Gendarmerie, numérique et police judiciaire

Histoire, voies et moyens de la cybersécurité au sein de l'institution

Par Fabrice Crasnier

L'histoire contemporaine de la gendarmerie nationale est jalonnée de tournants technologiques importants qu'elle a su négocier afin de toujours mieux honorer ses missions, notamment celles de service public. Les gendarmes du 20e siècle se mettent ainsi très tôt au diapason des technologies innovantes : dès 1921 est créé le Centre technique et scientifique de la gendarmerie nationale (CTSGN), qu'abritera le fort de Rosny-sous-Bois jusqu'en 2015. Le service d'information le plus célèbre fut, entre 1968 et 2016, le Centre national d'information routière (CNIR), organisme interministériel (Défense, Intérieur et Écologie) plus connu du grand public sous le nom de *Bison futé*, chargé du recueil, du traitement et de la diffusion, à partir de Rosny, de l'information routière vers les usagers, les médias et les autorités. Mais le fort de Rosny-sous-Bois a également abrité les trois principales entités liées à la cybersécurité du système d'information de la gendarmerie et à la poursuite des infractions pénales, sujet qui nous occupera prioritairement ici.

Il convient sans doute de rappeler d'entrée que le mot *cybersécurité* est un néologisme désignant, pour des États comme pour les organisations, l'ensemble des règlements ou des lois, des politiques, outils, dispositifs, méthodes de gestion des risques, concepts et mécanismes de sécurité, mais encore des actions, formations, bonnes pratiques et technologies, qui peuvent être appliqués ou utilisés pour protéger les personnes et les actifs informatiques existants, matériels et immatériels, connectés directement ou indirectement à un réseau. Le but est de garantir ou sauvegarder la disponibilité, l'intégrité, l'authenticité et la confidentialité d'une communication ou d'une transaction, sa preuve et sa "non-répudiation", c'est-à-dire l'impossibilité, pour une personne ou entité engagée dans un échange par voie informatique, de nier en être l'émettrice ou la réceptrice. Quant à la *cybercriminalité*, elle se définit comme l'ensemble des infractions pénales commises par le biais d'un moyen informatique au travers du réseau Internet.

Gendarmerie et traitement de l'information : besoins et antécédents

Le Service du traitement de l'information de la gendarmerie (STIG) est, selon l'article Wikipédia le concernant, l'entité qui assure la production, l'exploitation et l'intégration des applications informatiques sur le *Data Center* de la gendarmerie nationale. Ce service est certifié ISO-20000[1] et ISO-27001[2] et dispose actuellement d'une plate-forme de très haute

[1] L'ISO/CEI 20000, issue de la norme BS 15000 de BSI (British Standards Institution), est une norme de certification des services informatiques des organisations prouvant le respect de normes de qualité éditées au travers de phases, de contrôles et de procédures mises en place.

[2] L'ISO/CEI 27001 est une norme internationale de sécurité des systèmes d'information de l'ISO et la CEI. Publiée en octobre 2005 et révisée en 2013, son titre est "Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences". Elle fait partie de la suite ISO/CEI 27000 et permet de certifier des organisations.

Publié/ published in ***Res Militaris*** (http://resmilitaris.net), hors-série "Gendarmerie", novembre 2019

disponibilité appelée IPMS, pour "Infrastructure de production mutualisée et secourue". Le STIG assure la cybersécurité du système d'information de l'institution ; il assume en outre la fonction "support" dans le combat contre la délinquance numérique. La chaîne SIC est une composante intégrée et indissociable de l'action opérationnelle permanente de la gendarmerie. Elle assure aussi la gestion du parc des équipements et le pilotage des supports de proximité, grâce à quelque 2 700 policiers et gendarmes sur l'ensemble du territoire, pour plus de 245 000 utilisateurs.

Parmi les nombreuses missions de la gendarmerie, la police judiciaire occupe une place majeure : elle y consacre près de 40% de son activité quotidienne. La police judiciaire consiste à rechercher les infractions à la loi pénale, à les constater, à en rassembler les preuves et à en rechercher les auteurs. Le fort de Rosny-sous-Bois a abrité, entre sa création (le 28 avril 1976) et l'été 2015, le Service central de renseignement criminel (SCRC),[3] organisme central de police judiciaire de la gendarmerie française qui a pour mission de centraliser et d'exploiter les informations judiciaires relatives aux crimes et délits ainsi qu'aux recherches de personnes et de véhicules qui lui sont transmises par l'ensemble des unités de gendarmerie. Ces informations sont recueillies dans le but de recenser les phénomènes criminels, afin notamment de procéder à des rapprochements en matière de modes opératoires ou de typologie criminelle. Le SCRC gère par ailleurs les bases de données judiciaires de la gendarmerie et entretient des relations avec de multiples acteurs publics (police nationale, douanes, Interpol, Europol, etc.) ou privés (associations de victimes, constructeurs automobiles, centres de recherches, etc.), nationaux ou internationaux. Le SCRC est le service chargé de la fonction "enquête" dans la lutte contre la cybercriminalité.

