INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

TRAVAUX DES AUDITEURS

27e Session nationale « Sécurité et Justice » 2015-2016
Groupe de diagnostic stratégique (GDS) n°3

VERS UNE POLICE 3.0 : ENJEUX ET PERSPECTIVES A L'HORIZON 2025

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

JUIN 2016
ISSN 2265-447X

Les membres du groupe de diagnostic stratégique n°3 :

Présidente du GDS : **Claire BERNIER,** *avocate associée, Adsto*

Vice-Président du GDS : **Paul-Mathieu LE GAL-OTTAVIANI,** *Mairie de Paris*

Coordination de la rédaction : Alain IMBERT, *directeur du département recherche & analyses, McKinsey & Company*

Alain PERRAUD, *senior manager Conformité & contrôle, Renault*

Céline BRUNEAU, *journaliste, i-Télé*

Didier CANNESSON, *ingénieur commercial Grands comptes, Morpho*

Philippe CORREOSO, *colonel à la direction du personnel militaire, gendarmerie nationale*

Fadi DAHDOUH, *conseiller municipal de Troyes, ostéopathe*

Jean-Luc FAIVRE, *commissaire divisionnaire, cabinet du Directeur général de la police nationale*

François GARNIER, *directeur adjoint de cabinet du préfet, Préfecture de l'Essonne*

Christian GRAVEL, *préfet, directeur du service d'information du Gouvernement (SIG)*

Christophe GUEGUEN, *directeur des systèmes d'information, Securitas France*

Denis LAURETOU, *directeur de la sécurité, Banque de France*

Thomas LEGRAIN, *associé gérant, Thomas Legrain Conseil*

Kristof DE PAUW, *commissaire divisionnaire, directeur général du Secrétariat administratif et technique de Justice, police belge*

Emmanuel MAGNE, *directeur de la supervision globale, Mairie de Lyon*

Olivier ZAMPHIROFF, *magistrat*

Directeur de la publication M. Cyrille SCHOTT, directeur de l'INHESJ

VERS UNE POLICE 3.0 :
ENJEUX ET PERSPECTIVES
A L'HORIZON 2025

Travaux de la 27e promotion
(2015-2016) de la session nationale
« Sécurité et justice »

Sommaire

SYNTHÈSE

Qu'il s'agisse de la robotique avancée, du véhicule autonome, de l'automatisation des savoirs, de l'informatique quantique ou encore de la réalité augmentée, de nombreuses technologies de rupture vont affecter la société et avec elle, les forces de sécurité, d'ici à 2025. Si la France a commencé à s'y préparer au travers d'un plan de modernisation de la sécurité allouant 108 millions d'euros à cinq défis prioritaires pour la période 2015-2017, de nombreux enjeux restent encore à aborder : collecte d'information et veille sur internet, big data, internet des objets, vidéoprotection intelligente, productivité, ...

Dans le même temps, la délinquance (criminels isolés ou organisations terroristes) a su identifier les « opportunités » que lui offre la révolution numérique, faisant naitre une cyber criminalité aux moyens et aux modes opératoires nouveaux. Nos concitoyens ont eux aussi modifié leurs attentes et leurs comportements, obligeant police et gendarmerie à développer une présence nouvelle sur internet et à entrer dans une nouvelle ère de la communication. Même la relation des forces de sécurité avec le secteur privé est affectée par ces évolutions technologiques (collaboration conjointe aux efforts de R&D des entreprises, participation d'experts aux investigations, contributions – encore modérées – à la construction d'une industrie tricolore de la sécurité intérieure).

Comment nos forces de sécurité abordent-elles cette révolution numérique ? Par le passé, plusieurs projets de transformation technologique de grande ampleur (ACROPOL, terminaux informatiques embarqués, CHEOPS, ...) se sont soldés par des déboires non négligeables, principalement en raison d'une complexité organisationnelle excessive des structures qui en avaient la charge. Ce même manque de lisibilité se retrouve au niveau de la gestion des ressources humaines, où la culture de la transformation n'est pas encore assez présente en dépit d'initiatives intéressantes (officiers commissionnés de la gendarmerie, formation des spécialistes en cyber criminalité, ...) mais limitées.

Reste que la révolution numérique offre une double opportunité : celle d'une « expérience » renouvelée pour nos concitoyens (nouveaux services, nouvelle proximité avec les forces de sécurité, ...), mais aussi celle d'un fonctionnement optimisé (d'où un travail plus riche pour les policiers et les gendarmes, plus pertinent et plus au contact des populations). Les forces de sécurité françaises pourraient ainsi chercher à « *devenir, grâce à l'usage des technologies numériques, l'une des trois forces de sécurité de référence dans le monde, pour leur efficacité et pour la qualité du service offert à tous* ».

Pour concrétiser cette vision, nos préconisations s'articulent autour de huit axes.

- Transformer les structures en s'appuyant sur une vision à long terme : nouvelle loi d'orientation et de programmation, accompagnement du changement, décloisonnement, ...
- Développer les talents déjà présents au sein des institutions : gestion prévisionnelle des emplois et des compétences, filière métier dédiée à l'investigation numérique, ...
- Attirer de nouveaux talents : ouverture des concours, élargissement du champ des officiers commissionnés, interactions avec le monde extérieur, ...
- Mettre en œuvre la stratégie digitale : création d'un poste de directeur digital au sein du ministère de l'Intérieur, dématérialisation des processus, unification des systèmes d'identification et d'authentification, ...
- Muscler les dispositifs d'investigation numérique : dispositif de veille sur le marché des solutions d'investigation numérique, acquisitions de solutions, développement d'une cyber police, ...
- Accélérer et pérenniser les approches prédictives : élargissement des expérimentations y compris en zone de sécurité prioritaire, diffusion de la culture de l'analyse prédictive dans l'organisation, ...
- Moderniser les centres de commandement : intégration des potentialités du numérique dans les appels 17, décloisonnement, intégration des drones, des murs d'images et des réseaux sociaux, ...
- Ouvrir une relation nouvelle avec la population : renforcement des services numériques, encouragement de l'implication citoyenne, ...

Les mutations numériques auxquelles doivent se préparer les forces de sécurité françaises marquent l'absolue nécessité de remettre l'humain, citoyens ou membres des forces de sécurité, au cœur du dispositif et de l'action publique.

INTRODUCTION

Comme l'invention de l'imprimerie, de l'électricité ou de l'informatique, la révolution numérique bouleverse et va continuer à bouleverser profondément et durablement notre société. Parce qu'il crée de nouveaux modes de relation avec le grand public, qu'il optimise l'impact des actions grâce à l'exploitation massive des données, qu'il libère du temps (ou réduit les coûts) par la refonte des processus ou encore, parce qu'il permet de mieux adapter les services rendus, le « big bang digital » nous promet une plus grande efficacité des organisations, des entreprises ou des administrations. Il peut aussi représenter une aspiration positive pour tous ceux qui le mettront en œuvre ou qui en seront les utilisateurs.

La police n'échappera pas à cette mutation. Les initiatives numériques se multiplient partout dans le monde : a New York avec des outils de police prédictive, à Londres ou à Madrid avec l'utilisation d'internet et des réseaux sociaux pour communiquer avec les citoyens, à Tel Aviv avec des caméras de surveillance intelligentes ou à Singapour où Interpol a ouvert son *Global Complex for Innovation* en avril 2015.

Dans son allocution du 30 septembre 2013 aux forces de sécurité françaises, Manuel Valls, alors ministre de l'Intérieur, appelait à travailler sur « *une nouvelle frontière* », celle de « *la police et [de] la gendarmerie 3.0* ». Le ministre affirmait ainsi sa volonté d'anticiper et de préparer le futur par une réflexion prospective autour de thèmes tels que les équipements d'intervention, l'internet des objets, les services en ligne à la population, les outils cartographiques, la police technique et scientifique de masse ou plus prosaïquement, les sources de mutualisation entre police et gendarmerie.

Or, partout dans le monde et quelles que soient les époques, l'histoire de la police montre qu'elle a toujours été en posture d'adaptation réactive et non pas d'évolution proactive. Pourrait-il en être autrement face à la révolution numérique, à laquelle les délinquants, les groupes criminels ou les réseaux terroristes se sont déjà convertis ?

Au fil de leurs recherches et de leurs interviews d'experts, les auteurs de ce rapport ont acquis la conviction que la révolution numérique ne consistait pas en une simple mise à jour technologique, mais qu'elle correspondait, comme le montre la première partie de ce document, à des changements de paradigmes. Face à cela, la réponse ne peut être qu'une révolution culturelle et organisationnelle, détaillée dans notre deuxième partie. Pour l'enclencher, nous formulons dans une troisième partie, organisée autour de 8 grands axes, 30 préconisations dont un tiers pourraient être utilement mises en œuvre à court terme.

Parce qu'il accélère le temps, le numérique force la police et la gendarmerie à s'adapter plus vite encore.

RÉVOLUTION NUMÉRIQUE : DIAGNOSTIC ET PERSPECTIVES

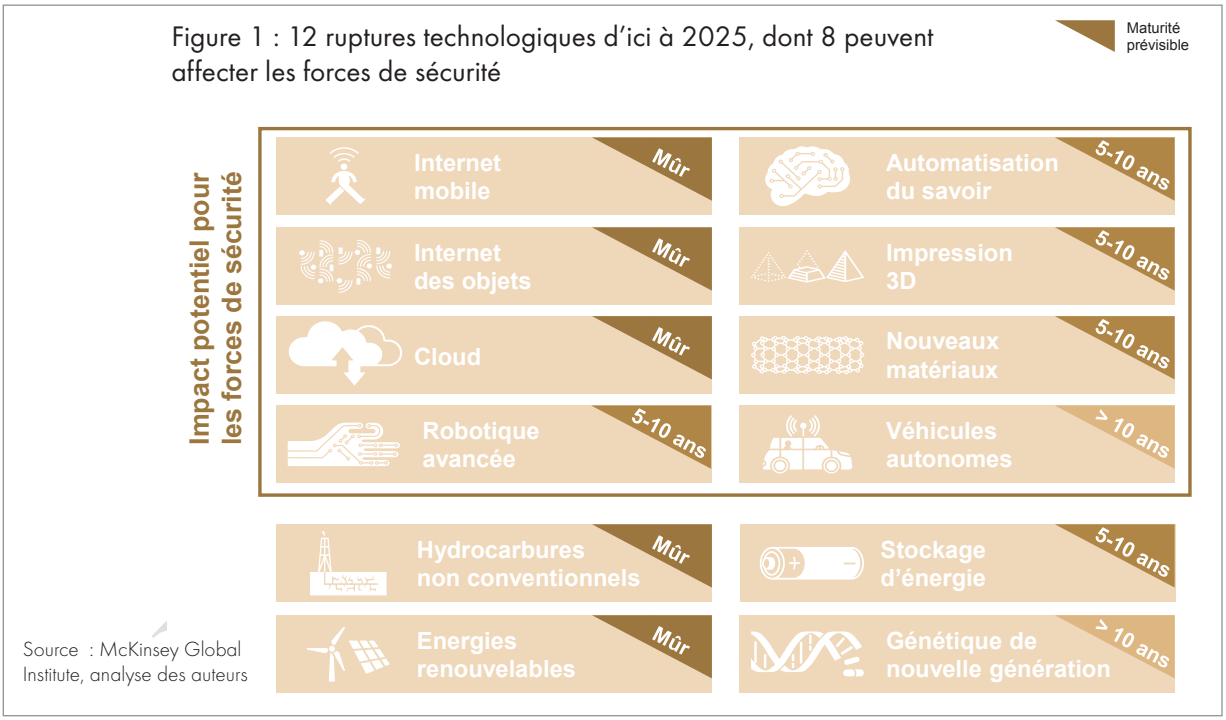
Vers un monde bouleversé par des technologies de rupture

Dans un rapport publié en mai 2013[1], le McKinsey Global Institute identifie douze technologies de rupture susceptibles d'entrainer des transformations radicales de nos sociétés d'ici à 2025. Certaines d'entre elles affecteront directement ou indirectement les forces de sécurité et les exemples d'application n'ont pour limite que notre imagination :

- l'internet mobile permettra l'accès distant à des bases de données ou à des applications métiers de plus en plus consommatrices de bande passante ;
- l'internet des objets pourra devenir une source de renseignement voire de surveillance comme l'est aujourd'hui la téléphonie ;
- la robotique avancée pourrait augmenter les capacités des forces d'intervention (port de charges lourdes, neutralisation, ...) et permettre des collaborations nouvelles entre humains et robots (déminage, surveillance, ...) ;
- le véhicule autonome modifiera l'approche des contrôles routiers ;
- etc.

(1) McKinsey Global Institute *"Disruptive technologies: Advances that will transform life, business, and the global economy"*, Rapport McKinsey Global Institute, mai 2013.

Figure 1 : 12 ruptures technologiques d'ici à 2025, dont 8 peuvent affecter les forces de sécurité



Source : McKinsey Global Institute, analyse des auteurs

La réalité augmentée[2] ouvrira elle aussi des champs nouveaux. Elle permettra par exemple aux opérateurs d'une force d'intervention d'échanger des informations en temps réel (e.g. localisation, présence suspecte, état physique des opérateurs, ...).

(2) Création d'un environnement où se superposent, en plus de notre propre vision ou appréhension d'une scène, des informations issues de sources diverses : lunettes Google, montre interconnectée 6W4U de Thales, ...

Enfin, une autre rupture résidera dans l'informatique quantique. Avec elle, les ordinateurs vont en effet acquérir une puissance de calcul 100 millions de fois supérieure à celle des ordinateurs actuels, ce qui rendra par exemple caduques les chiffrements cryptographiques actuels.

Les acteurs et décideurs de la sécurité intérieure doivent bien évidemment s'interroger sur ces perspectives et ce qu'elles signifient en termes de moyens, mais aussi de modes de travail, de compétences à acquérir ou de formations à développer.

Forces de sécurité, réseaux criminels et société civile : quel impact et quelles utilisations du numérique ?

Le plan de modernisation de la sécurité intérieure

Genèse et ambitions du plan

Pour accélérer l'appropriation par la police et la gendarmerie des évolutions technologiques et des mutations numériques, le ministère de l'Intérieur a constitué en septembre 2013 un groupe de travail sur les technologies de sécurité intérieure (GTTSI). Ses réflexions (perspectives stratégiques à cinq ans et démarche prospective à l'horizon 2025) ont conduit à la remise d'un rapport en juin 2014[3], dont le ministère a validé les axes d'action. Les principaux projets font l'objet d'une programmation et d'un suivi dans le cadre du budget triennal 2015-2017 et une enveloppe de 108 millions d'euros leur est consacrée.

(3) Rapport Delville, « *Les défis technologiques des forces de sécurité intérieure* », juin 2014.

Cinq défis prioritaires

Concrètement, le plan de modernisation de la sécurité (PMS) issu de ces travaux s'articule autour de cinq « défis technologiques » prioritaires que nous avons détaillés ci-après. Si tous paraissent aller dans le bon sens, certains auraient pu afficher plus d'ambition immédiate (les services en ligne aux citoyens, les outils prédictifs, ...).

• *Développer la proximité numérique avec le public :*

En dépit de la volonté affichée d'accentuer et de pérenniser la démarche déjà engagée concernant les usages interactifs des nouveaux supports de communication avec la population (e.g. pré-plainte en ligne, ...), ce volet du plan de modernisation peut sembler manquer d'ambition. Il se résume essentiellement à la plainte en ligne pour les escroqueries commises sur internet et à la possibilité de s'inscrire au dispositif « Opération tranquillité vacances » depuis le site « service-public.fr ». Le volet communication à l'égard du grand public est totalement occulté à ce stade (attractivité du site internet ministériel, présence sur les réseaux sociaux, ...).

• *Unifier les plates-formes de réception des appels d'urgence*

Plus ambitieux est en revanche cet aspect du PMS dans la mesure où il s'agit d'unifier les plateformes de réception des appels d'urgence (17, 18 et 112) au sein de chaque département, à l'instar de l'expérimentation mise en œuvre au sein de la préfecture de police de Paris depuis le printemps 2016. L'objectif consiste à obtenir une coordination plus efficace des services (police, gendarmerie et pompiers), à assurer une meilleure prise en compte de l'urgence vitale (y compris en filtrant davantage les appels non-urgents) et à garantir une plus grande efficience de la gestion des crises, tout en allégeant les coûts financiers et en effectifs grâce à la mutualisation.

• *Les solutions de mobilité (équipements numériques)*

Il s'agit ici de doter chaque policier et gendarme intervenant sur la voie publique d'un terminal mobile sécurisé susceptible d'accueillir les outils nécessaires : accès aux fichiers, à la messagerie, à certaines applications stratégiques (procès-verbal électronique, logiciel OCTET pour la répression des infractions à la coordination des transports, ...) mais aussi à internet. Ces terminaux se présentent sous la forme de tablettes et de smartphones fonctionnant sous une version Android sécurisée par l'ANSSI (Secdroïd).

Dans ce cadre et consciente du caractère obsolète de l'actuel terminal informatique embarqué (TIE), la gendarmerie expérimente dans le département du Nord depuis fin 2015 et en lien avec la police nationale, un nouvel équipement numérique baptisé Neogend (Neo pour l'équipement de la police). Le gendarme ou le policier n'est plus obligatoirement lié pour tous ses actes à son bureau et retrouve ainsi davantage de liberté d'action. Grâce aux outils intégrés, Neogend et Néo permettent d'interagir avec des correspondants internes et externes, facilitent les constatations d'infractions, les interrogations de fichiers, l'accès aux diverses messageries, la verbalisation des infractions et la prise de notes. La lecture optique des bandes MRZ (carte d'identité, passeport et certificat d'immatriculation) est également possible. L'application « opération tranquillité vacances » facilite le suivi des usagers inscrits. L'appareil photo ouvre la possibilité des clichés anthropométriques ou des constatations, facilement insérables dans les procédures. Enfin, une application de cartographie opérationnelle permettra la géolocalisation des patrouilles environnantes et des événements en cours. Elle constituera un outil d'aide à la décision et facilitera la gestion opérationnelle des interventions.

A l'issue des retours d'expérience, le service de l'achat, des équipements et de la logistique de la sécurité intérieure (SAELSI) sera chargé d'émettre fin 2016 un marché public d'équipement des policiers et gendarmes en terminaux grand public entre 2017 et 2018.

• *Moderniser et faire converger les réseaux radio*

Le ministère de l'Intérieur dispose aujourd'hui de deux réseaux radios distincts : Rubis pour la gendarmerie et l'INPT (infrastructure nationale partagée des transmissions) à l'usage des services de secours (police, SDIS, SAMU) et des préfectures notamment.

