an ❑ 2 ans

Je joins mon règlement de _____ Euros

❑ par chèque bancaire à l'ordre des Éditions ESKA

❑ par virement bancaire aux Éditions ESKA – BNP Paris Champs Elysées 30004/00804/ compte : 00010139858 36

❑ par carte bancaire : merci d'indiquer votre numéro de compte et la date d'expiration

N° carte bancaire : ❑ Visa ❑ Eurocard/Mastercard

|_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|

Date d'expiration : |_|_|_|_| Signature :

Derniers numéros parus

Sécurité globale 7 | 2016 (nouvelle série) : Islam activiste, réaction et révolution
Sécurité globale 6 | 2016 (nouvelle série) : Le monde criminel à l'horizon 2025
Sécurité globale 5 | 2016 (nouvelle série) : Dossier Stupéfiants
Sécurité globale 3-4 | 2015 (nouvelle série) : Toujours plus cyber-menacées : les collectivités territoriales / « Police prédictive » : les belles histoires de l'Oncle Predpol
Sécurité globale 2 | 2015 (nouvelle série) : Bandes, Braquages, Terreur
Sécurité globale 1 | 2015 (nouvelle série) : Iran 2015 : Qui gouverne à Téhéran (et comment) ?
Sécurité globale 25-26 | 2013 : La France face à ses ESSD
Sécurité globale 24 | 2013 : Cyber : la guerre a commencé (2e partie)
Sécurité globale 23 | 2013 : Cyber : la guerre a commencé (1re partie)
Sécurité globale 22 | 2012 : La Suisse : nation militaire
Sécurité globale 21 | 2012 : L'eau, enjeu de sécurité et de développement

ÉDITIONS ESKA
12 rue du Quatre-Septembre - 75002 Paris, France
Tél. : 01 42 86 55 65 | Fax : 01 42 60 45 35
http://www.eska.fr