Certains dossiers criminels à forte complexité ont fait émerger le besoin d'expertise dans la police judiciaire. Ainsi, apprenant de ses erreurs passées dans ce domaine, l'institution a mis en place, le 23 février 1987, toujours au fort de Rosny Rosny-sous-Bois, l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN). Ce centre d'expertise est chargé des aspects scientifiques des investigations avec pour missions d'analyser des prélèvements effectués sur le terrain par des personnels spécialisés appelés "techniciens en identification criminelle" (TIC), de soutenir et d'assister les unités de terrain lors d'enquêtes complexes, et d'assurer la formation et la recherche. L'ensemble de ses missions explique l'appellation d'Institut et non de Laboratoire. Il s'agit là du troisième acteur, chargé de la fonction "expertise" dans l'établissement de la preuve numérique, intervenant dans la prise en compte de la sécurité du système d'information.

Ainsi, dès les années 1970 et 1980, la gendarmerie nationale met en place les briques institutionnelles qui lui permettront d'assurer la continuité du service numérique, et de faire face aux nouvelles technologies à venir. Elle a su rester à l'écoute de la société tout en poursuivant son évolution. Mais à la fin des années 1990, un phénomène nouveau s'impose au monde : Internet.

---

[3] Anciennement STRJD : Service technique de recherches judiciaires et de documentation.

Internet et sa prise en charge au sein de la gendarmerie

Internet est le réseau informatique mondial accessible au public via divers moyens de communication électronique, filaire (réseau téléphonique commuté à bas débit, ADSL, fibre optique jusqu'au domicile), ou sans fil (WiMAX, par satellite, 3G+, 4G, ou 5G). Un internaute est une personne qui utilise un accès à la Toile, obtenu grâce à un fournisseur d'accès Internet (FAI). Sans centre névralgique, Internet se compose de millions de réseaux aussi bien publics que privés, universitaires, commerciaux et gouvernementaux, eux-mêmes regroupés en réseaux autonomes. L'information est transmise via Internet grâce à un ensemble standardisé de protocoles de transfert de données, qui permet à des applications variées (courrier électronique, messagerie instantanée, pair-à-pair et World Wide Web) de communiquer. C'est avec l'apparition du *Web* qu'Internet s'est popularisé. Ce n'est qu'à partir de la deuxième moitié des années 1990 que ce "réseau des réseaux" connaît une plus large diffusion en France. Selon l'INA,[4] si en 1995 l'on ne comptait qu'entre 200 000 et 300 000 internautes, ils seront environ 6,3 millions en 2001 et près de 15,6 millions à la fin de l'année 2003. L'année 2004 marque véritablement l'entrée de la France dans l'ère du numérique, puisque 31% des ménages ont alors accès à Internet, soit cinq fois plus qu'en 1999.

Devant cette croissance exponentielle, la gendarmerie s'est aussitôt adaptée et n'a pas attendu l'explosion de 2004 pour mettre en place un dispositif adéquat. Dès la fin de l'année 1992, le Département informatique-électronique (INL) est créé au sein de l'IRCGN et est hébergé sous les arches servant d'atelier dans le fort de Rosny-sous-Bois. Si ce département n'avait pas les moyens d'aujourd'hui, il devait déjà couvrir l'ensemble des domaines d'expertise liés à la preuve numérique. Il intervient sur tous types de supports, en particulier sur les disques durs et les téléphones portables découverts lors des enquêtes judiciaires. Il assure également des expertises judiciaires et des examens scientifiques au profit des magistrats et des enquêteurs, qu'il est en mesure d'assister sur le terrain ou à distance, lors de perquisitions ou d'auditions en milieu complexe. Le département est structuré aujourd'hui en quatre unités d'expertise ayant pour objet l'extraction de données, le traitement de l'information, les réseaux et télécommunications, et le soutien opérationnel. Intervenant dans de nombreuses formations en rapport avec le domaine des technologies numériques pour la gendarmerie comme pour d'autres administrations, il requiert un haut niveau de qualification de la part des personnels qui le composent. Les ingénieurs et techniciens qui y servent sont ainsi astreints à une remise à niveau permanente et à une veille technologique constante. Le Département développe également des liens riches et fructueux avec de nombreuses organisations internationales (Interpol, Europol, ENFSI,[5] etc.).