L'objectif est de faire converger ces deux réseaux qui arriveront en fin de vie d'ici 2025, dans la perspective non seulement de réaliser des économies substantielles (leur maintenance représente un budget de plusieurs dizaines de millions d'euros par an) mais également, d'accroître l'efficacité des communications (e.g. situation de crise où la présence massive des services sur une zone géographique limitée sature les réseaux, ...), tout en permettant l'intégration de nouveaux utilisateurs (douanes, polices municipales, ...).

• *Les outils décisionnels et prédictifs*

Le recours aux outils décisionnels et prédictifs doit permettre d'optimiser l'emploi des ressources disponibles sur la voie publique.

Concrètement, il s'agit d'étudier et d'analyser, au travers de techniques avancées d'analyse statistique, les phénomènes de délinquance, de trouble à l'ordre public, de sécurité routière et de secours tels qu'ils sont décrits dans les systèmes d'information de la police et de la gendarmerie, pour mieux les anticiper. En accompagnant cette démarche « prédictive » d'analyses géo-spatiales et d'outils cartographiques, le ministère donnerait les moyens aux services de police et de gendarmerie de mieux allouer, jour par jour, voire heure par heure, leurs ressources sur le terrain.

A cette fin, le service des technologies et des systèmes d'information de la sécurité intérieure (ST(SI)²) et le service central du renseignement criminel de la gendarmerie nationale (SCRC) travaillent actuellement sur des systèmes experts reposant sur des solutions d'analyse de données de masse et de « *business intelligence* ».

La démarche proposée est d'autant plus ambitieuse que jusqu'à présent, les services ont toujours eu les plus grandes difficultés à réaliser des cartographies de la délinquance ou de l'accidentalité dignes de ce nom, laissant le plus souvent aux unités de terrain le soin d'élaborer elles-mêmes, en fonction de leurs ressources locales, les outils cartographiques nécessaires.

En choisissant de focaliser ses prédictions sur le mois ou sur la semaine, le SCRC entend travailler sur une échelle de temps long et fait le pari d'un impact durable sur le long terme. Ainsi, l'établissement d'une cartographie mensuelle des risques permet de laisser l'initiative aux opérationnels et de mieux impliquer, dans un processus de concertation, l'ensemble des acteurs de la société (préfets, secteur

associatif, acteurs privés, ...). Les expérimentations en cours, depuis le début de l'année 2016 en Aquitaine (concernant toutes formes de délinquance en zone gendarmerie uniquement) et dans l'Oise (vols de voitures en zones police et gendarmerie) permettront de mesurer tant la pertinence des outils que leur acceptation sur le terrain.

Une nécessaire maîtrise de l'univers numérique par les forces de sécurité

Enjeux de la collecte d'informations et de la veille sur Internet

Les forces de sécurité disposent d'unités spécialisées en cybercriminalité dotées de moyens humains et matériels performants. S'il existe une veille internet pour prévenir les grands rassemblements de personnes relativement aisés à déceler, la collecte de renseignements criminels constitue depuis plusieurs années une véritable priorité, en évolution permanente.

Chaque mois en France, environ 3 000 plaintes de victimes d'infractions liées à la cybercriminalité sont enregistrées par les seules unités de gendarmerie[4]. Le préjudice est évalué à plus de 3,5 millions d'euros par mois. Outre le vol de données, la cybercriminalité regroupe deux familles d'infractions : celles qui utilisent les technologies numériques de façon centrale comme la diffusion de contenus illicites (pédopornographie, apologie du terrorisme, ...) et les infractions de droit commun qui utilisent internet de façon accessoire comme les escroqueries aux petites annonces, les recels en ligne ou les ventes de produits réglementés.

(4) Les données similaires pour la police nationale ne sont pas disponibles.

Depuis plusieurs années, la gendarmerie a développé un réseau d'environ 2 000 gendarmes qui évoluent dans la sphère de la cybercriminalité, dont les 260 enquêteurs N'Tech constituent le fer de lance. A l'échelon national, ce réseau est animé par le département prospective animation territoriale du centre de lutte contre les criminalités numériques (C3N), lui-même intégré dans le service central du renseignement criminel (SCRC). Le C3N est responsable de l'harmonisation des formations, des équipements et des processus de travail des « cyber gendarmes ».

Formés par la DCPJ (direction centrale de la police judiciaire) et déployés pour moitié en son sein, la police nationale dispose pour sa part de 430 « investigateurs en cybercriminalité » (ICC).

La DCPJ s'est par ailleurs dotée d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui comprend notamment la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) permettant aux internautes de signaler tout contenu ou comportement présumé illicite sur internet. En 2015, PHAROS a reçu et traité 188 055 signalements portant sur des domaines aussi variés que les escroqueries sur internet, la pédopornographie ou l'apologie du terrorisme.

Enjeux du big data

Le *big data* traite en temps réel des milliards de données. Leur analyse et leur interprétation dégagent des tendances, favorisent la prospective ou l'anticipation et constituent une aide à la décision.

Dans une approche préventive, l'enjeu du *big data* pour les forces de sécurité consiste à identifier les lieux et les périodes susceptibles de connaître une évolution défavorable de leur niveau de délinquance.

Mais le *big data* peut aussi être un outil d'investigation. Le recueil d'informations à partir d'objets connectés peut par exemple contribuer à l'amélioration de la sécurité routière et réduire les causes d'accidents (voitures connectées). Le traitement et l'exploitation du renseignement dans la lutte contre les atteintes aux personnes (pédophilie), la criminalité organisée, le terrorisme, le maintien de l'ordre public (prévention de manifestations de type « *rave parties* » ou autres grands rassemblements de personnes), la lutte contre la fraude, les infractions économiques et financières ou même la cybersécurité (détection des attaques et identification des « *hackers* ») sont aussi des domaines où le *big data* apportera une vraie plus-value.

Outil en grand développement, le *big data* ouvre donc aux forces de sécurité de nouvelles perspectives en élargissant leur champ d'action. Au point que la puissance publique prenne parfois l'initiative de la centralisation des données de sécurité. La ville de Turin a ainsi mis en place une plateforme de test à l'échelle de plusieurs de ses quartiers. Les commerçants peuvent enregistrer leurs images de vidéosurveillance sur des serveurs sécurisés de la ville. Le programme permet une centralisation de l'information (d'où une garantie d'exploitation plus facile) au profit des services de sécurité, et des expérimentations de vidéoprotection intelligente (analyses en temps réel, démarches de police scientifique, ...).

Reste que la collusion potentielle entre *big data* et « *Big brother* », entretenue par la place qu'occupent désormais les ordinateurs et internet dans la vie de nos concitoyens, constitue une menace selon certains (e.g. mouvement « La quadrature du Net », ...). A la logique du contrôle des flux doit donc être opposée la garantie de la seule poursuite de l'intérêt général.

Enjeux de l'internet des objets

On estime aujourd'hui à plus de 9 milliards le nombre d'objets connectés à internet à travers le monde, y compris ordinateurs et téléphones. A l'horizon 2025, les projections évoquent jusqu'à 1 000 milliards d'objets connectés[5]. Leur utilisation croissante aura de fortes implications en matière de sécurité et de confidentialité des données. Ainsi, le directeur national du renseignement américain, James Clapper, n'a pas hésité à déclarer lors d'une audition devant le Sénat américain : « *A l'avenir, les services de renseignement pourraient tirer parti de l'internet des objets pour identifier, surveiller ou localiser des suspects, découvrir des indicateurs potentiels, ou obtenir des mots de passe* »[6].

(5) McKinsey Global Institute, ibidem

(6) Le Monde, 10 février 2016

Les concepteurs d'éléments électroniques font des efforts pour intégrer une dimension sécuritaire dans les objets qu'ils produisent, car les risques sont multiples.

Le risque est tout d'abord économique. Il s›agit de préserver la confiance des clients en garantissant la confidentialité des données personnelles, la sécurité des transactions ou la protection contre les attaques informatiques et logiciels malveillants. Le risque peut aussi être celui de la mise en péril de la santé

publique, notamment s'agissant des appareils dont l'utilisation à un lien direct avec la santé des patients (e.g. contrôle à distance d'équipements de soin, ...).

Face à ces menaces, les réponses sont singulièrement faibles. En France, la loi « Informatique et Libertés » de 1978 connaît des évolutions et des mises à jour ponctuelles pour tenter de protéger au mieux les données personnelles, mais elle ne s'applique que sur le territoire français et hors sphère privée. De même, à l'échelon européen, si un règlement européen pour la protection des données personnelles a finalement été adopté en avril 2016, il n'entrera en vigueur qu'au deuxième trimestre 2018 et ne couvrira que les points sur lesquels les Etats membres sont parvenus à un consensus. Les points d'achoppement – parfois cruciaux pour une meilleure protection et gestion des données concernées – demeureront gérés par chaque Etat au travers de ses législations nationales. Mais en dépit de la volonté et des tentatives – voire des avancées significatives – des autorités d'encadrer et de réguler ces échanges de données, la question reste entière. Comment préserver la confidentialité et l'intégralité de l'énorme quantité de données collectées par les objets connectés qu'ils échangent avec d'autres objets connectés, sur internet ou avec des serveurs implantés sur toute la surface du globe ?

Cette interrogation reste aujourd'hui sans réponse, et le droit international, moins encore que le droit français, n'est pas totalement adapté.

Enjeux de la vidéoprotection intelligente

Alors qu'elle a connu une courbe de diffusion comparable à celle des objets connectés et est devenue un outil de travail à part entière des forces de sécurité (caméras fixes, embarquées ou piétons), la vidéoprotection « traditionnelle » est en passe d'évoluer, voire de disparaître, au profit de systèmes dits intelligents.

Portées par un contexte favorable de maturité idéologique et sociale d'une part, et d'opportunités technologiques d'autre part, de nouvelles générations de caméras et d'algorithmes sont en effet en train d'apparaître. La détection automatique d'anormalités, le suivi de personnes, la réaction suite au déclenchement d'une signature sonore, la reconnaissance faciale, le *tracking* qui permet le suivi des véhicules, ... deviendront la base des dispositifs de vidéoprotection intelligents. Ces systèmes seront alors des outils encore plus puissants d'aide à la prévention, à l'intervention, à l'investigation et à l'élucidation.

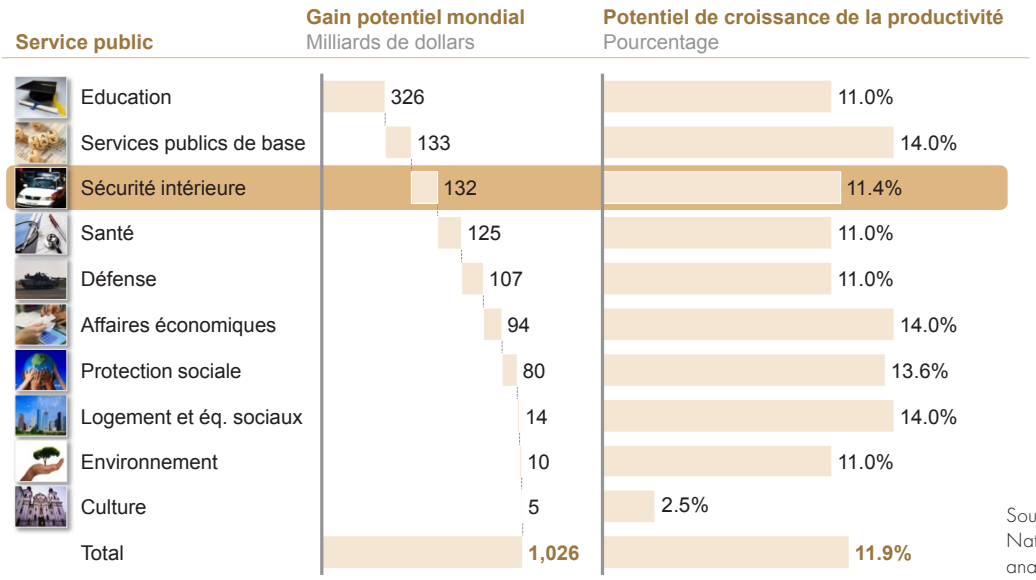
Leur potentiel est si important que les limites éthiques, déontologiques et légales qui contraignent l'usage actuel de la vidéoprotection devront s'accorder avec les exigences sociales et sociétales. Or l'arrêté interministériel portant sur les normes techniques de ces dispositifs date de 2007 et présente déjà un décalage certain avec les capacités actuelles des équipements. Une fois encore, le droit doit évoluer.

Enjeux de productivité

Au-delà des contributions concrètes aux métiers de base de la police et de la gendarmerie, la révolution numérique représente aussi, plus globalement, une source de productivité nouvelle et significative pour l'ensemble des services

publics. Les experts de McKinsey l'évaluent à un peu plus de 10% pour les services de sécurité intérieure. Si on parle des heures de travail libérées ou réaffectées, cela représenterait pour la France l'équivalent de plus de 20 000 postes de policiers ou de gendarmes.

Figure 2 : La digitalisation des services publics représente pour le monde entier un gain de productivité annuel de plus de 1 000 milliards de dollars



Source : Statistiques des Nations Unies et de l'OCDE, analyses McKinsey

Une délinquance qui s'approprie le numérique

Depuis les années 1990, l'accès facile à internet et la diminution du prix des technologies se sont traduits par une démocratisation rapide des outils de l'information et de la communication, et de leur utilisation, y compris frauduleuse.

Caractéristiques de la cybercriminalité

En matière de cybercriminalité, on peut aujourd'hui distinguer deux catégories de menaces :

- celles dont les technologies sont à l'origine d'infractions qui n'existaient pas jusqu'alors (déni de service[7], menaces persistantes avancées ou APT[8], défacement[9], ...) ;
- celles qui utilisent les technologies comme vecteur pour commettre des infractions « traditionnelles » (escroqueries telles que le hameçonnage, le vol à la nigérienne ou la fraude au Président ; les atteintes aux systèmes de traitement automatisé de données (STAD) pour commettre des vols de données ou de fichiers ; les demandes de rançons en bitcoins[10] ; ...).

Dans les deux cas et grâce aux technologies, la commission de l'infraction se fait à distance et de façon anonyme. Elle peut être le fait d'un individu seul, bénéficiant du soutien d'un réseau technique et informationnel étendu ou agissant dans le cadre d'une bande organisée géographiquement éclatée.

(7) Saturation d'un site internet par l'envoi massif et simultané de requêtes jusqu'à rendre le service indisponible.

(8) *Advanced persistent threat* : attaque s'appuyant sur des mécanismes complexes ou des vulnérabilités pas encore connues, et menée de manière répétée (e.g. attaque contre TV5 Monde en avril 2015).

(9) Prise de contrôle et modification non sollicitée de la présentation d'un site internet

(10) Monnaie numérique virtuelle.

L'infraction pourra revêtir un caractère local (e.g. volonté de vengeance contre un ancien employeur, associé ou conjoint, ...) ou international (les frontières géographiques, politiques et économiques n'existent plus). Son degré de sophistication ne sera pas nécessairement élevé (voire, l'infraction sera commise sans effort, ni investissement intellectuel ou physique ; d'où une faible conscience de la gravité des actes commis par le cyber délinquant). L'infraction pourra être d'autant plus discrète ou indétectable qu'elle sera conduite au travers de réseaux fermés (réseaux privés virtuels ou « *Dark Net* », réseaux détournés tels que Playstation, ...). Dans tous les cas, elle aura des conséquences financières, politiques, stratégiques, en termes d'image quasi immédiates et pouvant être de grande ampleur (déstabilisation temporaire mais sérieuse voire irréversible de la cible).

Facteurs de développement de la cybercriminalité

La démocratisation croissante des technologies n'est pas le seul terreau sur lequel se développe la cybercriminalité. La gratuité ou quasi gratuité de mise en œuvre et d'utilisation est bien sûr un puissant levier. Mais une conjonction d'autres éléments alimente son développement :

- l'importance grandissante du patrimoine informationnel dématérialisé ;
- la faible culture et les pratiques balbutiantes de protection des données du grand public comme des entreprises ;
- l'explosion continue des sites et des pages internet, qui rend leur surveillance quasi impossible ;
- les barrières technologiques (chiffrement des communications, routage en oignon au travers du réseau Tor, ...), parfois insurmontables pour les enquêteurs ;
- une forme de marchandisation du cybercrime (l'achat de virus informatiques, d'attaques cyber ou d'armes peut se faire en quelques clics) ;
- des carences dans la collaboration policière voire judiciaire au niveau international aboutissant à l'échec des poursuites ;
- des vides juridiques, tous les pays n'ayant pas intégré les aspects de cette cyber délinquance dans leurs législations (reconnaissance de l'identité virtuelle et répression de son usurpation, vol de données, atteintes aux STAD, ...).

Si cette délinquance est nouvelle au regard des moyens et de ses modes opératoires, ses motivations sont en revanche restées les mêmes : idéologiques (terrorisme, sectaire), vengeresses, cupides (obtention d'un gain financier important et rapide), ludiques ou intellectuelles (prouesse technique sans considération financière ou malveillante).

Des interactions nouvelles avec les citoyens

Une société qui se numérise dans un profond paradoxe

En quelques décennies, les nouvelles technologies de l'information et de la communication ont profondément bouleversé les attitudes et les comportements

de nos concitoyens : les téléphones mobiles, internet, les smartphones ou les tablettes sont devenus des objets du quotidien. Le haut débit favorise le travail à distance ou en mobilité. On achète, on s'informe ou on déclare ses revenus en ligne. Les réseaux sociaux créent de nouveaux modes de relation. Les prises de parole se font plus libres et plus spontanées. « Partage » et « collaboratif » deviennent les maitres mots de la nouvelle économie qui se met en place. En parallèle, le grand public développe de nouvelles exigences à l'égard d'internet : qualité de l'offre et des services proposés, design et fluidité applicative, sécurisation des transactions, suivi et mémoire des échanges, protection des données personnelles, ...

La numérisation de l'économie s'impose ainsi comme une norme qui va diffuser ses règles, ses usages et ses valeurs à l'ensemble de la société. Les services publics n'échappent pas à cette mutation, y compris les services de sécurité.

Dans le même temps, force est de constater que la révolution digitale s'inscrit dans un profond paradoxe. Avec le développement de sites comme Dailymotion, Facebook, Flickr, LinkedIn, Twitter ou encore WhatsApp, nos contemporains n'ont jamais autant dévoilé leur vie privée dans l'espace public. Au point que ceux qui ne disposent pas de compte personnel sur les réseaux sociaux ont souvent malgré cela une existence en ligne fournie, générée par l'activité de leurs conjoints, parents ou amis proches[11]. Or dans le même temps, nos contemporains réclament une parfaite protection de leur vie privée et sont particulièrement enclins à dénoncer toute immixtion de l'Etat, fut-elle au nom du contre-terrorisme et de la défense des libertés. Comme nous l'avons entendu dans le cadre de nos entretiens : « *On donne tout aux géants du Web, mais on refuse de donner des informations à la puissance publique qui elle est pourtant contrôlée* ».

