INTERNATIONAL > Défis juridiques et les nouvelles technologies

DROIT > Traçage des personnes et droits fondamentaux

TECHNIQUE > Biométrie et authentification

REVUE de la gendarmerie nationale

REVUE TRIMESTRIELLE / JUILLET 2016 / N° 255 / PRIX 6 EUROS

NOUVELLES TECHNOLOGIES ET SÉCURITÉ

AVEC LA COLLABORATION DU CENTRE DE RECHERCHE DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

retour sur images NUMÉRO 254

© Fotolia / Reborn55

Dans un écosystème numérique global, la protection des données véhiculées par les objets connectés et le Big data est particulièrement sensible. Elle s'intègre dans une stratégie nationale de sécurité tout en s'inscrivant dans un cadre juridique évolutif. Les mesures prises par les autorités françaises permettent de mesurer un type de gouvernance en termes de libertés individuelles, de souveraineté numérique et d'intégration aux flux économiques.

RETROUVEZ UNE RÉFLEXION SUR LES TECHNOLOGIES DE RECONNAISSANCE EN PAGE 102 DE CE NUMERO >>

© Foxstream

« L'homme et sa sécurité

doivent constituer la première préoccupation de toute aventure technologique

Albert Einstein

La miniaturisation des composants, l'instauration de normes internationales, des algorithmiques sophistiquées liant des bases de données favorisent l'éclosion de nouvelles technologies qui peuvent être déployées dans le domaine de la sécurité.

Les marchés mondialisés, soumis à une rude concurrence, obligent à des synergies productives entre pouvoirs publics, organismes de recherche et firmes industrielles pour produire des nouvelles techniques à forte valeur probatoire et pouvant contribuer à une prévention situationnelle. Elles doivent, pour pouvoir être exportables et rentables, s'appuyer sur une fiabilité et un paramétrage transparent pour les opérateurs. En effet, la captation de données biométriques et le relevé des activités personnelles touchent aux qualités substantielles du citoyen. Il convient en conséquence de les encadrer juridiquement afin de proroger la confiance des personnes dans une gouvernance sociale numérique.

SOMMAIRE

NUMÉRO 255

DOSSIER

Nouvelles technologies et sécurité

Fotalia - Zibor

UNE NECESSAIRE COHERENCE ENTRE L'ETAT DE L'ART TECHNOLOGIQUE ET LE DROIT

La sécurité des transactions commerciales, la protection des biens et des personnes nécessitent une forte corrélation, tant au niveau national qu'européen, entre la production du droit et les technologies appliquées aux domaines commerciaux et industriels. Il en va du juste règlement des contrats et des contentieux et de la sécurisation des investissements.

La gestion de la sécurité des biens et des personnes embrasse une approche globale de la sécurité et de la défense qui s'inscrit dans les priorités nationales mais également dans la politique de sécurité et de défense commune (PSDC) de l'Europe. Elle implique une stratégie nationale sur la recherche qui mette en synergie les opérateurs industriels, les organes de recherche et d'enseignement. Cela comprend également la préparation de l'encadrement juridique des solutions mises en œuvre. Cette stratégie repose également sur le drainage de fonds européens sur la sécurité qui nécessite une connaissance aboutie du formalisme de ces programmes et de leur approche multipartenariale.

Dans ce cadre, la préservation des libertés individuelles passe par une libre circulation de données protégées par une architecture juridique, un codage encadré des informations et ce dès la conception des processus (*privacy by design*).

Les défis juridiques posés
par l'émergence des nouvelles technologies

par ANNE CAMMILLERI

« Lorsqu'il se présente à la culture scientifique, l'esprit n'est jamais jeune. Il est même très vieux, car il a l'âge de ses préjugés. Accéder à la science (…) c'est accepter une mutation brusque qui contredise le passé »[1]**. Toute création technologique passe nécessairement chez le chercheur par un moment de doute car l'esprit scientifique qui ne doute pas confond alors la connaissance (l'épistémè) et l'opinion (la doxa). Au doute s'ajoute le facteur temps. Ce dernier définit à quel moment la technologie est obsolète, sa durée de vie. La technologie permet souvent l'instantanéité de l'information. Par nature, l'arrivée d'une nouvelle technologie, source de progrès, peut remettre en cause l'autorité du droit, tant au moment de l'élaboration de la norme qu'à celui de son application.**

ANNE CAMMILLERI

Professeure des Universités en droit public.