---

[4] L'Institut national de l'audiovisuel (INA) est un établissement public à caractère industriel et commercial français, chargé notamment d'archiver les productions audiovisuelles, de produire, d'éditer, de céder des contenus audiovisuels et multimédias à destination de tous les publics, professionnels ou particuliers, pour tous les écrans. L'INA est également un centre de formation et de recherche qui vise à développer et transmettre les savoirs dans les domaines de l'audiovisuel, des médias et du numérique.

[5] European Network of Forensic Science Institutes, dont le siège central est à Wiesbaden, en Allemagne.

Dès 1998, la gendarmerie nationale a identifié l'enjeu que représentent les nouvelles technologies en mettant en place des structures et des formations adaptées. En effet, la montée en compétence du Département d'expertise (INL) a fait émerger un besoin d'enquête sur le cyberespace. C'est ainsi que fut créé le Département cybercriminalité du Service technique de recherches judiciaires et de documentation (STRJD) qui assurera la surveillance du réseau en recherchant les infractions portant atteinte aux personnes et aux biens. Ces infractions relatives à la transmission de données à caractère illicite sur Internet (sites, réseaux IRC,[6] *newsgroups*, réseaux d'échanges communautaires, *peer-to-peer*[7]). Devant le nombre croissant de dossiers sur la pédopornographie, en octobre 2003, la gendarmerie s'est vu confier la charge de mettre en œuvre, à Rosny-sous-Bois, le Centre national d'images pédopornographiques (CNAIP) en collaboration avec la police nationale.

Dans cet élan, la première formation judiciaire sur Internet a lieu au sein du département INL en 1999. Une quinzaine de militaires de la gendarmerie sont conviés à assister à cette formation apportant un nouvel éclairage sur un épiphénomène naissant, la commission d'infractions au travers du réseau Internet. Ces futurs enquêteurs du Web étaient des volontaires qui se sont immédiatement attelés à la traque de diffuseurs d'images à caractère pédopornographique mettant en scène des mineurs sur les réseaux IRC. Cette formation donnera naissance à une nouvelle génération d'enquêteurs dans les unités de recherches, les N-TECH, pour nouvelles technologies, à partir de 2001. Il faut rappeler que les premiers enquêteurs spécialisés en investigation numérique ont été assistés des années durant par des militaires du département SIC particulièrement experts dans la connaissance des systèmes d'information qu'ils gèrent au quotidien. Ces derniers ont apporté un soutien important dans les investigations sur les réseaux et serveurs à perquisitionner.

Une formation spécifique dans le domaine des nouvelles technologies est mise en place après 2002 au profit d'enquêteurs spécialisés "N-TECH", d'abord au Centre national de formation de police judiciaire (CNFPJ), à Fontainebleau, puis à l'Université de Troyes, où cette formation deviendra diplômante. À l'issue, les stagiaires rejoignent leur unité de recherches, dotés d'un matériel spécifique dénommé "lot enquêteur". À raison de 30 enquêteurs formés chaque année, la gendarmerie dispose depuis 2008 d'environ 200 enquêteurs spécialisés au sein des unités dédiées de la chaîne territoriale.

Au fur et à mesure de la montée en compétence, deux missions sont clairement apparues, l'une dédiée à l'enquête judiciaire proprement dite, l'autre à l'analyse des supports. Il a donc fallu reconstruire à l'échelon régional ce qui existait à l'échelon central. Dès lors que les unités territoriales et les unités de recherches étaient confrontées à ce type d'infractions, ces enquêteurs pouvaient bénéficier du concours des N-TECH des unités de

---

[6] Internet Relay Chat (en français, "discussion relayée par Internet") est un protocole de communication textuel sur Internet. Il sert à la communication instantanée principalement sous la forme de discussions en groupe par l'intermédiaire de canaux de discussion, mais peut aussi être utilisé pour de la communication de un à un. Il peut par ailleurs être utilisé pour faire du transfert de fichier.

[7] Le *peer-to-peer* (souvent abrégé en "P2P"), en français "pair-à-pair", est un modèle d'échange où chaque entité du réseau est à la fois client et serveur, contrairement au modèle client-serveur. Les termes "pair", "nœud", et "utilisateur" sont généralement utilisés pour désigner les entités composant un système pair-à-pair.

recherches formés à la lutte contre la cybercriminalité. Pour répondre aux besoins grandissants d'analyse de supports numériques, un nouveau type d'unité est créé en 2005, les Brigades départementales de renseignement et d'investigations judiciaires (BDRIJ). Ces brigades sont implantées au chef-lieu de chaque groupement départemental de gendarmerie, dont elles constituent le pôle criminalistique. La concentration des effectifs de techniciens en criminalistique (techniciens en investigations criminelles, N-TECH, etc.) au sein de ces unités favorise les échanges d'expériences techniques, la pérennisation des savoir-faire et des compétences ainsi que le rapprochement avec les unités de terrain.