(11) Comme l'illustre le cas d'Edward Archer, qui a tiré sur un policier de Philadelphie (Etats-Unis) le 8 janvier 2016 et dont les publications de sa mère sur internet ont permis d'établir les liens avec Daech.

Des services sur internet qui doivent encore évoluer

Sous la pression de nos concitoyens mais aussi parce qu'elle porte en elle de réelles opportunités de transformation, les forces de sécurité pourront capitaliser sur les apports de la digitalisation pour engager une relation nouvelle avec le grand public, voire réconcilier certains citoyens avec leur police.

Plusieurs initiatives ont déjà été lancées dans ce sens : communication internet de recrutement, compte Twitter, pré-plainte en ligne, signalement de contenu illicite sur internet (PHAROS) ou plateforme de signalement à l'IGPN, ... On peut toutefois regretter une approche encore très institutionnelle et trop focalisée sur la communication et « l'image » au détriment de véritables propositions de services, ce qui nuit à la création et à la consolidation d'une dimension de proximité.

Un regard sur les meilleures pratiques des grandes forces de police étrangères suggère plusieurs axes de progrès potentiels.

En Espagne, la police nationale a décidé en 2006 de se lancer sur les réseaux sociaux. Initialement développée à l'attention des média, cette approche s'est progressivement élargie puis centrée sur le grand public (communication institutionnelle, messages de prévention, collecte de renseignements opérationnels, ...). Les huit personnes qui animent aujourd'hui ce dispositif ont réussi à instituer un véritable dialogue avec les citoyens (notamment auprès des jeunes) et déploient une véritable politique de gestion de la « marque » *Policía Nacional*.

Figure 3 : La Policía Nacional s'appuie sur les réseaux sociaux pour développer sa proximité avec les Espagnols

Source : Policía Nacional, Oficina de Prensa y Relaciones informativas, avril 2016.

Figure 4 : De nombreux canaux ou services peuvent être mis en œuvre à destination du grand public

Source : McKinsey (ligne de service Police, 2014)

D'autres exemples internationaux suggèrent d'autres idées pertinentes :

- à Los Angeles, la police utilise de multiples canaux pour créer et entretenir une relation de proximité avec les citoyens : comptes rendus d'activité, « *messages [mensuels] du chef* », conseils de prudence, appels à témoins, circulation, questionnaires en ligne, communication de recrutement, pages à destination de la communauté hispanophone, … ;
- à Londres (comme à Los Angeles), des pages internet de la *Metropolitan police* proposent d'accéder aux données de criminalité avec une extrême finesse géographique ;
- la police londonienne propose également sur son site des pages dédiées à l'assistance des victimes et des témoins.

Une pression positive sur la qualité de service et la déontologie

Quels que soient les services numériques déployés et la réactivité dont policiers et gendarmes feront preuve, les forces de sécurité devront aussi s'habituer à vivre une forme de pression positive sur la qualité de service imposée par la révolution digitale. La recherche d'un commissariat sur Google permet désormais, par exemple, de le noter et de publier un commentaire à son sujet. Plus fréquent déjà, les interventions policières sont filmées par des téléphones portables et circulent d'autant plus vite, jusqu'à finir à la une des média, qu'elles sont « spectaculaires » ou illustrent un comportement policier inapproprié. Des entreprises comme Citizenside se sont spécialisées dans ce « journalisme participatif » et proposent de racheter photo ou vidéo entre 20 et 900 euros.

La révolution digitale, première révolution où les organisations sont en retard sur la société, est avant tout une révolution des usages. L'enjeu pour les forces de sécurité est donc de s'approprier les usages innovants. La caméra-piéton est un élément de réponse : l'expérience montre qu'elle apaise effectivement les tensions. La prise de parole active voire proactive sur les réseaux sociaux en sera une autre.

Au-delà des outils et de la technologie, la révolution digitale appelle aussi à un renforcement du discours et des formations en matière de respect de la déontologie, voire la mise en place de formations spécifiques sur la qualité de service, le sens et les formes qu'elle doit prendre en matière policière.

Un partenariat avec le secteur privé qui doit encore se structurer

Le bras de fer qui a opposé début 2016 le FBI et Apple au sujet de l'accès au contenu de l'iPhone de l'un des terroristes de San Bernardino[12] illustre un phénomène qui pourrait bien avoir des conséquences de plus en plus lourdes dans les années à venir. Les mécanismes de sécurisation et, notamment, les technologies de chiffrement sont aujourd'hui plus puissants que les techniques d'investigation. L'algorithme utilisé par le moteur de chiffrement d'Apple, l'AES 256, n'avait jusqu'ici jamais été cassé et seule une recherche exhaustive (ou attaque par force brute, c'est-à-dire par test des combinaisons une à une) semblait permettre d'en venir à bout.

(12) Fusillade le 4 décembre 2015 aux Etats-Unis faisant 14 victimes. Daech affirmera que l'attaque a été menée par deux de ses partisans, neutralisés par les forces de sécurité alors qu'ils prenaient la fuite. C'est finalement l'intervention d'un tiers qui aura permis au FBI de déverrouiller l'appareil.

Si des moyens de contournement ne sont pas prévus dès la conception d'un produit (porte dérobée, mécanisme de désactivation des protections, ...), soulever la question *a posteriori* ne ferait qu'accroitre très largement les difficultés. Inversement, si ces solutions existent ou si la capacité à les créer existe réellement, refuser de répondre à une réquisition judiciaire constituerait une infraction pénale (contravention de deuxième classe).

Le développement des technologies et des services ouvre de nombreuses opportunités de collaborations entre le secteur privé et les forces de sécurité. Les outils de communication, les véhicules deux ou quatre roues, la dématérialisation financière, les objets connectés, la domotique et les compteurs électriques

intelligents, ... sont autant de capteurs qui permettent de suivre, débusquer ou tout simplement confondre les délinquants.

Dans ce contexte, les entreprises privées doivent-elles prendre en compte dans leur développement produit et dans leur architecture de sécurité, les besoins potentiels des forces de sécurité ? A notre sens, une collaboration est clairement possible, dès lors qu'elle est organisée.

Prendre part aux projets de R&D des entreprises

Pour qu'elle soit fructueuse et durable, la collaboration entre le secteur privé et la police ou la gendarmerie doit s'organiser dans le cadre de protocoles formalisés, précisant clairement les objectifs, les principes et les modalités d'échanges.

Renault a ainsi signé en 2012 un accord avec la gendarmerie nationale en matière de lutte contre le vol de voitures. Concrètement, les gendarmes accèdent à des bases de données ou à des mallettes techniques du constructeur, tandis que celui-ci construit une base de connaissance actualisée des techniques de vols de véhicules telles qu'observées par les gendarmes. Pour fluidifier ces échanges, les deux partenaires ont mis en place des équipes dédiées qui ont appris à se connaitre et à travailler ensemble.

C'est précisément le caractère gagnant-gagnant de l'échange qui permet au partenariat de se revendiquer comme tel et de s'inscrire dans la durée :

- le secteur privé doit pouvoir s'appuyer sur la connaissance de la criminalité qu'ont les forces de sécurité pour mieux maitriser les techniques d'attaque et faire évoluer ses dispositifs de sécurité ;
- les policiers et les gendarmes doivent pouvoir exprimer leurs besoins en amont et être impliqués dès les phases de conception des projets les affectant.

Pour initier ce type d'accords, faire en sorte qu'ils bénéficient à tous et que se crée une émulation positive entre sociétés du secteur privé, les forces de sécurité doivent se rassembler au sein d'une structure unique. Nous pensons que ce pourrait être une des missions de la délégation ministérielle aux industries de sécurité (DMIS). Elle serait chargée d'identifier les entreprises éligibles à ce type de partenariat, de formaliser les accords, de désigner les correspondants pertinents au sein de la police, de la gendarmerie et de la DGSI, et d'accompagner les réflexions prospectives.

Seul un travail d'anticipation mené en commun permettra d'aboutir à de réelles avancées : le secteur privé ne sait pas de quoi les forces de sécurité ont besoin et inversement, celles-ci ne connaissent pas les plans de développement du secteur privé.

Collaborer avec efficacité aux enquêtes

Les collaborations dans le cadre des investigations elles-mêmes se développent de plus en plus. Il s'agit tantôt de réquisitions à personnes, tantôt de demandes d'assistance ou d'expertise (ordonnances).

Face à l'accroissement des demandes (d'autant plus lourdes pour le secteur privé qu'elles prennent la forme de réquisitions successives), mettre en place un système d'information et un principe de guichet unique, partagés par l'ensemble des forces de sécurité qui bénéficieraient en retour d'interlocuteurs dédiés dans les sociétés privées, permettrait de fluidifier et d'accélérer les échanges. Cela se fait déjà aujourd'hui dans le monde des opérateurs téléphoniques.

Se pose aussi la question du coût de traitement de la réquisition : la charge de travail ne doit être ni intolérable et durablement désorganisatrice pour l'entreprise sollicitée, ni source de revenus récurrents et disproportionnés. La collaboration doit se faire dans un esprit *pro bono* équilibré.

Reste que la mobilisation des expertises privées pourrait se concevoir aussi dans les phases amont des enquêtes (e.g. détection des voyages ou mouvements financiers suspects, scoring des risques terroristes à partir des mouvements bancaires, utilisation des réseaux sociaux, ...). Elle se heurte souvent dans ce cas à la question de l'accréditation de l'expert ou de la personne qui sera amenée à en connaître. Des cloisonnements peuvent être envisagés pour y remédier, comme Interpol a par exemple su le faire dans le cadre de son programme INVEX[13]. Ainsi, alors que les législations nationales ne permettent pas à des acteurs privés d'accéder aux fichiers des véhicules volés, Interpol joue un rôle d'intermédiaire. L'agence consolide les données des pays adhérents au programme et les diffuse auprès des constructeurs. Ceux-ci peuvent alors alerter les autorités en cas de passage dans leurs concessions d'un véhicule recherché.

(13) *Interpol vehicles data exchange*

Les forces de sécurité françaises pourraient s'inspirer de cet exemple pour élargir les protocoles de collaboration, en veillant cependant à protéger le statut de l'expert, qu'il intervienne gracieusement ou non. Sa connaissance des faits (e.g. un véhicule confié en réparation est recherché par Interpol) ne doit pas le placer en porte-à-faux vis-à-vis de son client ou de la justice (dans notre exemple, l'intervention sur le véhicule est soumise à autorisation des forces de sécurité. Si elles tardent à l'accorder, le client se plaindra du délai d'intervention sur son véhicule. Si le garagiste passe outre, il risque d'être accusé de complicité pour avoir effacer des données ou messages d'alerte de l'ordinateur de bord).

Une industrie française de la sécurité intérieure qu'il faut encore développer

Si la France a su se doter d'une industrie de défense de premier plan grâce aux volumes et à la structuration de sa commande publique, force est de constater qu'il n'en va pas de même en matière de sécurité intérieure. L'Etat est certes un prescripteur majeur, mais il demeure un acheteur modeste. Au-delà des volumes, c'est bien la question de l'absence de vision sur les besoins matériels à moyen et à long terme qui est posée. Sans une structuration de la demande, il ne peut guère y avoir une structuration de l'offre et moins encore, de capacité d'entrainement de l'écosystème industriel et de sa R&D.

Structurer une vision à moyen-long terme des besoins

Pour aller de l'avant, les industriels évoquent l'idée d'une expression de besoins sectoriels et par grande mission (e.g. les besoins de la Sécurité Publique en milieu urbain, ses besoins en sites de contestation, les besoins des services de renseignement en matière de capteurs abandonnés, ...).

Par ailleurs, là où les Anglo-saxons acceptent de prendre des risques technologiques et industriels décidés par de véritables comités d'investissement, l'approche française consiste à réclamer des démonstrateurs. Cette lourdeur nuit à la rapidité et à l'effet d'entrainement des achats de l'Etat. La France gagnerait à prendre plus de paris industriels.

Une montée en puissance de la délégation ministérielle aux industries de sécurité, qui pourrait devenir « une DGA[14] de la sécurité intérieure », permettrait à la fois d'organiser cette expression de besoins par grandes missions et d'accélérer la validation des concepts pour passer plus rapidement du PoC au PoV[15].

(14) Direction générale de l'armement
(15) Respectivement, « *proof of concept* » (démonstration de faisabilité technique) et « *proof of value* » (prototype démontrant la validité des bénéfices attendus).

Investir dans l'industrie pour soutenir son développement

Pour permettre la construction d'une offre française taillée pour l'exportation, les industriels évoquent un doublement « *au minimum* » des investissements consacrés aux démonstrateurs de sécurité intérieure. A l'heure où notre pays prépare son troisième plan d'investissements d'avenir (PIA) d'une enveloppe totale de 10 milliards d'euros, on peut regretter qu'aucun crédit ne soit spécifiquement alloué à des thématiques sensibles de sécurité intérieure comme la sécurité informatique, le chiffrement, la surveillance d'internet, ... En particulier, l'Etat et même l'Union européenne gagneraient à accompagner Bull et Atos dans le développement des supercalculateurs, marché porteur qui ne compte que quelques acteurs, américains, chinois, japonais ... et français. Les capacités des ordinateurs quantiques, par exemple pour casser des codes d'accès, en feront un véritable enjeu de souveraineté nationale d'ici quelques années.

Plus symboliquement, si notre pays souhaite se doter d'une industrie de la sécurité de classe mondiale, notre Etat se doit de lui offrir les vitrines technologiques susceptibles de convaincre les futurs clients. Les industriels tricolores pourront ainsi organiser dans l'Hexagone des visites qui sont aujourd'hui délocalisées à Abu Dhabi, Dubaï, Mexico ou Singapour.

ENJEUX CULTURELS ET ORGANISATIONNELS : ADAPTATION OU RÉVOLUTION ?

Quelques leçons des expériences passées

Si de grands fichiers nationaux comme le fichier automatisé des empreintes digitales (FAED) ou le fichier national automatisé des empreintes génétiques (FNAEG) constituent d'indiscutables réussites, nombre de réalisations mises en œuvre au cours de ces dernières années au sein du ministère de l'Intérieur se sont soldées au mieux par des demi-succès, le plus souvent par des échecs significatifs.

Sans prétendre à une quelconque exhaustivité, plusieurs applications métier n'ont pas produit les résultats attendus, à tout le moins dans les délais annoncés.

Aux lourdeurs inhérentes aux marchés publics, l'organisation elle-même du ministère de l'Intérieur et plus particulièrement de la police nationale constitue un frein à la mise en œuvre et à la conduite du changement en matière technologique.

Ainsi, les services de police sont placés, selon leur positionnement géographique, sous l'autorité soit de la direction générale de la police nationale (DGPN), soit de la préfecture de police de Paris, avant d'être eux-mêmes éclatés entre différentes directions opérationnelles, soucieuses de cultiver leurs particularités et jalouses de leurs prérogatives relevant le plus souvent d'un simple héritage historique. De ce point de vue, le contraste qu'offre la gendarmerie nationale est saisissant. A ces particularités doit s'ajouter également le positionnement de la direction des systèmes d'information et de communication (DSIC) au sein du secrétariat général du ministère de l'Intérieur, exerçant une partie de ses compétences sur le périmètre de la police nationale (mais pas de la gendarmerie qui a toujours disposé de ressources propres).

Compte tenu des cloisonnements inhérents à toute structure bureaucratique et d'une organisation relevant davantage de « tuyaux d'orgues » que d'une pyramide, la conduite des projets liés aux nouvelles technologies se trouve ralentie, quand ce n'est pas entravée par des rivalités et des difficultés de coopération entre services. *De facto*, des retards significatifs accompagnent généralement la mise en production des réalisations attendues.

Plusieurs exemples viennent illustrer cette réalité :

- ACROPOL (automatisation des communications radio opérationnelles de police), le système de communication radio cryptée utilisé notamment par la police nationale. Ce système essentiel à la fiabilité et à la confidentialité des communications radio de la police a d'abord achoppé sur des problématiques d'expression de besoins (en raison de la multiplicité des directions concernées notamment) avant de commencer à être déployé en 1995 à une cadence fort peu soutenue. Ce n'est en effet qu'en 2007 que les dernières directions départementales ont été équipées. Comme l'analyse le plan de modernisation de la sécurité intérieure (*cf. supra*), ce réseau est aujourd'hui obsolète, huit ans seulement après sa généralisation et en dépit d'un déploiement débuté voici vingt ans.
- Ce décalage technologique a également été observé avec les outils de gestion des interventions de police (PEGASE – CORCICA) qui équipent les grandes salles d'information et de commandement (48 au total à ce jour), principalement en Sécurité Publique. Si le produit livré en 2004 a donné satisfaction aux utilisateurs, son développement a été dispendieux en termes de temps, tandis que son déploiement s'est révélé particulièrement lent (le dernier centre d'information et de commandement, en l'occurrence celui de la DDSP de l'Essonne, a été doté de PEGASE en 2015), si bien qu'il se trouve lui aussi frappé d'obsolescence peu de temps après sa mise en production généralisée.
- Les terminaux informatiques embarqués (TIE) à bord des véhicules de police offrent une autre illustration d'un produit peu satisfaisant et déjà périmé à peine livré. Succédant à d'autres projets qui au cours des années 1990 n'ont jamais réussi à convaincre les services (SITTER puis TESA), le TIE dispose d'une technologie complètement dépassée qui ne donne pas satisfaction aux utilisateurs. Plus de 8 000 de ces appareils équipent pourtant aujourd'hui les véhicules de police et de gendarmerie, sans qu'une utilisation efficiente ne soit réellement démontrée sur le plan opérationnel. Quant au volet « 4 en 1 » qui équipe certains terminaux (lecture automatisée de documents administratifs, tels que permis de conduire, carte d'identité, etc.), il s'est soldé par un fiasco retentissant et n'a jamais réellement fonctionné.
- Le portail CHEOPS, outil développé et entretenu par la DSIC, permet aux fonctionnaires du ministère de l'Intérieur d'accéder de manière sécurisée aux différents fichiers de police[16] et à certaines applications professionnelles[17]. Si à ses débuts CHEOPS a pu donner satisfaction, l'ajout progressif au fil des années de nouvelles fonctionnalités tout comme la multiplication exponentielle des profils générés permettant un accès sur mesure en fonction des droits attribués à chaque agent ont rapidement conduit ce système à connaître des phénomènes de saturation, provoquant l'indisponibilité chronique de certains fichiers et de certaines applications, sans parler de l'imbroglio qu'il représente désormais pour les gérants d'habilitation locaux amenés à créer ou à modifier les droits des différents utilisateurs. Le passage, une fois encore lent et tardif, de CHEOPS (client lourd) à CHEOPS-NG (nouvelle génération : application web avec un pilotage du ST(SI)²) ne permet de solutionner qu'une partie du problème.