(1) Bachelard, *La formation de l'esprit scientifique*, ed. J.Vrin, 1938.

(2) *Crédibilité scientifique et droit*, Toulouse 3 décembre 2010, colloque CNES, ed. 2012 A. Cammilleri, conclusions du colloque, *De la doxa à l'épistémè*, Université Aix Marseille CERIC, publication CNES, centres de compétence technique ed. 2012.

Lors d'un colloque sur la crédibilité scientifique et le droit l'une des questions posées était celle de savoir si la crédibilité scientifique passait nécessairement par le mariage parfait entre la preuve scientifique et la preuve juridique[2]. L'une des réponses apportée consistait à retenir que pour que le droit accompagne le progrès, ce dernier doit être évident. Il faut se référer à la notion “d'évidence rationnelle” de Spinoza : est évident ce qui s'impose par sa clarté. Mais il convient d'émettre deux réserves : d'une part, si le droit doit accompagner le progrès, il faut néanmoins que les mentalités soient prêtes ; d'autre part, historiquement, lorsque la technologie nouvelle est mise au service du fanatisme,

Fotalia - Argus

Une posture qui permet une interopérabilité des moyens et une détection des menaces dans un cadre légal.

il faut en réfuter l'utilisation. La nécessaire conformité de l'utilisation d'une nouvelle technologie à la loi peut se rapprocher de l'évidence rationnelle de Spinoza que, si et seulement si, la preuve est faite qu'elle est au service des standards juridiques universels, tels que le noyau dur des droits fondamentaux issus des principaux textes européens et internationaux. Le juriste se repère dans l'ordonnancement juridique par la hiérarchie des normes. Le droit accompagnera sans difficulté le progrès technologique, dès lors que ce dernier sera au service du juste, appréhendé dans sa dimension morale. Aujourd'hui, dans le cadre très particulier de l'état d'urgence décrété par le Président de la République et prorogé par le Parlement jusqu'au 26 mai 2016, après avis favorable du Conseil d'État du 2 février 2016[3], les technologies sont au cœur de notre approche conceptuelle nationale de la protection du citoyen au regard de l'usage qui en est fait par les services régaliens. L'utilisation des technologies s'appuie actuellement dans ce contexte particulier sur des évolutions nationales (I) et européennes majeures (II).

(3) Loi n°2016-162 du 19 février 2016 prorogeant l'application de la loi n°55-385 du 3 avril 1955 sur l'état d'urgence ; avis du Conseil d'Etat, Assemblée générale, section de l'intérieur du 2 février 2016 sur le projet de loi prorogeant l'application de la loi n°55-385 relative l'état d'urgence, JO 20 février 2016.

Au niveau national

L'électrochoc des attentats du 13 novembre 2015 et la mise en œuvre des mesures de l'état d'urgence engendrent une prise de conscience de la nécessité d'une approche globale des questions de sécurité et de défense en

droit. Les résultats obtenus par les fonctionnaires compétents de tous les services de l'État concernés s'appuient indéniablement aussi aujourd'hui sur la qualité des technologies mises à leur disposition, pour des missions de nature variable et spécifique. Ce constat est valable tant au niveau opérationnel qu'au niveau scientifique.