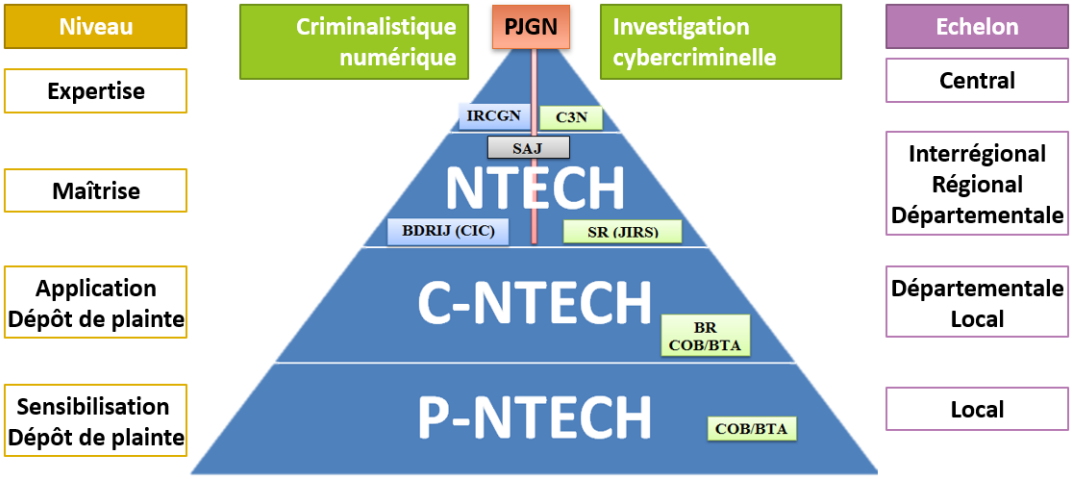
Malgré tous les moyens déployés pour lutter contre la cyberdélinquance, des demandes d'enquête toujours plus nombreuses ont très vite débordé la capacité de traitement des enquêteurs spécialisés. De nouvelles ressources avec des compétences intermédiaires devaient venir rapidement en soutien. C'est ainsi que les "correspondants en technologies numériques" (C-NTECH) ont été mis en place au sein des brigades territoriales et dans les unités de recherches. Ils procèdent aux saisies et à la mise sous scellés des objets lors des perquisitions. Ils sont habilités à réaliser des analyses simples sur des téléphones, à vérifier les données accessibles sur un ordinateur et à perquisitionner les ordinateurs en fonction lors des perquisitions. Enfin, ils préparent l'intervention du N-TECH en garantissant la non-dénaturation des preuves numériques. Depuis peu, cette chaîne s'est enrichie avec la formation en *e-learning* de "Premiers intervenants en technologies numériques" (P-NTECH). Sensibilisé à la problématique de la cybercriminalité, le P-NTECH peut prendre une plainte concernant une infraction de droit commun ayant comme moyen principal les systèmes d'information et de communication, telle l'usurpation d'identité en vue de commettre une escroquerie par Internet. Le C-NTECH et le P-NTECH obtiennent, dans les cas simples, des résultats plus rapides pour le directeur d'enquête et allègent considérablement le travail de l'enquêteur N-TECH. L'arrivée de ces renforts en enquêteurs numériques permet également d'accroître la somme globale de connaissances au sein de la communauté numérique judiciaire, et d'identifier de potentiels futurs N-TECH, voire experts, de la chaîne cyber.

L'évolution technologique ne faisant pas de pause, de nouveaux besoins sont apparus pour lutter contre les phénomènes cybercriminels, et la Gendarmerie nationale s'est une fois de plus dotée d'une nouvelle structure pour faire face au problème posé : le Pôle judiciaire de la Gendarmerie nationale (PJGN), créé le 1er janvier 2011, composé d'environ 600 personnes et doté d'une capacité de projection sur le terrain lors de faits les plus graves. Initialement installé au fort de Rosny à Rosny-sous-Bois, le PJGN déménagera en mai 2015 dans de nouveaux locaux à Pontoise. Avec l'arrivée de cette nouvelle entité, le département cybercriminalité se transforme en Centre de lutte contre les criminalités numériques (C3N). Ce centre pilote et anime le réseau CYBERGEND (communauté numérique judiciaire), composé de 3 500 gendarmes spécialisés en technologie numérique, formant un réseau de proximité au niveau local ("référents Cyber"), de spécialistes au niveau départemental (Cyber N-TECH), et d'experts au niveau national (PJGN). Aux côtés des bureaux *ad hoc* de la DGGN et de l'IRCGN, il contribue à définir les politiques de