(16) FPR, FOVeS, TAJ, SNPC, FNE, ...

(17) PVe, WinOMP, LRP-PN, ...

- Le logiciel de rédaction des procédures de la police nationale (LRP-PN) a connu un accouchement particulièrement laborieux. Cumulant retards et contretemps, il a d'abord été annoncé en 2007 sous l'acronyme ARDOISE. Tous les procéduriers opérant dans le giron de la police nationale ont été formés entre 2007 et 2008 aux fins de se préparer à l'arrivée, présentée comme imminente, de ce nouveau logiciel de rédaction de procédures. Devant l'immensité des difficultés techniques non résolues, le projet a finalement été retiré sans jamais avoir été installé dans les services et ce n'est qu'en 2011-2012 qu'une nouvelle version a pu être livrée aux OPJ et APJ (formés préalablement une seconde fois à l'outil). Il est significatif de constater que la gendarmerie nationale, confrontée elle aussi à la nécessité de mettre à la disposition de ses effectifs un logiciel de même nature, a fait preuve d'une ambition plus modeste mais plus réaliste quant aux fonctionnalités de l'outil, en faisant participer à son développement une communauté de gendarmes de terrain, garante des attentes des unités territoriales. Elle a ainsi été en mesure de le livrer plusieurs années avant la police.
- En dépit d'un plus grand réalisme, la gendarmerie nationale a aussi rencontré des difficultés dans la mise en œuvre de certaines applications, développées par des ressources propres. Il en a par exemple été ainsi avec le logiciel Pulsar regroupant de nombreuses fonctionnalités essentielles pour le travail des unités : gestion des courriers, de l'activité, des procès-verbaux, des droits (délivrés par les gérants d'habilitation), création des feuilles de service, des comptes rendus, des bulletins d'accidents, des statistiques, sans parler du dossier de circonscription et du suivi budgétaire. En 2005, un consortium de sociétés a développé la première version de Pulsar, sans parvenir à réaliser la version départementale « Pulsar Service ». La gendarmerie a alors abandonné le projet non sans avoir au préalable formé ses cadres, jusqu'à ce qu'un groupe exclusivement composé de gendarmes le reprenne en 2011.
- Plus récemment, soucieux de s'adapter à des modifications du niveau de qualification des cartes professionnelles des gendarmes, le ST(SI)² a conclu un marché modifiant le profil de la puce contenu dans ces cartes. Or cet ajustement technologique va affecter le bon fonctionnement d'applications auxquelles ces cartes donnaient accès. A l'été 2016, 40 000 gendarmes ne vont plus pouvoir se servir des terminaux de verbalisation en dotation dans leurs unités.

Ces exemples démontrent la lourdeur que revêt au sein du ministère de l'Intérieur la mise en œuvre de nouveaux systèmes informatiques et de l'innovation en général.

L'administration centrale, prise au sens large, semble s'épuiser (et parfois s'enliser) dans des chantiers qui finissent par devenir « pharaoniques », tout en négligeant des réalisations plus modestes mais dont les services de terrain ont besoin au quotidien. Cette particularité explique que les services déconcentrés se soient longtemps résolus, plutôt que d'attendre des solutions ne descendant pas du sommet, à développer chacun leurs propres outils en faisant appel aux compétences informatiques détenues par leurs personnels, conduisant ainsi à multiplier, sans doute bien inutilement, des solutions voisines les unes des autres. Si tant est que ces pratiques ne subsistent pas à l'insu des directions centrales (ce

qui reste à démontrer), la multiplication à l'excès d'applications informatiques similaires ne constitue bien évidemment ni un facteur d'efficacité ni une bonne gestion de moyens qui demeurent contraints.

A cet égard, il est intéressant de noter la décision prise par le directeur général de la police nationale qui, dans une note en date du 3 avril 2014, a instauré une « communauté de développement de la police nationale » visant notamment à interdire la pratique incontrôlée des développements informatiques au niveau des services territoriaux. Cette « communauté » devait être constituée de développeurs présents sur le terrain et volontaires pour intégrer une structure fédérée par le ST(SI)² qui fournissait les outils collaboratifs appropriés. Il s'agissait à la fois de faire remonter des besoins spécifiques et de mobiliser une ressource aisément disponible (sous réserve de l'accord des chefs de service). Deux chantiers étaient proposés lors de cette création : la gestion des gardes à vue et la gestion des scellés (autrement dit, deux « serpents de mer » ayant donné lieu à un nombre difficilement calculable d'applications locales). Deux ans après, le bilan de cette communauté de développement est peu encourageant. D'une part, peu de volontaires se sont fait connaître et, d'autre part, les deux projets de lancement n'ont guère avancé et aucun nouveau projet n'a été mis à l'étude jusqu'au printemps 2016.

Diagnostic de la gouvernance actuelle du changement

Un besoin de simplification et de meilleure lisibilité des structures

Le paysage numérique et ses défis pour les forces de sécurité, imposent de réconcilier trois fondamentaux : organisation, ressources humaines et stratégie.

Loin de se focaliser sur le seul développement d'outils, la réussite du changement proviendra essentiellement de la mobilisation des personnels (recrutement, fonctions, formation continue). Aussi, la course effrénée à la technologie ne doit pas détourner l'attention des pouvoirs publics. Il convient de prendre en compte les difficultés initiales générées par la multiplicité des intervenants (police nationale, gendarmerie nationale, polices municipales, acteurs privés de la sécurité, citoyens), l'hétérogénéité des structures et des pratiques, la rigidité de certaines règles (cadres d'emploi inhérents aux principes de recrutement, pratiques budgétaires, etc.) et enfin, un manque pénalisant de leadership managérial.

La question des organisations se pose en premier lieu. Lorsque l'on examine les grandes directions concernées (DGPN, DGGN, DGSI, DGSCGC), la mission RH s'avère sous-dimensionnée et son pilotage s'apparente à un mille-feuille. Force est de constater qu'à missions et objectifs égaux, policiers et gendarmes

ne fonctionnent pas à l'identique. Toutefois, les sources de rapprochement existent : la gendarmerie est désormais placée sous l'autorité fonctionnelle du ministre de l'intérieur, police et gendarmerie mutualisent certains de leurs moyens voire engagent des réflexions communes. Mais, les systèmes d'information des forces de sécurité ne forment pas encore un système commun. Est également à déplorer la coexistence d'outils distincts pour une même utilisation (logiciels de rédaction des procédures : LRP-PN et LRP-GN), lesquels aboutissent de surcroît à des statistiques différentes.

Enfin, on constate ici et là une véritable absence de culture de la transformation, frein majeur aux évolutions nécessaires de ces maisons. Or la capacité à insuffler la culture du changement et à savoir évaluer la performance relève de la définition même du pilotage.

Une politique de recrutement qui évolue

À l'évidence, la société civile regorge de talents informatiques individuels. L'administration ne peut que chercher à attirer vers elle ce potentiel. L'innovation ouverte est par exemple un sujet pour la DGSI. Compte tenu des tensions à l'embauche sur ces profils et de l'évolution rapide des marchés, faut-il favoriser les recrutements en CDD ? Cette option fondée sur le pragmatisme comporte au moins une difficulté : celle de l'habilitation d'un personnel non titulaire. Dans tous les cas, le ministère doit éviter de s'en remettre uniquement aux ingénieurs et consultants des sociétés prestataires.

L'absence d'une gestion des corps techniques digne de ce nom et d'un profilage *intuitu personæ* se fait sentir. De même, l'ouverture du corps des commissaires de police à des scientifiques serait bienvenue. Un accompagnement personnalisé des fonctionnaires désireux de changer de voie est à favoriser.

Le recrutement d'opérateurs situés hors hiérarchie et issus de la société civile, à l'instar de la structuration d'une unité de contre-terrorisme au sein du NYPD[18], permettrait d'apporter un regard dérangeant mais assurément constructif.

Les attentats de Paris de janvier et novembre 2015 ont conduit les autorités à décider d'importants recrutements, qui auront un impact principalement sur les missions de voie publique et de renseignement. Dans ce dernier domaine, le Premier ministre envisage en outre, un recrutement spécifique de civils.

Pour les 2 731 policiers embauchés, des épreuves allégées et une formation ramenée à un an au lieu de deux, illustrent un changement qui n'est pas seulement symbolique. Au sein de la gendarmerie nationale, la création de 1 763 postes également en 2016, bouscule les méthodes en concentrant l'instruction sur les aspects opérationnels, les enseignements théoriques étant quant à eux, dispensés à distance (e-learning notamment). De fait, une forme de simplification s'engage.

Au sein des polices municipales, un effort conséquent de professionnalisation globale est indispensable, la maîtrise des outils informatiques en particulier n'est pas homogène.

(18) Mise en place après le 11 septembre 2001 sous l'impulsion de Raymond Kelly, la police de New York (NYPD) a créé une unité entièrement dédiée au contre-terrorisme. Dirigé par un ancien responsable du contre-terrorisme de la CIA, cette unité se caractérise par le fait qu'elle compte moitié de policiers et moitié d'universitaires, de chercheurs, d'avocats, de journalistes, ... Tous sont fermement invités à travailler en binôme, à faire remonter des informations (d'autres seront responsables de les analyser et de les filtrer), et à créer et entretenir des réseaux d'informateurs (35 000 : agents du métro, des services HLM, des services de l'emploi, ...). Un nouveau principe de fonctionnement étant que ceux qui livreront une information justifiant la mise en place d'une enquête seront associés à cette enquête.

Des adaptations qui doivent prendre en compte les évolutions du secteur privé

Parallèlement, des pistes de collaboration sont engagées avec le secteur privé (géants d'internet, industriels de la sécurité, ...) afin de ne pas isoler la sphère publique de cette réalité numérique.

Si le ministère de l'Intérieur n'a que récemment défini sa politique industrielle, on peut souhaiter la création d'un « Palantir[19] » à la française. Le passage à la police 3.0 mériterait même de se doter de personnels « capteurs immédiats d'évolution ». Autrement dit, d'agents aptes à suivre sans retard toutes les évolutions technologiques. À ce jour, il n'existe pas de démarche proactive de l'administration dans les salons de l'électronique. Une veille permanente est à penser.

Enfin, les disparités organisationnelles et méthodologiques évoquées et *a fortiori*, les manquements de l'action transverse et de coordination, renforcent cette nécessité d'opérer un diagnostic partagé. Il s'agit de se forger une vision coproduite en évitant dorénavant de démultiplier les projets.

(19) Société californienne créée en 2004, spécialiste de l'analyse des données et sous-traitant régulier des services de renseignement ou policiers américains, qui pousse actuellement ses pions en Europe.

Une nécessaire ouverture des recrutements

Au-delà des outils technologiques mis à la disposition des forces de sécurité, se pose la question des ressources humaines nécessaires à leur pleine exploitation, qu'il s'agisse de besoins ponctuels, pérennes ou spécifiques.

La valorisation des ressources internes

Face aux défis technologiques et opérationnels croissants, les forces de sécurité ont analysé leurs ressources internes. Au nombre des expériences menées, deux semblent plus significatives.

La sous-direction de la lutte contre la cybercriminalité (SDLC) à l'office central de lutte contre la criminalité aux technologies de l'information et de la communication (OCLCTIC) propose depuis une quinzaine d'années une formation métier dont l'objectif est de spécialiser des enquêteurs pour en faire en huit semaines des investigateurs en cybercriminalité (ICC). Chaque année, une cinquantaine d'ICC est formée et dotée des équipements matériels et logiciels indispensables à leur mission[20]. A l'issue de cette formation, ces nouveaux « experts » retournent dans leur direction d'origine pour intervenir, le cas échéant, sur des problématiques de cybercriminalité spécifiques.

L'absence de réelle sélection sur le niveau initial (compétences informatiques ou bureautiques minimales, ...) ou sur la répartition territoriale de ces nouveaux spécialistes laisse penser que la démarche engagée mérite certainement des améliorations.

(20) Pack d'une valeur de 11 000 euros intégralement financés par la DCPJ, quelle que soit la direction d'appartenance du futur ICC. On pourra s'étonner de ce principe budgétaire.

La gendarmerie nationale, qui affiche une culture plus scientifique que la police nationale de par son recrutement à la sortie des grandes écoles d'ingénieurs, a pris l'option depuis 2005 d'envoyer une sélection de gendarmes aux savoirs identifiés se former à l'Université de Technologie de Troyes. Ces enquêteurs N'Tech diplômés retournent par la suite dans chaque région de gendarmerie pour permettre à l'institution de disposer d'un maillage adéquat en ressources scientifiques.

L'institution militaire évalue à trois ans environ la durée nécessaire pour doter un agent, dont le potentiel a été détecté, d'une expertise employable au sein d'une direction demandeuse. Il sera bien entendu indispensable d'entretenir le potentiel de ce nouveau spécialiste, par l'intermédiaire de formations et d'une gestion de carrière adaptées.

Il s'avère complexe de former les agents qui sont en poste car cela prend du temps et de plus, ce type de ressource demeure rare, surtout dans le domaine informatique où les compétences deviennent rapidement obsolètes. Cela implique donc de procéder au recrutement de personnels déjà (hautement) qualifiés et dont les compétences sont à l'état de l'art au moment de leur recrutement.

L'intégration de profils scientifiques au sein des forces de sécurité

En matière de recrutement et d'une manière générale, la police nationale et la gendarmerie nationale orientent leurs besoins vers des généralistes. Ces forces sont en effet organisées afin de pouvoir intervenir en tout lieu et en tout temps ; les apports de profils scientifiques ou spécialisés restent une exception.

Progressivement, les spécialistes en nouvelles technologies, les investigateurs numériques, les primo-intervenants techniques, les cyber-enquêteurs, les référents sureté ou intelligence économique, ... ont vu leurs effectifs croitre sensiblement. Qu'ils soient en unités spécialisées, relais ou intégrés à des équipes mixtes, leur positionnement correspond à la satisfaction d'un besoin. Pourtant, les freins à l'employabilité sont réels.

L'acquisition d'une expertise prend du temps, suppose une démarche prospective en matière de ressources humaines, conditionnée notamment par l'usage d'outils adaptés et d'une politique volontariste dans ce domaine. Ces profils, pour certains à haute technicité, sont également très recherchés par les entreprises privées qui proposent des rémunérations supérieures à celles offertes par l'administration.

La tâche semble donc complexe pour la police et la gendarmerie.

La DGSI s'est engagée depuis quelques années dans l'élaboration d'un plan stratégique de recrutement et n'hésite pas à partir à la chasse aux talents via une recherche active, y compris en sortie des Grandes Ecoles. Pour cela, la direction sait devenir concurrentielle en matière d'émoluments.

En dépit de quelques expériences positives, la capacité de la police et de la gendarmerie à effectuer les changements RH nécessaires pour qu'elles disposent

des moyens de leurs objectifs demeure un sujet particulièrement aigu. Il persiste de nombreux freins structurels qui, combinés à une timide gestion prévisionnelle des emplois et des compétences, ne prédisposent ni la gendarmerie, ni la police à constituer de réelles opportunités de carrières pour nos jeunes talents.

L'intégration de ressources extérieures

Face à la difficulté à disposer au sein de ses propres effectifs de compétences spécifiques, la gendarmerie s'est organisée pour s'adapter aux enjeux émergents et compenser les carences en profils particuliers. Par le décret n°2008-959, l'institution a la possibilité de recruter par contrat des officiers ou sous-officiers pour satisfaire des besoins immédiats. Un arrêté du 21 janvier 2011 fixe la liste des emplois concernés. Assez hétérogène, ce panel est évolutif et doit couvrir l'ensemble des domaines.

Au nombre de 15 en 2005, ces « commissionnés » étaient 98 début 2016, reflet d'un recours accru à ce levier de recrutement. Toutefois, 75% sont des psychologues et le C3N n'a incorporé que trois docteurs en informatique.

Par ailleurs, le cadre administratif du « commissionnement » demeure rigide. Si la durée maximale cumulée des contrats est relativement longue (17 ans), les personnels n'ont pas la possibilité d'intégrer définitivement la gendarmerie à l'issue de cette période. Le commissionnement peut aussi s'avérer contraignant en termes de gestion globale des ressources humaines. Les commissionnés sont en effet intégrés à des grades correspondant à un niveau de rémunération. Or les grades ainsi occupés sont autant de promotions potentiellement bloquées pour les militaires de la filière classique.

Moins nombreux que les commissionnés, la gendarmerie a aussi recours à des agents contractuels pour des besoins davantage ponctuels et des missions spécifiques. Sans offrir d'opportunités de carrière sur le long terme, les émoluments proposés seraient en phase avec le secteur privé. Ce type de recrutement est toutefois en voie de diminution.

Dans un cas comme dans l'autre, un travail d'analyse et d'anticipation des besoins est réalisé et permet à chaque direction ou région d'exprimer ses objectifs de recrutement ou de formation.

Pour sa part, la police ne dispose pas d'équivalent au principe des emplois commissionnés. C'est ainsi que la plupart des besoins en profils scientifiques sont pourvus par l'intermédiaire de recrutements sur concours ou via les formations spécialisantes des policiers en poste. La sous-direction de la police technique et scientifique (PTS) parvient toutefois à intégrer des personnels contractuels au sein de ses effectifs, même si la règle reste l'intégration par voie de concours.

La DGSI dispose elle aussi de la possibilité de recourir à des recrutements contractuels. Cette tendance semble s'être accélérée depuis que cette direction est devenue autonome. Mais la part des effectifs contractuels y a été plafonnée à 15% afin de « *garantir l'identité policière du service* ». A titre de comparaison, cette proportion atteint déjà 23% à la DGSE[21].

(21) Commission des finances du Sénat, « *Les moyens consacrés au renseignement intérieur* », rapport d'information de la Commission des finances du Sénat, octobre 2015.

Au final, l'emploi de contractuels au sein des forces de sécurité s'apparente davantage à une exception très localisée qu'à une réelle possibilité offerte à l'ensemble des directions.

La nouvelle donne opérationnelle oblige pourtant les institutions policières à adapter leurs stratégies RH, notamment en matière d'emplois scientifiques. Les institutions doivent encore améliorer leur attractivité et apprendre à anticiper leurs besoins. Pour cela, les règles de gestion doivent évoluer vers plus de souplesse et de fluidité. Une dynamique naissante mais prometteuse semble engagée, qu'il convient d'encourager et de faciliter.