formation et d'équipement des gendarmes en matière cyber, et à harmoniser outils (p.ex. : le manuel des opérations N-TECH) et méthodes de travail. Il administre le site intranet *Cyber-Aide* (8 000 fiches pratiques, 5 000 visiteurs distincts par semaine), le forum des enquêteurs spécialisés, ainsi qu'une liste de diffusion par courriel. La nouvelle organisation centrale a également entraîné une nouvelle organisation de certaines entités locales sur le terrain, et mené à la modification de certains services des sections de recherches : cette nouvelle compétence sera attribuée aux SR des chefs-lieux de Juridiction inter-régionale spécialisée (JIRS).[8] Une plateforme CYBER, constituée de quatre à six N-TECH est alors créée pour répondre à ces nouvelles missions. S'agissant d'Internet, une nouvelle formation OSINT est également proposée aux militaires de ces unités, qui auront vocation à exercer une surveillance ciblée du réseau en liaison avec le C3N.

Cette surveillance ciblée sera indispensable avec la montée de la radicalisation dans les réseaux sociaux, et prioritaire en 2015 après les attaques de l'État Islamique sur le territoire national. En parallèle, dans les régions confrontées à une forte activité judiciaire, les Sections d'appui judiciaire (SAJ) de la gendarmerie font progressivement leur apparition dans le paysage entre 2012 à 2016. Ces unités ne se substituent pas aux autres formations, mais apportent un appui dans le cadre de la subsidiarité. Elle sont constituées de deux entités : la Division observation et surveillance (DOS), et la Division analyse criminelle et investigations spécialisées (DACIS). Cette dernière est pluridisciplinaire et comprend des personnels en charge de la cybercriminalité (N-TECH et C-NTECH), de l'analyse criminelle (ANACRIM opérationnel et ANACRIM stratégique), de la coordination des scènes de crime (COCRIM régionale), de la mise en place de moyens spéciaux liés aux supports vidéo (VIDEO PJ), et d'une cellule des avoirs criminels (CERAC). Elle intègrera progressivement les sections d'analyse du renseignement (SAR).

Structure pyramidale du réseau CYBERGEND



[8] Les Juridictions inter-régionales spécialisées (JIRS) regroupent des magistrats du parquet et de l'instruction et sont spécialisées en matière de criminalité organisée, de délinquance financière mais aussi pour les affaires dont la complexité justifie des investigations importantes (meurtres commis en bande organisée, blanchiment, crimes aggravés d'extorsion...).

Cette chaîne de lutte contre la criminalité numérique permet de mener toutes les formes d'enquête dans ce domaine avec des moyens en matériel et en personnel adéquats. Toutefois, devant une cyberdélinquance hautement évolutive et polymorphe, l'adaptabilité est requise. Le réseau CYBERGEND répond à cette exigence, et est en mesure de faire face à la cybercriminalité présente et, on peut l'espérer, à venir dans toutes les zones sombres du cyberespace.

La lutte contre la cybercriminalité et l'action en faveur de la cybersécurité vues de l'intérieur

Un aperçu de la pratique des enquêteurs ou des acteurs de la sécurité numérique, et de l'expérience qu'ils ont acquise au fil des ans, viendra utilement compléter cet historique de l'évolution de la gendarmerie nationale dans le domaine du "cyber". On pardonnera à l'auteur de ces lignes d'utiliser pour ce faire son vécu de praticien, et de donner à son exposé un tour plus personnel.

Au service de la police judiciaire

J'ai eu l'honneur de vivre 27 années d'évolution de la gendarmerie en la matière au travers d'une carrière d'enquêteur de police judiciaire, dont 17 en tant qu'enquêteur N-TECH. J'ai ainsi pu observer la progression et l'évolution des compétences de l'institution au regard des phénomènes liés à la cybercriminalité.

En 2000, une première approche de l'enquête numérique conduit à la création d'un stage Internet. À cette époque, les moyens de communication sur Internet se limitaient aux *newsgroups* et aux IRC,[9] tandis que les investigations étaient orientées vers les infractions de détention et de diffusion d'images à caractère pornographique mettant en scène des mineurs. De nombreuses images de ce type étaient échangées sur les IRC, et il fallait intervenir. Bien que qualifiées, les infractions pénales ne pouvaient être traitées sans une caractérisation de leur élément matériel, ce qui n'était pas chose aisée. L'enquête sous pseudonyme n'existant pas à l'époque, il a fallu redoubler d'imagination et de débrouillardise, ce dont en l'occurrence les gendarmes impliqués n'ont pas manqué. L'adjudant Philippe Jarlov, de la section de recherches de Bordeaux, a fait appel à un informaticien, Frédéric Aidouni, pour pouvoir utiliser un nouveau logiciel, "LogIRC", afin de matérialiser les preuves numériques. *L'investigation numérique sur le Web était née*. Dans la foulée est apparu un nouveau média d'échange de données, le P2P,[10] qui permettait la diffusion de très grandes quantités d'images, possibilité dont les amateurs de vidéos pédopornographiques n'ont pas tardé à se saisir. Les informaticiens ont alors réagi très vite, grâce à la mise au point du logiciel "LogP2P" permettant la surveillance ("*monitoring*") et l'analyse des données échangées.

Forte de cette expérience, la gendarmerie a investi dans une première formation numérique lancée en décembre 2001 sur la base du volontariat. Toutefois, il est très vite

[9] *Cf.* note 6 *supra*, p.4.
[10] *Cf.* note 7 *supra*, p.4.

devenu évident qu'un pas de plus vers une professionnalisation était requis. C'est ainsi qu'après une série d'examens écrits et oraux, 15 enquêteurs d'unités de recherches et de services centraux intègrent en juin 2002 le stage N-TECH pour obtenir la qualité d'"investigateur en technologie numérique".

C'est à cet instant qu'a officiellement débuté ma carrière d'enquêteur judiciaire numérique. À l'issue d'une formation de six semaines, les stagiaires dont j'étais sont repartis dans leurs unités d'emploi avec de nouvelles connaissances sur la délinquance informatique, un peu plus tard rebaptisée "cybercriminalité", mais hélas sans matériel pour mener leurs investigations. En revanche, nous étions riches d'un nouveau tissu relationnel, et de logiciels "*open source*" que nous avions partagés en fin de formation. Le CDROM qui les contenait nous a permis de commencer notre travail de lutte avec de grandes ambitions. Quelques mois plus tard, un outillage d'investigation numérique dernier cri nous fut alloué pour aborder les dossiers cyber. La prise en compte de ce nouveau, et extraordinaire, matériel a pris un peu de temps, mais notre attente fut récompensée. Une machine puissante, accompagnée de tous les périphériques d'investigation numérique du moment, allait en effet nous permettre de réaliser des investigations sur tous les supports numériques. Nous appellerons plus tard ce travail "analyse post-mortem", en référence à l'investigation criminalistique sur les corps. Pour pallier le relatif isolement de ces nouveaux enquêteurs, le capitaine Éric Freyssinet, alors en poste au Département INL de l'IRCGN, crée un forum vite appelé "Communauté N-TECH", où nous partageons retours d'expérience, logiciels à connaître et expertise de chacun, auxquels viendront bientôt s'ajouter les mémoires des étudiants N-TECH de l'Université de Troyes, ainsi que de nombreux tutoriels d'investigation.

Les supports numériques, les ordinateurs fixes et portables ainsi que les téléphones s'amoncelaient dans mon bureau à la Section de recherches de Toulouse au sein du groupe DEFI chargé de la délinquance économique et financière. La spécificité des enquêtes numériques et le besoin toujours croissant d'assistance m'a conduit, en 2004, à créer le groupe N-TECH au sein de cette même section de recherches afin de répondre aux besoins des enquêteurs. Le travail y consistait à assister ces derniers dans leurs perquisitions et dans leurs investigations numériques sur les supports saisis. Je devais également suivre mes propres saisines du parquet qualifiant des infractions dont l'objet était le numérique. Nombre de ces saisines revêtaient un aspect financier, ce qui rendait précieuse ma formation DEFI. Une de ces enquêtes m'a notamment amené en 2005 à prendre la direction de la première enquête numérique de la JIRS de Bordeaux, en l'occurrence sur une escroquerie numérique ayant engendré un préjudice de plusieurs millions d'euros par an dans cinq pays européens en quatre ans et plus de 100 millions de dollars aux États-Unis. La gendarmerie montrait ainsi sa capacité de porter des enquêtes numériques au niveau international avec l'appui des organismes européens Europol et Eurojust.