La collaboration ponctuelle avec les experts

Alors que nous évoquons les options administratives et contractuelles permettant l'intégration durable de compétences pointues au sein de la sécurité intérieure, force est de constater que d'autres voies gagneraient encore à être explorées pour mettre à la disposition des enquêteurs les expertises de certains de nos universitaires, journalistes ou autres personnalités qualifiées. Leur rôle d'observateur ou leur expertise pourraient à la fois enrichir et mettre en perspectives le champ de connaissances des enquêteurs et analystes de la police, de la gendarmerie ou des services de renseignement. Leurs connaissances fines (historiques, sociologiques, internationales, ...) de certaines formes de criminalité (stupéfiants, mafia, terrorisme, ...) ou tout simplement de certains milieux (radicalisme religieux, banlieues, mouvements contestataires, ...) ne devraient pas constituer un savoir « à part », mais représenter une source d'appui dans les enquêtes autant que dans la formation initiale ou permanente des personnels.

Cette mixité d'expertises n'a jusqu'alors guère été mise en œuvre. On ne peut donc qu'appeler, comme l'a fait Bernard Cazeneuve dans son discours du 20 avril 2016 à la DGGN, « à ce que les *années qui viennent soient des années d'ouverture du ministère de l'Intérieur à son environnement et notamment à son environnement universitaire et aux centres de recherche* ».

Une stratégie digitale pour quoi faire ?

Les enjeux d'une ambition digitale pour les forces de sécurité

La révolution numérique qui traverse actuellement toutes les organisations, qu'elles soient privées ou publiques, est traditionnellement présentée comme une double opportunité. Elle doit permettre d'une part, d'offrir aux clients ou aux usagers une nouvelle « expérience », intégrée et à plus forte valeur ajoutée. Elle

doit conduire d'autre part, les organisations à optimiser leur fonctionnement ; une aspiration d'autant plus pertinente pour le secteur public, soumis partout dans le monde à l'implacable équation du « faire mieux, avec moins ».

Pour les policiers et les gendarmes, la promesse de la révolution numérique est donc celle d'un travail plus riche, plus pertinent, plus proche des usagers et au final plus efficace.

Reste que les experts des transformations digitales soulignent la lourdeur du processus « *qui peut bien représenter dix années* » dès lors que la transformation se veut complète. Savoir ce que seront les technologies d'ici dix ans est impossible. Mais savoir ce que l'on veut être à ce même horizon, savoir ce que l'on veut faire et ce pour quoi on veut être reconnu est essentiel pour animer et entrainer les hommes et les femmes des forces de sécurité vers un but commun et une ambition collective. C'est cette vision stratégique qui définit le cadre dans lequel on pourra s'interroger sur les outils, moyens et technologies à mettre en œuvre pour atteindre ce but.

Proposition d'une vision digitale pour les forces de sécurité

Définir une ambition digitale à horizon de dix ans est un exercice d'autant plus lourd et périlleux qu'un ministre de l'Intérieur – la figure emblématique qui devra incarner, avec le DGGN, le DGPN et le DGSI, cette stratégie – ne reste en poste en moyenne que deux ans[22]. Avec des exercices sensiblement plus longs (le plus souvent, trois à cinq ans), les directeurs généraux peuvent plus facilement inscrire leur travail dans la durée.

(22) Sous la Ve République, il faut remonter à Raymond Marcellin pour trouver un ministre ayant travaillé sur un temps long, du 30 mai 1968 au 27 février 1974.

Souhaitons que les heures sombres qu'a traversées notre pays en 2015 permettent aux leaders qui porteront cette stratégie digitale pour les forces de sécurité de la lancer et de la porter jusqu'à un point de non-retour. Nous pouvons alors être ambitieux et proposer la vision suivante :

> *Devenir, grâce à l'usage des technologies numériques, l'une des trois forces de sécurité de référence dans le monde, pour son efficacité et pour la qualité du service offert à tous*

Le champ de progrès (passer de « bon » à « excellent ») est ambitieux, le but est noble et cette aspiration porte en elle-même un rapport gagnant-gagnant pour toutes les parties.

Déclinaison en une stratégie digitale opérationnelle

La stratégie digitale des forces de sécurité pourra alors s'articuler autour de quatre piliers :

- les points de contacts physiques (commissariats, brigades, mais aussi patrouilles ou stands mobiles, ...) : l'objectif sera ici d'offrir une expérience nouvelle aux citoyens ;

- les services rendus : quelle palette de services numériques offrir et développer ?
- les données : leur utilisation plus en profondeur et leur partage plus systématique garantiront des décisions mieux éclairées ;
- les processus internes : leur numérisation permettra une réduction des coûts (réels ou cachés), un gain de temps administratif au profit d'un temps à valeur ajoutée, et une plus grande efficience dans la gestion des tâches (la numérisation de la garde à vue[23] recèle par exemple un très fort gisement de productivité).

(23) La garde à vue est encore actuellement une procédure gérée sur papier au travers de multiples registres.

Toutefois, les coûts et la complexité d'une transformation sont tels que l'on ne peut pas agir sur tous ces leviers en même temps. Le point de départ de la transformation numérique devra rester adapté à la maturité de l'organisation et à ses objectifs stratégiques.

La figure ci-après illustre ce que pourrait être une première série d'actions (certaines sont déjà entamées).

Figure 5 : La transformation numérique des forces de sécurité nécessitera de prioriser les leviers et les opportunités

Une transformation digitale passe par trois étapes :

1. Définir une stratégie digitale
2. Actionner les leviers sur un élément de la chaîne de valeur (prévention, recherche, …) ou sur une problématique spécifique
3. Mettre en place les fondamentaux

1	**Stratégie digitale** *(vision et plan)*			
2	**Points de contact**	**Services**	**Données**	**Processus**
Prévention	Conseil aux usagers sur base de scoring	Intégration des objets connectés dans dispo. d'alerte	Analyse prédictive	Organisation des patrouilles
Recherche	-	Cyber patrouille	Big data (analyse des phénomènes criminels, …)	▪ LAPI ▪ Caméras intelligentes
Accueil et enregistrement des plaintes	▪ Proposition de rendez-vous ▪ Dossier à pré-remplir sur tablette en commissariat	▪ Plainte en ligne ▪ Dialogue en ligne avec un policier	▪ Suivi statistique ▪ Alertes locales sur infractions similaires	Allocation prédictive des ressources
Investigation	-	Appels à témoins	Big data (recherche de pistes, indices, …)	Partage d'information
Intervention	Alertes et conseils de prudence	-	Enrichissement des dossiers de cible	Accès en mobilité
Instruction	-	Appels à témoin	Big data (recherche de preuves, …)	Echanges numériques avec la justice
3	**Catalyseurs** *(structure organisationnelle, talents numériques, catalyseurs SI et changement culturel)*			

Source : McKinsey, analyse des auteurs

Bonnes pratiques en matière de déploiement d'une stratégie digitale

Pour organiser et réussir une transformation digitale en profondeur telle que nous le suggérons, quatre actions fortes devront être menées.

- Expliquer les raisons du changement et convaincre : pour que les individus comprennent ce qui est attendu d'eux, y trouvent du sens et y adhèrent (développement et partage d'une « histoire » couvrant tous les sujets et tous les niveaux de l'organisation).

- Développer les savoir-faire et les compétences : pour que les individus adoptent les comportements voulus (formation, gestion de carrière).
- Montrer l'exemple : pour que les individus comprennent l'importance et le caractère inéluctable du changement à partir des comportements qu'ils observeront chez leurs supérieurs, leurs pairs ou chez les leaders d'opinion et influenceurs de l'organisation.
- Renforcer le tout par des mécanismes formels : pour que les individus soient encouragés au changement par des structures, des processus, des systèmes d'information et des pratiques de reconnaissance et de récompense.

Une fois la stratégie digitale définie (quoi, pourquoi et avec quels objectifs), il importera de réfléchir (toujours en amont) aux indicateurs de performance chiffrés que l'on voudra suivre dans le temps pour mesurer et encourager les progrès, voire amener le passage à une phase suivante. Cela peut sembler élémentaire ; c'est pourtant une condition clé de réussite d'une transformation digitale. Comme évoqué lors de nos entretien avec les experts : « *Une des raisons majeures de faillite des systèmes digitaux dont nous avons suivi la mise en place tient dans l'absence de suivi d'indicateurs chiffrés. Ce qui fonctionne le mieux, c'est de définir une stratégie à 3-5 ans, qu'on pilote avec des indicateurs à 3-6 mois.* »

Un bon indicateur de performance doit couvrir trois aspects : la satisfaction des utilisateurs, le processus lui-même (e.g. degré de généralisation au sein de toutes les unités, ...) et le gain généré (financier, de temps, ...). Pour garantir une approche du changement à la fois ambitieuse et volontariste, la définition des objectifs chiffrés doit revenir aux leaders du changement (mode « *top down* ») et non pas être calquée sur des observations issues du terrain.

A titre illustratif, trois indicateurs pourraient être définis pour la numérisation de la garde à vue.

- Satisfaction des utilisateurs (policiers et gendarmes), avec l'objectif d'une note moyenne d'au moins 4 / 5.
- 50% des gardes à vue numérisées d'ici 12 mois.
- 20% de temps libéré pour les effectifs.

PRÉCONISATIONS POUR UNE POLICE 3.0

Transformer les structures en s'appuyant sur une vision à long terme

Préparer une nouvelle loi de programmation sur la sécurité intérieure et la justice

Dans un monde en mutation rapide où la menace terroriste constante conduit à des prises de décisions majeures et immédiates, le besoin d'un cadre et d'une vision à moyen-long terme parait d'autant plus nécessaire. Cela permettrait par exemple aux opérationnels de disposer d'une vision pluriannuelle de leur budget et de planifier leurs actions et leurs investissements plus sereinement et donc plus efficacement.

Ce cadre pourrait être apporté par une nouvelle LOPPSI (loi d'orientation et de programmation pour la performance de la sécurité intérieure). Cette troisième loi du genre pourrait voir son sigle s'enrichir d'une nouvelle lettre[24], « LOPPSIJ », afin d'étendre la réflexion à la justice et de mieux intégrer démarche d'investigation et chaine pénale. Respectueuse de la séparation des pouvoirs, cette loi consisterait dans les faits en deux textes distincts mais concomitants, et analyserait en détail les enjeux des ministères de l'Intérieur et de la Justice à horizon de dix ans.

(24) La LOPPSI 2 (2011) s'était déjà enrichie d'une lettre supplémentaire avec le « P » de performance.

Elle s'interrogerait notamment sur les ambitions, les moyens à y associer et sur des questions telles que la vidéoprotection, le *big data*, internet, le rôle et l'usage des réservistes (réserves opérationnelles et civiles), l'investissement en R&D (démonstrateurs, initiatives à explorer, ...), le renouvellement des matériels anciens ou devenus obsolescents, etc.

Il s'agit bien évidemment d'un exercice de méthode, à lancer et à piloter au plus haut niveau du gouvernement, pour dépasser les initiatives et contributions utiles mais ponctuelles que peuvent représenter les propositions de la délégation ministérielle aux industries de sécurité ou de quelques inspecteurs généraux de l'armement, les réflexions du Centre des hautes études du ministère de l'Intérieur et de l'INHESJ ou encore, les contributions des *think tanks*.

Mettre en place un véritable accompagnement du changement

Le pilotage du changement exige non seulement une volonté politique affirmée mais aussi une très large acceptation (au sens compréhension et adhésion) de la transformation des métiers. Le degré de maturité des structures est donc un facteur important. Le sommet de la chaîne hiérarchique doit impérativement s'approprier ces éléments, l'impulsion devant venir du Premier ministre et du ministre de l'Intérieur.

La gouvernance du changement peut alors se concevoir, sans créer de structures nouvelles, notamment à partir des six actions suivantes.

- Définir une vision pluriannuelle et une stratégie d'ensemble cohérente par l'intermédiaire d'une loi de programmation (voir *supra*).
- Associer la DGAFP au dialogue de gestion avec la direction du budget (la démarche a timidement débuté durant l'exercice 2016. Il appartient au cabinet du Premier ministre d'ancrer durablement ce principe).
- Instaurer un leadership dans le domaine du *big data* coordonné par un responsable ministériel des données et quelques animateurs (voir *infra*).
- Instituer des méthodes de travail nouvelles (recrutement sur profil, retours d'expérience systématiques, formation continue tout au long de la carrière, émission de propositions par les équipes de terrain via des ateliers de la performance).
- Créer un collège restreint d'experts indépendants, afin d'analyser les résultats et de lancer les orientations souhaitables. Situé hors hiérarchies ministérielles, cet organe aurait vocation à être le « poil à gratter » du système. Il serait composé de référents du monde de la recherche, du secteur privé et d'anciens hauts fonctionnaires de la police et de la gendarmerie. Ce collège examinerait à intervalles réguliers (semestriels voire trimestriels) les résultats de la délinquance ou les programmes d'actions initiés, non pas dans le but de « certifier » les chiffres, mais de livrer une analyse libre et hors système, s'appuyant notamment sur des retours d'expériences, d'enquêtes, de traitements informatiques que le collège aurait le pouvoir de solliciter. Son recul permettrait d'explorer des options que les services n'auraient pas naturellement tendance à retenir.
- Généraliser la pratique de remontée de propositions concrètes d'amélioration par les acteurs de terrain. Ainsi, les « Ateliers de la performance », processus fructueux mis en place par la gendarmerie nationale, peuvent trouver une déclinaison dans l'ensemble des services du ministère de l'Intérieur. Les équipes de terrain (tous grades, toutes fonctions) expriment des bonnes pratiques sous forme de fiche soumise à un collège de concepteurs, puis à un comité de suivi (avec avis des directions compétentes). Celui-ci valide les actions les plus pertinentes pour diffusion sur tout le territoire et appropriation par l'ensemble des services. Libre à ces derniers d'adopter les mesures les plus en rapport avec leurs besoins propres. Un premier bilan synthétique de l'action menée par la gendarmerie nationale pourrait servir de passerelle à la démarche de développement au sein de la police nationale.

Amplifier le décloisonnement

Les menaces contemporaines ont précipité les forces de sécurité et particulièrement les services de renseignement dans un monde caractérisé par le temps court et le besoin d'échanges. Ce qui a longtemps été aux antipodes de la culture policière (celle du secret et du temps long). La collaboration et le partage d'informations deviennent donc une priorité absolue.

Des initiatives ont montré qu'une collaboration entre services ou que des équipes pluridisciplinaires (les groupes d'intervention régionale, les juridictions inter-régionales spécialisées, la DGSI et le service central de renseignement territorial (SCRT) qui associent leurs forces pour lutter contre la radicalisation, ...) pouvaient obtenir de meilleurs résultats.

Toute action ou toute réorganisation qui permettra de construire une police décloisonnée doit donc être encouragée :

- mutualisation et convergence des équipements et des outils informatiques (entre police et gendarmerie, mais aussi entre services au sein de chaque maison) ;
- mutualisation des formations ;
- exercices ou réflexions prospectives menés en commun ;
- mobilité croisée entre services ou institutions et management partagé des équipes support ; échanges de cadres dirigeants comme cela a été fait avec succès entre la DGSI et la DGSE ;
- désignation de correspondants au sein de chaque service ;
- réunions d'échanges régulières (suivi d'activité, échanges de bonnes pratiques, ...) ;
- système de suivi des performances et de dialogue de gestion qui, du plus haut niveau jusqu'à l'échelon local, analyse et encourage la collaboration et le partage d'informations ;
- Intégration de la dimension « collaboration » dans la politique d'évaluation, de promotion et de rémunération ;
- rapprochements organisationnels (e.g. faut-il réunir la DGSI et le SCRT, mais aussi la sous-direction de l'anticipation opérationnelle (SDAO) de la gendarmerie ? Faut-il regrouper les services de police et de gendarmerie en charge de la cybercriminalité ? ...) ;
- etc.

Décloisonner en particulier l'accès à l'information

L'application stricte du principe de spécialité des fichiers a conduit à une démultiplication des fichiers étatiques (police, justice, social, financier, fiscal, ...). Cette prolifération et le cloisonnement des fichiers rendent leur accès difficile sinon impossible. Quant au croisement des informations qu'ils contiennent avec des fichiers privés (opérateurs de télécommunication, fournisseurs d'accès, ...), il est quasiment exclu.

Une simplification des procédures de consultation, de traçabilité et de contrôle *a posteriori* permettrait d'optimiser leur exploitation, tout en garantissant une meilleure protection des droits fondamentaux et de la vie privée des personnes.

Ceci pourrait se faire par la mise en place des trois procédures suivantes.

- Une procédure d'accès ponctuel et de consultation simplifiée aux différents fichiers de l'Etat, par toutes forces opérationnelles et sous réserve de traçabilité. Cette procédure pourrait se faire notamment par la mise en place d'un identifiant unique propre à tout enquêteur et d'une sécurisation (mot de passe, certificat, carte professionnelle, ...) permettant une identification préalable et garantie.
- Un formulaire unique de demande d'informations issues des différents fichiers de l'Etat. Son utilisation permettrait d'éviter des saisies multiples et successives sur des formulaires propres à chaque fichier, tâche extrêmement chronophage pour les enquêteurs. Ceci pourrait être réalisé grâce à des champs de collecte des données harmonisés et applicables à tous les fichiers, ainsi qu'à une uniformisation des systèmes d'information des services. Un tel formulaire faciliterait le contrôle des informations obtenues, des bases de données sollicitées et de leur exploitation. Par ricochet, le droit d'accès et de modification des personnes en serait également amélioré.
- Une procédure de contrôle stricte par une autorité judiciaire (magistrat tel que le juge des libertés et de la détention) et *a posteriori* permettant de garantir le respect des droits des personnes et des conditions dans lesquelles ces consultations et extractions ont été effectuées, sans ralentir l'avancement des enquêtes.

Le respect des exigences législatives serait assuré, d'une part, grâce à l'absence de constitution d'un fichier global, d'interconnexion de fichiers ou d'accès libre et constant par les enquêteurs et, d'autre part, grâce à la parfaite traçabilité des accès, consultations et extractions, et leur contrôle *a posteriori* par une autorité distincte et indépendante. Cette approche serait par ailleurs en ligne avec les valeurs et droits fondamentaux défendus notamment par la commission nationale de l'informatique et des libertés (CNIL).

A l'avenir, il serait bon d'imposer dans le cahier des charges de tout système de gestion de données, son interopérabilité obligatoire avec les autres systèmes d'information préexistants afin de faciliter une cohésion d'ensemble et la pérennité des procédures précédemment évoquées.

Réfléchir à la mise en place d'un service dédié à l'analyse de l'information numérique

La création d'un service unique chargé de centraliser et de traiter des données d'origines diverses (police, gendarmerie, justice, publique ou privée), qui serait animé par des experts de la signification et de l'usage de ces données, pourrait apparaitre comme une idée séduisante. Elle soulève toutefois des questions organisationnelles et légales dont la lourdeur déborde le cadre de nos travaux.