L'activité numérique augmentant chaque année, le groupe N-TECH de la section de recherches a lui aussi évolué, tandis que l'effectif de gendarmes qualifiés N-TECH dans la région Midi-Pyrénées passait de 3 à 11 enquêteurs. Cette évolution a donné naissance à

une nouvelle génération d'"assistants N-TECH" pour répondre à la demande ; nous formions des C-NTECH dans tous les départements de la région pour nous relayer sur le terrain. La machine était en route. Les matériels d'investigation, renouvelés tous les quatre ans, ont suivi en devenant de plus en plus spécialisés (à l'instar de la mallette d'investigation de téléphone numérique *Cellebrite* qui remplaça les cartons de câbles et de connecteurs de téléphones), évolution imprimée par l'apparition des smartphones, lesquels ne sont plus vraiment des téléphones mais des ordinateurs offrant une fonction de téléphonie. Les données qu'ils contiennent doivent être extraites et analysées dans le temps de la garde à vue, tâche qui pour cette raison est de plus en plus difficile à mener. L'information numérique est périssable, et les délais à tenir absolument sont un enjeu important pour la réussite l'enquête judiciaire. À défaut de pourvoir l'analyser sans délai, il faut la protéger contre toute altération ou destruction volontaire ou involontaire. Les processus d'investigation ont donc évolué pour faire face à ce nouvel impératif, notamment avec la formation des NTIC (N-TECH en laboratoire) et des N-TECH en unité de recherches.

Quittant la Section de recherches de Toulouse après onze ans d'investigations, j'ai rejoint, à sa création en 2013, la Section d'appui judiciaire (SAJ) dans cette même ville pour prendre la direction de la Division d'analyse criminelle et d'investigations spécialisées. Cette unité, dont la fonction était alors à peine ébauchée et restait à définir au-delà de ses grandes lignes, était un véritable laboratoire d'expérimentation pour l'assistance judiciaire au sein de la région de gendarmerie Midi-Pyrénées. Une division DACIS, dotée de moyens exceptionnels avec une équipe de huit enquêteurs spécialisés en matière de technologie avancée ("IT forensics", "cyber infiltration"), d'analyse criminelle, de coordination criminalistique, d'avoirs mal acquis et d'analyse vidéo, était une formidable opportunité. Nous avions un outil d'assistance et d'enquête surpuissant pour expérimenter de nouvelles pistes d'investigation. Je me suis donc consacré au processus de rédaction de la procédure judiciaire permettant, dans le cadre d'enquêtes sous pseudonyme, de se diriger le plus vite possible vers une réponse pénale, avec présentation immédiate devant le tribunal.

L'enquête sous pseudonyme a fourni le cadre juridique d'action, et le binôme que je formais avec l'adjudant Gilles Berdinelles, "C-NTECH infiltré", a permis en moins d'un an d'arrêter et d'incarcérer sept pédophiles agissant sur le Net depuis Toulouse. Notre mode de fonctionnement permettait en deux mois de matérialiser les faits et, lors de la garde à vue, d'analyser les supports pour consolider les éléments recueillis lors de la phase d'infiltration. La rédaction d'un procès-verbal circonstancié permettait aux magistrats du parquet une lecture immédiate des éléments d'incrimination et la présence de données justificatives permettait, au moment de la phase de jugement, au Président du tribunal ou de la Cour d'avoir une lecture totale de la procédure avec des incriminations justifiées voire imagées.

Au service de la cybersécurité

Cet exposé serait incomplet si, quittant pour finir la traque et la répression des cybercriminels, je n'évoquais brièvement l'autre volet, envers du premier, de l'action de la gendarmerie en matière de cyber : les mesures et programmes de prévention et de défense

contre les attaques dont victimes sites et réseaux de la part d'escrocs, mais encore d'États étrangers ou d'associations d'activistes diversement déterminés à promouvoir une cause y compris par des moyens illicites, ou à subvertir l'ordre social existant. Il m'a été donné, au cours des trois dernières années de ma carrière, d'aborder ce second aspect, celui de la cybersécurité au sens strict, lorsque me fut confiée la charge d'animer le Relais Occitanie de la Réserve citoyenne cyberdéfense (RCC). Cet épisode et ce qu'il m'a montré me semblent avoir valeur d'exemple de ce qui peut se faire, et se fait, ailleurs sur le territoire national dans ce domaine, notamment avec le concours de la gendarmerie nationale.