Compte tenu du poids que représenteront demain les données dans la lutte contre toutes les formes de criminalité, une réflexion en ce sens pourrait utilement être engagée par le ministère de l'Intérieur.

Un tel service permettrait par exemple de mieux capitaliser sur les bonnes pratiques d'exploitation des données (cohérence des données stockées, centralisation des responsabilités de conservation, traitements pertinents, partage rapide d'expériences entre opérateurs, ...), de mieux contrôler l'accès aux données et d'en assurer la traçabilité.

Mettre en place une véritable gestion de projet des systèmes d'information

De nos entretiens, il ressort que les causes d'échec de nombreux projets informatiques ou technologiques s'expliquent notamment par leur durée trop longue et des ambitions excessives voire pharaoniques en matière de fonctionnalités.

Pour tenir compte de l'évolution de plus en plus rapide de la technologie et des besoins fonctionnels, les futurs projets devraient répondre aux règles suivantes.

- Limiter à trois ans leur durée maximale (garantie contre le risque d'obsolescence).
- Mettre en place une maitrise d'ouvrage forte, commune à la police et à la gendarmerie pour gérer le schéma directeur.
- Viser un objectif de standardisation entre la police et la gendarmerie sans en faire une question de principe.
- Ajouter à l'objectif de standardisation un objectif d'interopérabilité, pour une efficience globale renforcée.

Développer les talents déjà présents au sein des institutions

Mettre en place une véritable gestion prévisionnelle des emplois et des compétences

Pour préparer la police telle qu'elle devra être dans cinq à dix ans, police et gendarmerie doivent s'interroger sur leurs besoins par poste, par mission et par territoire sur cet horizon de temps. Il s'agira non seulement de s'interroger sur les emplois futurs, mais aussi sur les évolutions de carrière.

Cette véritable démarche de gestion prévisionnelle des emplois, des effectifs et des compétences (GPEEC) devra être coordonnée, sinon unifiée, entre police et gendarmerie. Surtout, elle devra être sanctuarisée pour ne pas subir les à-coups des évènements ou des décisions politiques à court terme.

En ce sens, la direction générale de l'administration et de la fonction publique (DGAFP) peut jouer un rôle critique, tant comme garante de l'homogénéité de la politique de ressources humaines au sein de l'administration, que pour veiller au respect des trajectoires d'emplois et de compétences par rapport aux choix qui auront été faits et mis à jour périodiquement.

Créer et valoriser des filières dédiées à l'investigation numérique

Des formations de grande qualité existent déjà qui permettent à la police et à la gendarmerie de disposer de centaines d'investigateurs spécialisés en analyse numérique et en cybercriminalité. Mais peu semble fait pour maintenir, animer et valoriser ces compétences qui seront demain essentielles dans un monde digital et hyper connecté.

Une première démarche, qui s'inscrirait dans une vision à long terme, consisterait à mutualiser les efforts de formation de la police et de la gendarmerie. Mieux : dans la mesure où l'on sait que les emplois numériques peineront à être pourvus dans les années qui viennent faute d'individus formés[25], police et gendarmerie pourraient mettre en place une structure commune dédiée à la formation continue numérique. Véritable pôle d'excellence, ce centre proposerait des modules spécifiques à la cybercriminalité et à l'investigation numérique. Dispensées par des experts extérieurs (ANSSI, chercheurs des universités, acteurs privés, ...) et des enseignants maison (enquêteurs, ...), ces formations seraient à la pointe de l'art tout en restant en phase avec les besoins opérationnels courants. Elles seraient accessibles aussi bien au titre de la formation continue (sur inscription motivée et pour des individus affichant un bagage minimal en bureautique voire en numérique) que sur concours externe (constitué d'épreuves spécifiques et pertinentes), et sans que cela ne vienne affecter les possibilités de recrutements contractuels lorsque les besoins (compétences ou immédiateté) l'exigent.

D'ici là, les programmes mis au point par les uns doivent être ouverts et reconnus par les autres. Il est ainsi regrettable que le label ICC puisse être attribué à des gendarmes, mais que la réciprocité ne joue pas avec le label N'Tech.

Une fois formée, les ICC et les gendarmes N'Tech doivent voir leurs compétences sollicitées[26], donc activement mises en pratique et entretenues, ce qui peut supposer une gestion nationale et centralisée de ces profils (voir par ailleurs nos préconisations en matière d'analyse prédictive et de gestion des talents analytiques associés). Les attentes de ces personnels en termes de statut, de plan de carrière, de gratification financière voire de validation diplômante des acquis de l'expérience (VAE) pourront alors trouver un écho légitime.

(25) Inspection Générale des affaires sociales, « *Les besoins et l'offre de formation aux métiers du numérique* », Rapport conjoint de l'IGAS, février 2016

(26) Une enquête récente de la sous-direction de la lutte contre la cybercriminalité (SDLC) montrait que 10% des ICC n'avaient pas eu de dossier de cybercriminalité à traiter au cours des douze derniers mois. Certains n'en avaient eu qu'un seul.

Assurer une juste correspondance entre besoins, dotations et utilisations

L'envoi des policiers en formation ICC étant défini par les directions centrales d'emploi en fonction des quotas annuels auxquels elles ont droit, l'organisation peut vite paraitre manquer de planification ou de vision d'ensemble. Une

analyse des besoins par service ou par géographie préalable à l'attribution des formations pourrait apporter plus d'efficience dans le système.

De même, une validation préalable des profils à former, tant en termes de motivation que de compétences élémentaires, semble s'imposer. Le suivi de modules d'auto-formation serait ainsi un excellent prérequis. La sélection des candidats sur entretien apporterait une garantie ultime.

Enfin, l'attribution de l'équipement standardisé d'ICC en fin de formation doit elle aussi s'adapter aux besoins et aux utilisations futures. Il nous parait préférable de privilégier une technologie à la pointe et un ordinateur récent, à un équipement complet qui risque d'être frappé d'obsolescence avant même d'avoir été « rentabilisé ».

Attirer de nouveaux talents

Adapter et ouvrir les concours

Dans le monde contemporain, rien ne semble justifier la primauté des formations juridiques parmi les cadres supérieurs de la police et de la gendarmerie, qui ont bien d'autres compétences à mobiliser que le droit. Force est ainsi de constater que sa plus large ouverture aux profils scientifiques confère à la gendarmerie une plus grande agilité dans l'appropriation du défi numérique.

Les épreuves doivent donc être repensées, notamment dans les concours de la police, pour permettre aux non-juristes de postuler sans partir avec un handicap.

Dit autrement, les forces de sécurité doivent veiller à intégrer notamment des profils scientifiques et numériques parmi leurs nouvelles recrues, y compris sur des postes de commissaires ou d'officiers. Police et gendarmerie devront pour cela renforcer leur attractivité en tant qu'employeurs par rapport au secteur privé et développer des atouts suffisants (rémunération, perspectives de carrière, formation, mobilité, ...) pour identifier, attirer et intégrer les meilleurs éléments.

Enfin, une mise en phase des processus de recrutement (calendrier des concours) avec les sorties d'école ou l'arrivée sur le marché du travail de jeunes diplômés permettrait d'éviter que police et gendarmerie ne soient des orientations par défaut (même si les attentats de 2015 semblent avoir changé la donne). Une campagne de communication adaptée, menée dans des établissements ciblés, tout comme le développement de contrats d'apprentissage, pourraient constituer d'autres leviers de sélection efficace des candidats.

Elargir le champ des officiers commissionnés

Si le principe du recrutement d'officiers commissionnés est intéressant pour l'accès à des compétences pointues et la diversification des profils qu'il permet, les volumes concernés demeurent encore trop modestes pour générer un impact significatif.

La formule peut par ailleurs gagner en souplesse, tant en termes de perspectives de carrière offertes (promotion, intégration définitive au sein de l'institution, ...) que de variété des profils et compétences éligibles. La liste des emplois admis pourrait ainsi intégrer une dimension de gestion prévisionnelle des compétences.

Ceci étant et compte tenu des contributions positives de la formule, on pourrait s'interroger sur son extension à la police nationale et à la DGSI.

Favoriser les interactions avec le monde extérieur

Nous avons détaillé (voir chapitres 1.2.5 et 1.2.6) ce que pourrait être un partenariat efficace entre la police, la gendarmerie et le secteur privé (collaborations en matière de R&D, d'enquêtes, d'accès à des expertises de pointe, de soutien à l'exportation, ...).

Parce qu'elle constitue aussi une façon d'impliquer les citoyens et de cultiver l'image de proximité et de professionnalisme des forces de sécurité, la sollicitation des compétences ou de contributions externes, académiques ou privées, doit être encouragée. Ces échanges pourraient être mis à profit pour maintenir le niveau de connaissance et d'excellence de nos forces dans la durée. Pour les encourager, une « bibliothèque » des profils experts partenaires pourrait être créée et rendue accessible au plus grand nombre. Elle contribuerait au partage des contacts entre services et à l'élargissement des domaines d'intervention de cette communauté externe.

L'initiative du « marathon de la programmation informatique » organisé en avril 2016 par la gendarmerie nationale va dans ce sens. Encadrés par le ST(SI)², 26 étudiants d'écoles d'ingénieurs ont pu ainsi contribuer à améliorer le fonctionnement de l'application GendLoc.

Enfin, cette « complicité » pourrait bien entendu viser les sociétés de sécurité privée. Dans le comté de Stockholm, la collaboration est par exemple forte depuis 2009 entre les patrouilles de Securitas et les forces de police locales ou nationales : transmission d'informations ciblées aux autorités, notification des véhicules en stationnement gênant pour verbalisation, prévention d'attroupements nuisant à la tranquillité publique, ... Les équipements radios des agents privés sont même compatibles avec ceux des pompiers pour permettre une assistance face à une situation critique, tandis que les équipements vidéos embarqués sont connectés au réseau de surveillance municipal pour apporter tout élément probant aux forces de sécurité.

Mettre en œuvre la stratégie digitale

Nous avons débattu (voir chapitre 2.4) ce que pourrait être une ambition digitale pour les forces de sécurité françaises, ainsi que les bonnes pratiques à suivre pour assurer son déploiement. Pour écrire et mettre en musique cette stratégie digitale, nous pensons qu'elle doit être incarnée au plus haut niveau

et travailler prioritairement à libérer les personnels des tâches chronophages et sans valeur ajoutée, en tirant profit des gains de productivité que peuvent apporter les nouvelles technologies.

Créer un poste de directeur digital au sein du ministère de l'Intérieur

Pour attester de l'enjeu et réussir la transformation digitale telle que nous la suggérons (« *Devenir, grâce à l'usage des technologies numériques, l'une des trois forces de sécurité de référence dans le monde pour son efficacité et pour la qualité du service offert à tous* »), le ministère de l'Intérieur pourrait se doter d'un directeur digital.

Rattaché directement au ministre, il piloterait l'intégralité de l'agenda de transformation numérique du ministère (définition et mise en œuvre de la stratégie, formation, ...) et aurait vocation à travailler transversalement avec l'ensemble des directions générales pour mener à bien la digitalisation de toute l'organisation.

Avant tout spécialiste du numérique et entouré de conseillers experts[27], le directeur digital veillera à la numérisation de plusieurs processus (e.g. garde à vue, authentification des Officier de police judiciaire par signature électronique, archivage et accès aux archives, ...), tout en s'assurant d'intégrer dans les processus policiers l'ensemble de la chaîne administrative (Justice, Trésor, ...).

(27) Le Président exécutif d'Alphabet (Google), Eric Schmidt, va par exemple diriger un comité de conseil du Pentagone en matière d'innovation technologique (analyses complexes de données, organisation du partage d'information, ...), *Les Echos*, 4 mars 2016.

Il sera responsable de développer les points de contacts en ligne et les services internet (e.g. dialogue en ligne, prise de rendez-vous, pré-remplissage des dossiers à partir de tablettes mises à disposition du public à l'arrivée au commissariat ou en gendarmerie, politique de cyber patrouille, politique de communication sur internet, ...).

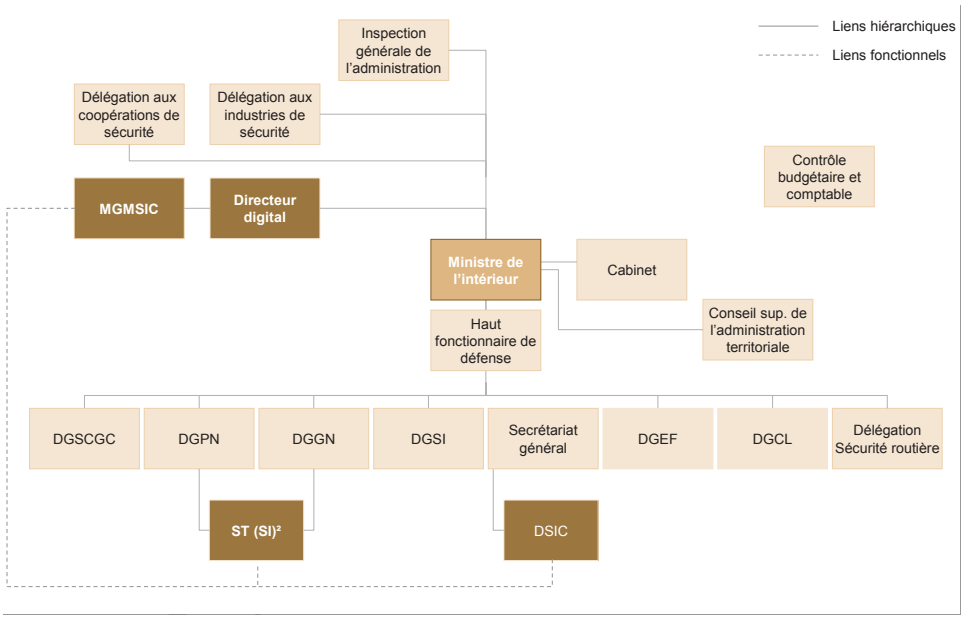
Le directeur digital exercera encore son leadership dans le domaine du *big data*, pour accélérer la diffusion de ces techniques au sein du ministère (en mode réactif pour aider à la résolution d'enquêtes, comme en mode proactif pour éclairer les axes de surveillance) et encouragera les initiatives d'analyses avancées (analyse prédictive, surveillance d'internet et des réseaux sociaux, ...). Il œuvrera à faciliter le maillage des fichiers et définira la politique d'ouverture publique des données (« *open data* »), en lien et en cohérence avec l'approche développée par l'administrateur général des données.

Pour faciliter la coordination entre les différents services en charge des systèmes d'information (ST(SI)² et DSIC notamment) et garantir l'indépendance des arbitrages sur ces sujets, nous préconisons que la MGMSIC (Mission de gouvernance ministérielle des systèmes d'information et de communication), actuellement rattachée comme la DSIC au Secrétariat général du ministère de l'Intérieur, soit à l'avenir placée sous l'autorité du directeur digital. Cet aménagement organisationnel devrait être source de cohérence d'ensemble, de continuité et de plus grande efficacité dans le développement et la gestion des systèmes d'information.

Plus généralement, le directeur digital travaillera au développement des compétences digitales et analytiques (*data scientists*, ...) au sein des directions,

tout en veillant à développer une culture numérique du top management du ministère et de ses directions générales. Il sera une des chevilles ouvrières du décloisonnement de l'accès à l'information.

Figure 6 : Positionnement du directeur digital au sein du ministère de l'Intérieur



Source : réflexions des auteurs

Compte tenu de l'étendue de son rôle, il participera aux décisions d'investissements clés du ministère, notamment pour contribuer directement aux réflexions en matière de priorités, d'ambitions à moyen et long terme, ou d'arbitrages à court terme.

C'est donc *in fine* la création d'un poste extrêmement stratégique de « Directeur du numérique, de la stratégie et des programmes » que nous appelons de nos vœux.

Dématérialiser les processus métiers, y compris avec la Justice

Dans un univers encore largement dominé par l'écrit et le papier (registres de suivi et de contrôle des activités, circulaires, notes de services, télex, ...), la numérisation des processus policiers permettrait de réaliser de très nets gains de productivité et d'efficacité. Comme nous l'avons montré plus haut, les heures de travail ainsi libérées pourraient représenter l'équivalent de plus de 20 000 postes de policiers et de gendarmes.

Le remplacement de l'intégralité des registres existants (gardes à vue, écrous, armes, armes non létales, armes pour les adjoints de sécurité, ...) par des applications informatiques de type intranet apparait donc comme une priorité. Cette numérisation pourra s'appuyer sur une gestion adaptée des profils utilisateurs et un recours systématique à la carte professionnelle, encore trop peu utilisée, comme moyen d'authentification et de signature électronique. C'est

la voie qu'a décidée d'emprunter la gendarmerie nationale voici quelques années. A son tour, la DGPN s'engage dans une dématérialisation complète de la gestion des gardes à vue. Il reste à convaincre l'autorité judiciaire de supprimer le registre correspondant dans sa version papier et de numériser la transmission des informations aux procureurs ou aux magistrats instructeurs.

De la même façon, les instructions hiérarchiques doivent pouvoir bénéficier des fonctionnalités nouvelles offertes par le projet « mobilité » en cours de déploiement. On pourra aussi s'interroger sur le formalisme des télex transmis via le RESCOM, dont la lourdeur n'est pas nécessairement gage d'efficacité. Dans ce domaine, la gendarmerie nationale a résolu de se tourner vers une messagerie tactique, beaucoup plus légère et proche d'une messagerie de type Outlook, pour faire transiter les instructions de commandement.

Dématérialiser la preuve numérique et sa gestion

Alors que le numérique fait émerger et se multiplier de nouveaux types de preuves issues des smartphones, de la vidéoprotection, des objets ou des véhicules connectés, les règles procédurales imposent toujours de matérialiser la preuve numérique sur un support physique afin qu'elle soit traitée comme telle.

Ce processus pourrait être optimisé par l'adoption d'un standard commun à tous les enquêteurs en matière de collecte et d'analyse des preuves numériques. Leur partage et leur archivage s'en trouveraient facilités.

Police et justice gagneraient donc à s'interroger sur les solutions techniques qui permettraient précisément de traiter la preuve numérique dans son environnement originel, quitte à ce qu'elles imposent une révision de la procédure pénale.

Compte tenu de leur abondance, une solution tout d'abord dédiée au traitement des fichiers vidéo (collecte, identification, gestion, partage, analyses avancées, ...) pourrait être mise en œuvre. Conçue dès le départ comme une plate-forme ouverte, cette solution pourrait par la suite être étendue à d'autres formes de preuves numériques, ce qui permettrait de neutraliser les risques associés à une approche voulue immédiatement plus globale.

La carte professionnelle pourra ici encore appuyer ce processus de numérisation, en permettant aux officiers de police judiciaire de signer numériquement leurs preuves comme ils le feraient avec la pose d'un scellé sur une preuve matérielle.

Au final, un tel dispositif de gestion des preuves serait pour les enquêteurs une source de gain de temps, permettant une meilleure focalisation sur leur cœur de métier et les tâches à plus forte valeur ajoutée.

Unifier les systèmes d'identification et d'authentification

Les accès aux systèmes d'information de la police et de la gendarmerie sont gérés de manière disjointe. Il n'est pas possible aujourd'hui de se connecter à l'ensemble des applications avec une identification et authentification unique.

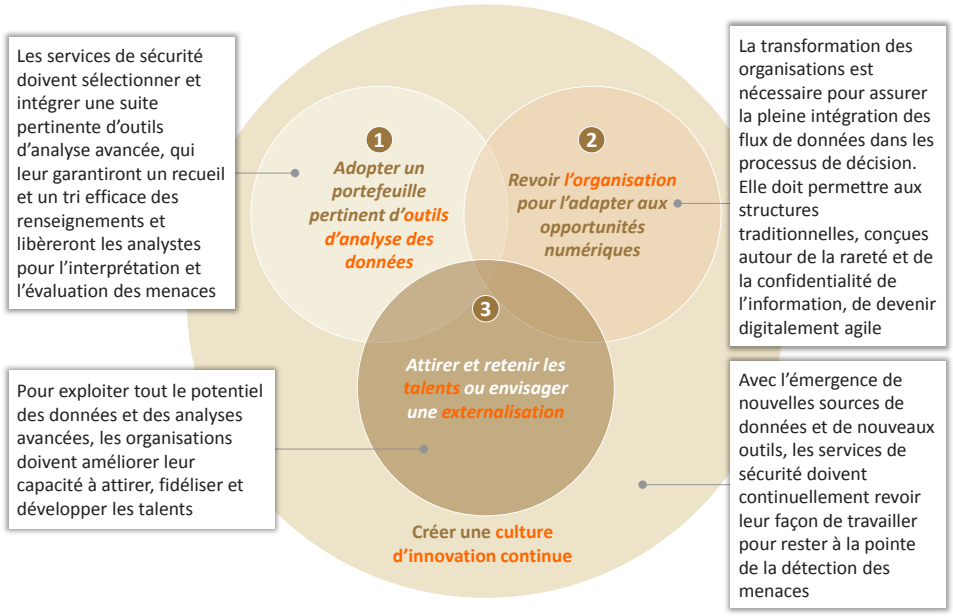
Pour encourager la convergence, il convient de travailler à unifier les systèmes d'identification et d'authentification des deux institutions.

On pourra profiter de l'opportunité de ce projet pour simplifier la gestion des droits par la mise en place de profils et de rôles standards communs aux deux entités.

Muscler les dispositifs d'investigation numérique

Mettre en place des dispositifs d'investigation numérique place les forces de sécurité, partout dans le monde, face aux trois mêmes défis : technique, organisationnel et de gestion des talents.

Figure 7 : les forces de sécurité font actuellement face à trois défis pour exploiter pleinement et effectivement la puissance des données



Source : McKinsey (ligne de service Police, 2016)

Pour répondre efficacement à ces impératifs, nos forces de sécurité doivent se doter d'un dispositif de veille sur l'investigation numérique, s'équiper et se structurer pour surveiller internet et les réseaux sociaux, et considérer le cyberespace comme un nouvel espace à défendre.

Mettre en place un dispositif de veille sur le marché de l'investigation numérique

Les logiciels et solutions technologiques de surveillance d'internet et des réseaux sociaux sont extrêmement nombreux. L'offre est mondiale, en perpétuelle évolution

et souvent tirée par de jeunes pousses innovantes (américaines, israéliennes, ...) dont les produits sont complémentaires mais jamais substituables.

Bien que cela ne soit pas leur cœur de métier, policiers et gendarmes se doivent de suivre au plus près l'évolution de ces marchés, identifier les innovations au plus fort impact potentiel et s'interroger sur leur intégration. Laisser ce travail de veille aux mains des éditeurs ou des fabricants eux-mêmes serait perdre en indépendance. Le confier à une agence de veille technologique aurait un coût et poserait la question de son expertise sécuritaire.

Sans que cela représente un investissement majeur, police et gendarmerie pourraient, de manière mutualisée, conduire ce travail de veille active. Un groupe de trois à six personnes, mêlant informaticiens passionnés et enquêteurs expérimentés, constituerait une communauté de collecte, de diffusion et d'expertise s'appuyant sur des visites de salons internationaux, des lectures, des échanges avec d'autres forces de sécurité à travers le monde, etc. Le partage se ferait avec des référents désignés au sein de chaque direction centrale et à plusieurs échelons géographiques. Cette communauté d'experts serait bien sûr associée à chaque nouveau projet ou à chaque appel d'offres relatif à l'investigation numérique.

S'équiper et se structurer pour surveiller internet et les réseaux sociaux

Pour détecter les signaux faibles de menace, les forces de sécurité doivent se doter des outils les plus à la pointe en matière de surveillance d'internet (recherche sur l'internet profond ou sur le « *Dark web* ») et de surveillance des réseaux sociaux (analyse des liens interpersonnels, des rediffusions de contenus, ...). Les applications opérationnelles sont nombreuses : surveiller la propagande terroriste et les échanges entre profils radicalisant, lutter contre le trafic d'armes ou contre la pédopornographie, suivre les mouvements contestataires et anticiper leurs actions, ... De nombreux outils existent que nous n'évoquerons pas ici.

Même si les besoins et les missions diffèrent, un minimum de mutualisation devra être recherché dans le déploiement de ces moyens : partage de l'accès aux outils, transparence sur les axes de travail pour éviter les doublons, fertilisation croisée grâce à l'échange d'informations et d'analyses et bien sûr, économies d'échelle.

Le SCRC, le C3N, l'OCLCTIC, la SDAO, le SCRT et la DGSI (tout comme la DGSE) sont *a priori* les services qu'il conviendra de doter de telles capacités. A terme, on pourra s'interroger sur la mise en place d'une entité unique chargée de ces surveillances du cyberespace et qui travaillerait pour l'ensemble des forces.

D'ici là, le travail doit être mené par des analystes aguerris à l'univers d'internet, spécifiquement formés aux nouveaux outils et travaillant en binôme avec des enquêteurs (comme les ICC de l'OCLCTIC) de manière à assurer la pertinence et le caractère opérationnel de leurs analyses.

Enfin, il est essentiel que ce travail de surveillance d'internet et des réseaux sociaux se fasse dans un esprit de partage de l'information. Les analyses devront donc alimenter régulièrement et proactivement les directions centrales et l'ensemble des services, centraux ou territoriaux, en charge du renseignement, du contre-terrorisme, du contrôle aux frontières ou du maintien de l'ordre.

Intégrer le cyberespace comme un nouveau terrain à occuper

L'espace numérique devenant un espace de souveraineté à part entière, police et gendarmerie devront, à l'image des armées, l'envisager comme un nouvel espace à occuper pour éviter que n'y prospèrent les zones de non-droit.

Au-delà de la surveillance « en civil » que nous venons d'évoquer, les forces de sécurité devront dans la décennie à venir affirmer une présence crédible sur internet et sur les réseaux sociaux. Cette présence reste encore à imaginer : « ilotage » sur les forums de discussion ou chez les fournisseurs de service, sollicitation de « police secours » depuis sa session de navigation internet, diffusion de messages de prévention ciblés sur certains sites voire présence visible, ...

En particulier, cette cyber-police a un rôle à jouer en matière de contre-propagande ou de contrôle des rumeurs (djihadisme, manifestation dans les « zones à défendre », ...). L'expérience montre que l'impact peut être réel. Ainsi lors des émeutes d'août 2011 à Birmingham, la police britannique a su, depuis internet et en agissant ouvertement aussi bien que dans l'ombre, apaiser les tensions naissant autour des manifestations.

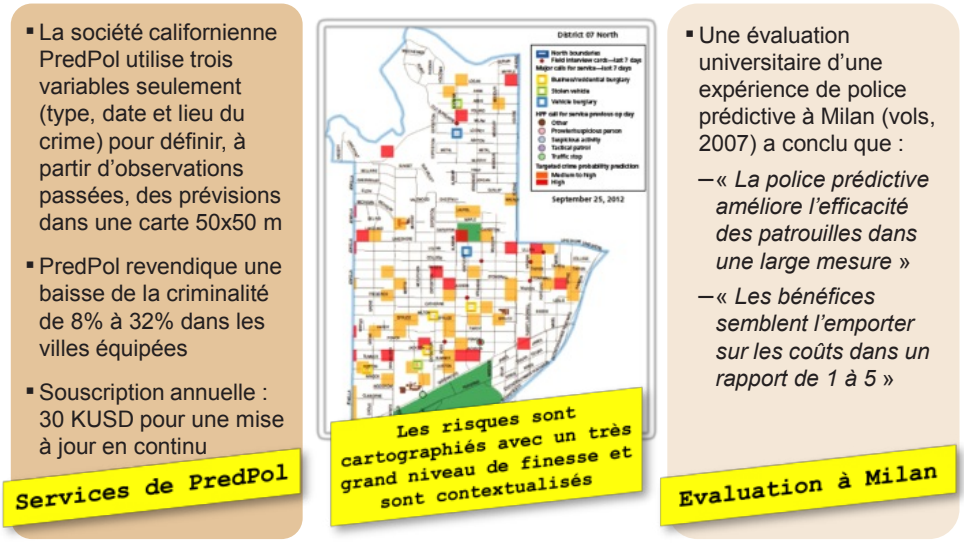
Accélérer et pérenniser les approches prédictives

Etendre les expérimentations, notamment en ZSP, en vue d'une généralisation

Depuis plusieurs années, les expériences de police prédictive se multiplient, principalement outre-Atlantique. Après New York et une démarche statistique presque élémentaire, Los Angeles, Atlanta et des villes de taille moyenne revendiquent des baisses significatives de la criminalité grâce à la mise en place de patrouilles définies en fonction des « prédictions » issues d'algorithmes parfois extrêmement simples. Plusieurs villes d'Europe (en Allemagne, en Italie, au Royaume-Uni, ...) sont désormais gagnées par cette vague « prédictiviste ».

La France est culturellement attentive à préserver l'esprit d'initiative de ses policiers de terrain et une décision « d'origine humaine », tout en évitant un

Figure 8 : plusieurs illustrations accréditent l'idée d'efficacité de la police prédictive



Source : site internet de PredPol ; Le Monde (04/24/2015) ; Université d'Essex, "*Information Technology and Police* Productivity", G. Mastrobuoni, 2015 ; Rand Corporation, *"Predictive policing"*, 2013

1 Créée en 2012 ; 25 employés ; chiffres d'affaires 2014 : 0.62 MUSD. Les villes clientes incluent Atlanta, Londres, Los Angeles, Montevideo, Munich, ...

traitement à courte vue qui pourrait générer un déplacement géographique de la délinquance. Mais dans un contexte de ressources limitées voire sur-employées, les forces de sécurité n'ont d'autre choix que de gagner en efficacité opérationnelle en utilisant les outils, données et ressources dont elles disposent.

Il parait donc important que les expérimentations actuellement menées par le Service central de renseignement criminel de la gendarmerie nationale[28] soient étendues rapidement à d'autres zones géographiques. Le ministère de l'Intérieur dispose sur ce terrain d'une belle opportunité de mutualisation, qui consisterait à transférer les développements statistiques et le savoir-faire des gendarmes dans l'univers métier et géographique de la police.

On pourrait aussi considérer que parmi les 80 zones de sécurité prioritaires (ZSP), les plus sensibles bénéficient sans délai d'une expérimentation d'analyse prédictive, en osant sans tabou construire et regarder des prédictions par demi-journée, propres à l'organisation des patrouilles.

(28) Le SCRC expérimente actuellement un programme d'analyses prédictives en Aquitaine (délinquance générale en zone gendarmerie) et dans l'Oise (vol de voiture en zones police et gendarmerie).

Développer une stratégie de gestion à long terme des talents analytiques

La mise en place et l'utilisation opérationnelle d'analyses prédictives imposent des compétences nouvelles : analyses statistiques, traitement de données, capacité à comprendre le métier et les besoins des patrouilles ou des enquêteurs pour les traduire en une méthodologie mathématique de recherche.

Au-delà des recrutements ciblés qu'il faudra lancer pour intégrer ces compétences nouvelles, il conviendra de définir ce qui permettra de retenir ces « *data scientists* » que le secteur privé s'arrache déjà : salaire, contenu du poste, filière de développement, ... La collaboration avec les universités ou les centres de recherche (par exemple, l'Observatoire national de la délinquance et des réponses pénales, ...) peut apporter une stimulante émulation. De même que la constitution de binômes *data scientist* et enquêteur.

Accompagner la diffusion de l'analyse prédictive dans l'organisation

Nos entretiens ont permis de mesurer une certaine résistance qui pourrait freiner le déploiement de l'analyse prédictive. Comme l'installation des systèmes de géolocalisation dans les véhicules, elle pourra être perçue comme une perte d'autonomie par une base qui considère que l'expérience et les capacités de jugement feront toujours la différence.

Pour réduire ce risque et au contraire favoriser une adoption rapide et convaincue, une communication adaptée et une méthode d'implémentation spécifique devront être élaborées : conviction par l'exemple, désignation de référents dans les brigades et commissariats, transparence sur les résultats, système visuel de management de la performance autour des patrouilles et des prédictions (ex. : cartographie de la délinquance, ...), briefings quotidiens, retour et partage d'expériences au sein des patrouilles, association et implication des *data scientists* sur le terrain.

Moderniser les centres de commandement (CIC et CORG)

La modernisation des centres de commandement (CIC pour la police et CORG pour la gendarmerie) constitue un enjeu majeur et l'un des cinq « défis » du plan de modernisation de la sécurité du ministère de l'Intérieur. Un effort significatif a été accompli par la gendarmerie en 2011-2012 avec la mise en place de la base de données de sécurité publique (BDSP)[29]. Pour sa part, la DGPN a considéré cet objectif suffisamment prégnant pour affecter en février 2016 dans ses rangs un commissaire divisionnaire exclusivement chargé du pilotage de ce projet et responsable de la maîtrise d'ouvrage.

Sans évoquer le contenu de ce vaste chantier qui verra le jour à l'horizon 2019, il y a lieu de retenir quelques axes majeurs qui pourront servir de fil conducteur à la rénovation envisagée.

(29) Développée par Thales, la BDSP permet aux gendarmes, depuis les centres de commandement jusqu'aux patrouilles, d'accéder à la synthèse de toutes les informations disponibles en lien avec une mission ou une intervention.

Intégrer les potentialités numériques dans les appels 17

Accompagnant la montée en puissance du téléphone filaire au sein des foyers au début des années 1970, le « 17 police-secours » s'est construit autour de l'appel téléphonique. Depuis une quarantaine d'années, aucune évolution significative n'a marqué ce dispositif qui peut aujourd'hui bénéficier des potentialités offertes par le numérique.

Ainsi, les appels d'urgence largement effectués depuis un téléphone portable pourraient utilement géolocaliser automatiquement les smartphones utilisés. Cela permettrait aux opérateurs chargés d'envoyer des effectifs sur place de connaître immédiatement la position exacte de l'appelant qui, souvent en situation de stress, peut éprouver des difficultés à préciser l'endroit où il se trouve.

De la même façon, les plates-formes de réception des appels 17 doivent pouvoir recevoir de la part des appelants des documents (photographies, vidéos, SMS, MMS, ...) de nature à éclairer les premiers intervenants et, le cas échéant, à être exploités immédiatement par des services d'enquête. Un tel dispositif est déjà en œuvre pour le numéro d'urgence de la SNCF (31 17 par téléphone ou 31 177 par SMS).

Enfin, un SMS pourrait automatiquement être envoyé à l'appelant lorsqu'un véhicule d'intervention est activé pour répondre à sa demande.

Décloisonner les centres de commandement

Le décloisonnement nécessaire des différents centres de commandement au sein du ministère de l'Intérieur (et au-delà) doit se traduire horizontalement aussi bien que verticalement.

Il s'agit d'abord d'améliorer l'interopérabilité des centres, d'une part entre les différents services participant à la gestion des urgences (police, gendarmerie, pompiers, voire SAMU) et d'autre part entre les centres d'une même direction, notamment dans le périmètre de la police nationale. S'agissant de ces derniers, on constate généralement un fonctionnement en « tuyaux d'orgue » qui, s'il permet aux services de travailler normalement dans des configurations habituelles, pose de sérieuses difficultés en situation de crise. Dès lors que les droits auront été ouverts, les CIC voisins pouvant être impactés par les répercussions d'une situation locale doivent bénéficier d'une complète visibilité sur l'événement considéré. De la même façon, la cartographie disponible au niveau d'un CIC doit également intégrer celle des départements limitrophes (interventions sur un secteur « frontalier », poursuites au-delà du département, ...).

Des outils permettant une certaine interopérabilité entre services existent actuellement mais se révèlent insuffisants, surtout lorsqu'il s'agit de gérer une situation complexe ou de grande ampleur. Là encore, par l'adoption de socles techniques communs ou d'interfaces adaptées, policiers, gendarmes et pompiers doivent être en mesure de partager leurs informations tout comme le contenu de leurs interventions. Ces nouvelles possibilités pourraient aller jusqu'à la géolocalisation partagée de tous les intervenants et la communication

réciproque des forces disponibles, y compris les forces militaires du dispositif Sentinelle (données qui ne font aujourd'hui l'objet d'aucun échange sur les applications informatiques).

Le décloisonnement doit également se traduire de manière verticale au sein d'une même direction. Un centre de commandement doit *a minima* disposer d'une visibilité sur l'activité d'un centre voisin de taille plus modeste, afin de l'épauler au besoin, voire de prendre la main (situation de crise). De même, cette visibilité doit être assurée de manière continue jusqu'aux états-majors des directions centrales de la police et de la DGPN (fiches événements, cartographie, géolocalisation, ...) vers lesquels la remontée d'information ne s'opère actuellement que par le truchement de courriers électroniques ou de comptes rendus téléphoniques.

Les mêmes possibilités doivent être ouvertes aux centres de crise des préfectures (cf. C.O.D. : centre opérationnel départemental).

Piloter plus efficacement les événements grâce au numérique

Outre la prise en compte évoquée supra dès la réception des appels 17, l'utilisation des outils numériques est susceptible d'apporter une plus-value importante en matière de gestion des événements et de pilotage des effectifs sur le terrain.