J'ai découvert à cette occasion l'intérêt et la pertinence du rôle que jouent en ce domaine les réservistes, qu'ils soient membres de la Réserve citoyenne, de la Réserve opérationnelle ou de la Réserve scientifique, qui prennent sur leur temps de manière désintéressée pour faire œuvre hautement utile. Au sein de la région Midi-Pyrénées, cette action s'est orientée dans trois directions-clés de la cybersécurité : la sensibilisation de l'opinion aux menaces cyber et aux moyens d'y parer, l'aide apportée aux entreprises soucieuses d'évaluer leurs dispositifs de prévention et de réponse face aux attaques numériques, et l'enrichissement, assorti d'un ciblage local, des modalités de communication au service de la sécurité numérique. Trois groupes de travail furent créés au fur et à mesure des demandes, chacun prenant en charge l'une de ces orientations, épaulés par des personnels d'active de la gendarmerie départementale et des transports aériens.

Le premier groupe, cherchant à faire de la cybersécurité une priorité nationale, s'est notamment concentré sur les aspects régaliens et stratégiques. Il a participé à toutes les manifestations régionales de sensibilisation (débats, fédération d'initiatives locales, etc.), et organisé la sienne propre à Fleurance, dans le Gers, autour du thème "Cyberdéfense & Territoires", pour faire comprendre que le cyberespace est partout et concerne tout le monde – événement que des autorités venues de Paris ont honoré de leur présence.

Le deuxième groupe s'est attaché à répandre auprès des entreprises de la région le recours à l'aide que fournissent les outils mis au point par l'Agence nationale de la sécurité des systèmes d'information (ANSSI[11]), et à son propre tableau de bord de sensibilisation aux dangers numériques. Son action a pris un tour très concret avec le lancement du projet "AerospaceValley" d'aide en matière de cybersécurité aux entreprises du secteur aéronautique implantées dans le bassin toulousain. Ces actions ont été suffisamment appréciées pour attirer l'attention des responsables nationaux de l'ANSSI, qui n'ont pas hésité à venir assister à l'une de ses réunions mensuelles à Toulouse.

Le dernier groupe de travail s'est tourné vers la mobilisation d'énergies et de compétences particulières locales au service d'une communication innovante en direction des secteurs les plus exposés aux menaces numériques, notamment celui de la "cyber-aérodéfense".

---

[11] L'ANSSI, créée par décret en juillet 2009, est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

De façon remarquable, tous ces efforts ont bénéficié du concours sans réserve des services déconcentrés locaux de l’État dont la vocation inclut, à un titre ou à un autre, la prévention et la défense numérique : Direction du renseignement et de la sécurité de la défense (DRSD), Direction générale de la sécurité intérieure (DGSI, ex-DCRI), Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l’emploi (DIRECCTE). Toutes choses qui m’ont convaincu qu’il n’y a pas à désespérer, loin de là, du système mis en place tant que ne feront pas défaut les ressources, la bonne volonté et l’enthousiasme de ceux qui lui permettent de fonctionner.

Au total et avec le recul, il m’apparaît que rien de ce qui a été accompli en matière tant de lutte contre la criminalité numérique que de cybersécurité préventive ou défensive, n’aurait pu l’être sans l’assentiment et les encouragements d’une chaîne hiérarchique qui, sur toute sa longueur – de mes chefs immédiats jusqu’à ceux qui occupaient les sommets –, en avait bien saisi les enjeux. Ce qui ne veut pas dire qu’il n’y eut jamais de difficultés. Mais comme d’autres, j’ai pu travailler, construire, apprendre, surmonter les obstacles sans jamais me lasser. Ce métier qui fut le mien, celui d’enquêteur en cybercriminalité puis d’animateur d’une équipe de haut vol attachée à la sécurité numérique, fut passionnant, riche et indéniablement utile à la société face aux problèmes technologiques que pose l’enquête judiciaire, aux travers d’usages qu’il est indispensable de réguler, aux escroqueries et malveillances à réprimer, ou aux menées hostiles contre lesquelles il convient de se prémunir.

Conclusion

Tout au long du siècle dernier, la gendarmerie nationale a su montrer sa pleine capacité d’adaptation aux nouvelles technologies. Elle a joué, au tournant du présent siècle, un rôle de précurseur dans le domaine numérique en prenant très rapidement conscience des enjeux de la cybersécurité. Cette évolution n’a été rendue possible que parce que notre institution est bien la “force humaine” qu’elle prétend être – c’est son slogan préféré –, et qu’elle sait mobiliser les énergies de militaires passionnés par leur métier, en l’occurrence ici celui du numérique. Quel que soit leur domaine de compétence spécialisée, parfois momentanément mal outillés mais toujours emplis de conviction et d’imagination pour avancer, ils ont tous ensemble su faire grandir l’institution, et lui savent gré en retour de leur avoir permis de grandir avec elle.