Tirant le meilleur parti de la mobilité à venir (utilisation de smartphones et de tablettes par les policiers et les gendarmes), les centres de commandement doivent être dotés de la possibilité d'envoyer directement aux patrouilles des documents numérisés (fiches réflexes, notices de renseignements, fiches de recherches, instructions diverses, photographies, images issues de la vidéoprotection, ...) susceptibles de compléter les instructions transmises sur les ondes radios. Les expérimentations en cours, en France comme à l'étranger, démontrent clairement que la voix ne constituera plus dans un proche avenir le seul vecteur de transmission de l'information opérationnelle. Des choix techniques doivent donc être effectués rapidement afin d'anticiper les usages du multimédia dans les échanges entre les centres opérationnels et les unités de terrain, rendus possibles notamment par le recours à des terminaux multi-applicatifs de type grand public. Parallèlement, une doctrine de commandement opérationnelle devra accompagner ce mouvement afin de prévenir tout développement anarchique de dispositifs non maîtrisés.

Ces mutations supposent l'aboutissement du remplacement de l'actuel réseau INPT vieillissant par un réseau radio haut débit sécurisé. C'est à cette condition que les services de police et de gendarmerie pourront prendre en compte les nouveaux modes de transmission de l'information, utilisés quotidiennement par la population, et tirer profit des informations essentielles portées par l'image, le son, le texte ou la localisation.

Enfin, même si les opérateurs humains doivent avoir le dernier mot et conserver une capacité d'initiative, on pourrait réfléchir à ce que le *big data*, servi par des algorithmes sophistiqués et des solutions de police prédictive éprouvées,

pourrait apporter en matière d'aide à la décision : affectation des interventions selon la géolocalisation des véhicules, organisation de dispositifs de poursuite ou de nasse, surveillance d'un périmètre spécifique à un instant T, adaptation du cycle de rotation des caméras de vidéosurveillance, ... Un test préalable, aussi complexe soit-il à organiser, sera probablement le meilleur juge de pertinence et d'efficacité.

Intégrer les drones aux capacités des centres de commandement

Qu'il s'agisse de surveiller des convois, la circulation routière, des mouvements de foule ou de participer à des recherches, les hélicoptères apportent déjà un support précieux aux unités au sol comme aux salles de commandement.

Demain, les drones complèteront ce dispositif, aussi bien pour des surveillances de manifestations que pour des opérations d'approche discrète (situations de crise, ...), en extérieur comme en intérieur.

Il convient donc dès maintenant de réfléchir à l'intégration de l'ensemble des moyens aériens dans les capacités opérationnelles des CIC et des CORG : déploiement de flottes, pilotage, accès aux images, ...

Tirer le meilleur parti des murs d'images

Contrairement à la préfecture de police qui a très tôt compris l'intérêt de murs d'images au sein de sa salle de commandement (DOPC) avec la prise en compte de près de 20 000 caméras déployées sur l'espace public, la DGPN et la DGGN ont longtemps cantonné la vidéoprotection dans un rôle de prévention de la délinquance, renvoyant la gestion de ces images aux polices municipales ou aux centres de surveillance urbains (CSU).

L'amélioration rapide de la qualité des vidéos transmises en temps réel et le poids croissant de l'image au sein de l'information ont rendu incontournable la prise en compte de la vidéoprotection comme outil d'aide à la décision au sein des CIC et des CORG. Les évolutions observées récemment dans ce domaine doivent encore être poursuivies et généralisées.

Les centres de commandement doivent ainsi disposer des principales fonctionnalités permettant de prendre la main sur les caméras (direction, zoom, ...). S'agissant de la gestion d'un événement ou d'une intervention, le module cartographique doit être en mesure d'indiquer aux opérateurs la présence de caméras de vidéoprotection implantées à proximité et de les visionner à l'écran. De courtes séquences vidéos doivent pouvoir être enregistrées et jointes à la fiche événement correspondante. Enfin, les centres de commandement doivent être dotés des interfaces nécessaires pour accepter largement l'affichage de vidéos provenant de partenaires institutionnels voire privés (e.g. transporteurs, parcs de stationnement).

Faire pénétrer les réseaux sociaux dans les centres de commandement

Parce qu'ils sont un outil de mobilisation immédiate et qu'ils ont le pouvoir de toucher en temps réel un maximum d'individus, le suivi des réseaux sociaux peut constituer pour les forces de sécurité un atout précieux : détection d'un évènement, évolution d'une manifestation, anticipation des mouvements de foule par l'analyse de la rediffusion des messages, suivi d'une situation de crise (catastrophe naturelle, accident majeur, attentat, ...) et diffusion en retour de messages d'alerte ou de contre-rumeur, ... La brigade des sapeurs-pompiers de Paris l'a mis en pratique dans son centre de commandement voilà plusieurs années déjà.

Retraitées ou reformatées, ces informations pourraient aussi être diffusées aux effectifs engagés sur le terrain pour leur permettre d'adapter leur intervention. Elles pourraient encore venir enrichir les comptes rendus effectués à l'autorité hiérarchique.

Intégrer une telle capacité soulève bien entendu la question des solutions et de l'équipement technologique qui permettront surveillance et réactions en matière de communication. Se posent aussi les questions relatives à l'aménagement ergonomique et à l'organisation du travail dans la salle de commandement : tirer parti au mieux de cette capacité nouvelle exige fluidité et réactivité des échanges entre les opérateurs. Cela exige aussi des équipements pour permettre la présence de personnels spécialement formés (tant aux outils qu'à la communication de crise) et habilités à communiquer en temps réel.

Ouvrir une relation nouvelle avec la population

Renforcer la proximité grâce à de nouveaux services numériques

Pour créer un lien nouveau, profond et durable avec les citoyens, il convient de compléter le travail de communication institutionnel par une véritable palette de services en ligne pour précisément créer une dimension de proximité, d'intimité et de « service ».

Plusieurs options peuvent d'ores et déjà être proposées.

- Elargir le champ de la pré-plainte en ligne.
- Proposer des alertes (par courrier électronique ou SMS) personnalisées en fonction du lieu de résidence, des biens possédés, de critères démographiques voire de géolocalisation.

- Permettre des échanges à vocation informative en ligne (par messagerie instantanée ou par webcam).
- Créer un canal de remontée directe et immédiate d'informations ou de témoignages ouvert à l'ensemble du grand public lors d'une situation de crise (prise d'otages, accident majeur de la circulation, catastrophe naturelle, ...), à l'image du dispositif « Alerte enlèvement ».
- Offrir une assistance aux victimes et aux témoins (pages de présentation des principes et canal de communication dédié).
- Développer l'appel à témoins.
- Mettre en ligne des données publiques sur la criminalité (transparence mais aussi cohérence avec la politique gouvernementale d'ouverture des données).
- Proposer en ligne des contacts personnels au sein des commissariats de quartier (e.g. nom et coordonnées du commissaire central, noms et coordonnées des personnels d'accueil).

Encourager et consolider l'implication citoyenne

Au-delà de ce que pourront apporter les technologies numériques, le renforcement du lien de proximité avec les citoyens passera aussi par leur implication et leur contribution, au travers de tâches adaptées, au travail de la police et de la gendarmerie.

Les réserves, opérationnelles ou civiles, sont une excellente opportunité de donner vie à ce lien, dès lors qu'une gestion et une animation active de ces réseaux est mise en place.

S'appuyant sur la géolocalisation des téléphones mobiles, plusieurs initiatives proposent de développer le volontariat en situation de crise. Des citoyens, préalablement enregistrés, aux compétences validées et qui se trouveraient présents sur le lieu d'un évènement grave, apporteraient leur concours en termes de secours aux victimes, de témoignages et de renseignement donnés aux équipes opérationnelles, ou de renfort dans la sécurisation ou la délimitation d'un périmètre. Ce principe de géolocalisation pourrait d'ailleurs être appliqué aux membres des réserves.

Des initiatives similaires se développent aussi dans la sphère privée, comme par exemple celle de l'application mobile Qwidam. Celle-ci vise à renforcer la sécurité des citoyens, en encourageant la solidarité et l'entraide au quotidien, sur la base de SOS ou d'alertes émises par les utilisateurs de l'application et partagés avec d'autres utilisateurs présents dans un rayon de 500 mètres. Police et gendarmerie peuvent s'interroger sur le rôle qu'elles veulent ou non jouer devant la montée de tels acteurs et le développement de leur offre.

L'implication citoyenne peut encore se construire au travers d'un recours plus fréquent, plus visible et donc mieux assumé aux procédures d'appels à témoins. Encore trop discrètes, les procédures d'appel ne doivent pas se faire uniquement sur internet et peuvent concerner tout type d'affaire et toutes les

géographies. La culture française est certes traditionnellement réticente à tout ce qui s'apparenterait à des appels à la délation, mais les initiatives menées par la *Policia Nacional* espagnole confirment que ces appels à témoignage ont un impact réel et parfois même, ont été un élément indispensable à la conclusion de certaines affaires[30].

(30) Une campagne de lutte contre le trafic de drogue menée sur les réseaux sociaux espagnols en janvier 2012 a permis la réception de 25 000 courriels et a conduit à 850 arrestations. D'autres campagnes ont eu un même succès : lutte contre les violences conjugales, recherche de fugitifs, ...

Enfin, la proximité avec les citoyens pourrait aussi se construire en allant au-devant d'eux et de leurs attentes (organisation régulière de réunions publiques de quartier, de sondages ou d'enquêtes qualitatives, ...), en faisant s'exprimer aussi les policiers et les gendarmes de terrain sous la forme de cercles de qualité. Au début des années 2010, la police de Pittsburgh (Etats-Unis) a ainsi révisé sa stratégie de lutte contre la criminalité à partir d'une enquête auprès de la société civile et au sein de ses propres effectifs. La meilleure compréhension des attentes qui en est résultée a permis d'améliorer la communication et la coopération au sein des services de police, la collaboration avec le grand public et plus généralement, la confiance accordée à l'institution. *In fine*, c'est la lutte contre la criminalité qui a gagné en efficacité.

***

Au terme de nos travaux, nous avons la ferme conviction que les mutations numériques auxquelles doivent se préparer les forces de sécurité françaises n'ont rien d'une course à la technologie. Elles marquent au contraire l'absolue nécessité de remettre l'humain, qu'il s'agisse des citoyens à servir ou des membres des forces de sécurité, au cœur du dispositif et de l'action publique.

Comme l'affirmait Charles de Gaulle dans une conférence de presse du 25 mars 1959, « *En vérité, en notre temps, la seule querelle qui vaille est celle de l'Homme. C'est l'Homme qu'il s'agit de sauver, de faire vivre et de développer* ».

***

ANNEXES

Annexe 1

Sigles utilisés

ANSSI	agence nationale de la sécurité des systèmes d'information
APJ	agent de police judiciaire
BDSP	base de données de sécurité publique (gendarmerie nationale)
BEFTI	brigade d'enquêtes sur les fraudes aux technologies de l'information (Préfecture de Police)
C3N	centre de lutte contre les criminalités numériques (gendarmerie nationale)
CIC	centre d'information et de commandement
CORG	centre opérationnel de renseignement de la gendarmerie (niveau départemental)
CROGEND	centre de renseignement opérationnel de la gendarmerie (niveau national)
CSU	centre de surveillance urbain
DCPJ	direction centrale de la police judiciaire
DGAFP	direction générale de l'administration de la fonction publique
DGGN	direction générale de la gendarmerie nationale
DGPN	direction générale de la police nationale
DGSE	direction générale de la sécurité extérieure
DGS	direction générale de la sécurité intérieure
DGSCGC	direction générale de la sécurité civile et de la gestion des crises
DINSIC	direction interministériel du numérique et des systèmes d'information et de communication
DMIS	délégation ministérielle aux industries de la sécurité
DOPC	direction de l'ordre public et de la circulation (préfecture de police de Paris)
DSIC	direction des systèmes d'information et de communication (ministère de l'Intérieur)
EC3	European cybercrime center (Europol)

GIR	groupe d'intervention régional
ICC	investigateur en cybercriminalité (police nationale)
INPT	infrastructure nationale partagée des transmissions
JIRS	juridiction inter-régionale spécialisée
LAPI	lecteur automatisé des plaques d'immatriculation
LOPPSI	loi d'orientation et de programmation pour la performance de la sécurité intérieure
LRP-GN	logiciel de rédaction des procédures de la gendarmerie nationale
LRP-PN	logiciel de rédaction des procédures de la police nationale
MGMSIC	mission de gouvernance ministérielle des systèmes d'information et de communication
OCLCTIC	office central de lutte contre la criminalité aux technologies de l'information et de la communication ; police nationale)
OPJ	officier de police judiciaire
PHAROS	plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (police nationale)
PTS	police technique et scientifique
RESCOM	messagerie d'autorité de la police nationale
SCRC	service central de renseignement criminel (gendarmerie nationale)
SCRT	service central de renseignement territorial
SDAO	sous-direction de l'anticipation opérationnelle (gendarmerie nationale)
SDIS	service départemental d'incendie et de secours
SDLC	sous-direction de la lutte contre la cybercriminalité (police nationale)
SGMAP	secrétariat général à la modernisation de l'action publique
STAD	système de traitement automatisé de données
ST(SI)²	Service des technologies et des systèmes d'information de la sécurité intérieure

Annexe 2

Experts rencontrés

Mme Vic BAINES, Trust and Safety Manager Europe, Middle-East and Africa, Facebook

Général de division **Simon-Pierre BARADEL,** coordonnateur de la police judiciaire, DGGN

M. Alain BAUER, criminologue, CNAM

M. Willy BRUGGEMAN, président du Conseil fédéral de la police belge

M. Elie BURSZTEIN, responsable anti-fraude et abus, Google

M. Patrick CALVAR, directeur général de la sécurité intérieure, DGSI

M. Matthieu CLOUZEAU, directeur de la prévention et de la protection, mairie de Paris

Vice-Amiral **Arnaud COUSTILLIÈRE,** officier général cyber, ministère de la défense

M. Thierry DELVILLE, délégué aux industries de sécurité, ministère de l'Intérieur

Colonel **Jean-Marc DETRÉ,** chargé de mission, direction des opérations et de l'emploi, DGGN

Colonel **Christophe DUBUIS,** bureau de la formation, DGGN

M. Christophe DURAND, directeur de la cyber stratégie, et son équipe, Interpol

M. Christophe FICHOT, contrôleur général, adjoint au chef du STSI²

M. Eric FILIOL, directeur du laboratoire de virologie informatique et de cryptologie opérationnelle, ESIEA

M. Emile GABRIÉ, chef du service des affaires régaliennes et des collectivités territoriales, CNIL

MM. Alejandro MARTINEZ GARCIA, directeur, et **José Maria Rodriguez,** directeur du développement, Centre 112 de Madrid

M. Benoit GODARD, officier de liaison de l'European cybercrime center (EC3) à Interpol, Europol

Mme Carolina GONZÁLEZ et **M. Enrique SACRISTAN,** chefs de section du bureau de la presse et de l'information, police nationale espagnole

M. Cyril GOUT, commissaire, service central de l'informatique et des traces technologiques, sous-direction de la police technique et scientifique

M. Olivier GRUMELARD, sous-directeur du centre opérationnel de la sécurité des systèmes d'information, et **M. Vincent STRUBEL,** sous-directeur Expertise, ANSSI

M. Joachim KÄLLSHOLM, président, Securitas Sverige AB

Mme Caroline KRYKWINSKI, sous-directrice de l'animation interministérielle des politiques de RH, et son équipe, DGAFP

M. Lionel LE CLEI, vice-président Communication & Sécurité, conseiller « Global Security Activities » du Président, Thales

M. Blaise LECHEVALLIER, commissaire, conseiller technologies, cabinet du DGPN

Colonel **Dominique LUCHEZ** et Lieutenant-Colonel **Bruno MAKARY,** direction des personnels militaires, DGGN

M. Philippe LUTZ, contrôleur général, directeur adjoint des ressources et des compétences de la police nationale

M. Matteo PACCA, directeur associé, McKinsey & Company

Lieutenant-Colonel **Pierre PASSÉ,** bureau du recrutement, des concours et des examens, DGGN

MM. Dominique RENARD et **Cédric MURGIER,** capitaines, OCLCTIC

M. Steve RICHARD, président de l'observatoire national des polices municipales

Mme Sylvie SANCHIS, commissaire, chef de la BEFTI

M. Yaron SAVORAY, Directeur pour l'Europe et le Moyen-Orient du McKinsey Center for Gouvernment et chef de file de la ligne de service Police, McKinsey & Company

Colonel **Jérôme SERVETTAZ,** commandant du service central de renseignement criminel et Colonel **Patrick PERROT,** chef de la division analyse et investigations criminelles, Colonel **Franck MARESCAL,** chef de l'observatoire central des systèmes de transport intelligents, gendarmerie nationale

M. Bernard STIEGLER, philosophe

M. Henri VERDIER, directeur interministériel du numérique et des systèmes d'information et de communication, SGMAP et **Mme Laure LUCCHESI,** directrice adjointe, Etalab

Annexe 3

Bibliographie

Conseil fédéral de la police Belge, « *Une police en réseau : une vision pour la police en 2025* », rapport Willy Bruggeman, juin 2014.

Cour des comptes, « *La gestion des carrières dans la police et la gendarmerie nationales* », Référé n° 71735, 3 février 2015.

Cour des comptes, « *La fonction de police judiciaire dans la police et la gendarmerie nationales* », Référé n°71433, 22 décembre 2014.

INHESJ, « *L'implication des citoyens dans la sécurité intérieure : jusqu'où ?* », Travaux des auditeurs, 2016 (à paraitre).

INHESJ, « *La participation des militaires à la sécurité intérieure* », Travaux des auditeurs, 2016 (à paraitre).

INHESJ, « *Enjeux et difficultés de la lutte contre la cybercriminalité* », Travaux des auditeurs, juillet 2015.

INHESJ, « *Les politiques publiques de vidéo-protection : l'heure des bilans* », Travaux des auditeurs, février 2015.

INHESJ , « *Fichiers de police et libertés : des enjeux nationaux, une nouvelle donne internationale* », travaux des auditeurs, janvier 2015

McKinsey Global Institute "*Disruptive technologies: Advances that will transform life, business, and the global economy*", Rapport McKinsey Global Institute, mai 2013.

Ministère de l'Intérieur, « *Les défis technologiques des forces de sécurité intérieure* », rapport Delville, juin 2014.

PERRY Walter L., McINNIS Brian, C. PRICE Carter, SMITH Susan, HOLLYWOOD John S., "*Predictive policing: the role of crime forecasting in law enforcement operations*", Rand Corporation, 2013.

ÉCOLE MILITAIRE
1 place Joffre
Case 39
75700 PARIS 07 SP
Tél.: 33 (0)1 76 64 89 00
Télécopie : 33(0)1 76 64 89 31