Au niveau opérationnel, l'opération SENTINELLE, qualifiée par le ministre de la Défense "d'événement majeur dans l'histoire de notre pays" dans le rapport remis au Parlement le 10 mars 2016[4] sur le recours à la force militaire sur le territoire national, plaide "pour une approche globale de la sécurité et de la défense" dans les quatre espaces terrestre, maritime, aérien et le cyberespace. Les technologies qui sont au cœur de ces missions doivent permettre une "posture" que le ministre veut "permanente" , de "sauvegarde" maritime, de "sûreté" aérienne et de "protection" terrestre[5]. Elles doivent susciter des contremesures nucléaires, radiologiques, biologiques et chimiques. Elles sont au service des missions de surveillance en continu, de détection des quatre espaces, de planification ou encore d'évacuation. L'emprise des technologies est constante sur la lutte contre le terrorisme et le crime organisé, la défense des intérêts économiques et des accès aux ressources stratégiques, la sauvegarde maritime, la sûreté aérienne, la sécurité civile dans la lutte contre les sinistres et les catastrophes naturelles ou technologiques.

(4) Rapport au Parlement du ministre de la défense, 10 mars 2016 sur les conditions d'emploi des armées lorsqu'elles interviennent sur le territoire national pour protéger la population.

(5) P.26 et 28 du rapport pré cité

Dès lors, leur efficacité face au progrès scientifique doit être constamment évaluée, au regard de leur modernité tant en matière de sécurité que de défense. C'est en ce sens qu'il faut comprendre le constat ministériel de la nécessité “de renforcer les capacités" spécifiques de surveillance et de détection terrestres, maritimes et aériennes (imagerie, interception, localisation brouillage), ou encore “l'autonomie logistique et l'interopérabilité” des moyens de communication et de planification[6] encadrée par la loi du 28 juillet 2015 sur la programmation militaire[7]. En matière de défense, le retour d'expérience sur l'opération SERVAL avait permis de montrer la puissance de l'interopérabilité réussie des forces.[8]

(6) P. 43 du rapport Sentinelle pré cité

(7) Loi n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense JORF du 29 juillet 2016: https://www.legifrance.gouv.fr/Droit-francais/Selection-du-JORF/2015/Juillet.

(8) Opération SERVAL, le retour de la manœuvre aéroterrestre dans la profondeur. Quels facteurs de succès, quels défis à relever pour demain? Réflexions tactiques, n°spécial du Centre de doctrine d'emploi des forces, 2014.

Aux niveaux scientifique et académique, la recherche française est également pro active. Les chercheurs français, toutes disciplines confondues, ne sont pas en reste sur les moyens d'assurer une

meilleure protection des personnes. L'Agence nationale de la recherche (ANR) promeut la recherche en sécurité dans le cadre d'un plan d'action et d'un appel à projets spécifique au sein du défi[9] "Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents", conforme à la Stratégie Nationale sur la recherche, publiée par le ministère de l'Enseignement Supérieur et de la Recherche. Afin de répondre aux besoins technologiques sont associés à la rédaction de cet appel à projets des représentants des principaux ministères dont, par exemple, la gendarmerie.

(9) Comité de la *Filière industrielle de sécurité* (CoFIS) fort de l'association de grands groupes et d'un tissu dense et extrêmement dynamique d'ETI et de PME.

Dans ce cadre, l'ANR a organisé les 10 et 11 février 2016, un workshop interdisciplinaire sur la sécurité globale (le WISG). Cet événement annuel a été organisé en association avec le Secrétariat général de la Défense et de la Sécurité Nationale, la Direction Générale de l'Armement du ministère de la Défense et la Direction générale des entreprises du ministère de l'Économie, de l'Industrie et du Numérique. Il a été l'occasion de montrer le rôle crucial des nouvelles technologies dans le cadre de la sécurité globale. Cet événement national a réuni les acteurs de la sécurité tant régaliens que privés, notamment les industriels regroupés dans la filière du CoFIS9 et les chercheurs du monde académique. Les contributions des chercheurs sur la gestion des risques (méthodologie de l'aide à la décision, détection, localisation et décontamination, gestion des risques naturels) , sur l'ouverture européenne de la recherche en sécurité , sur les nouveaux outils technologiques de lutte contre des menaces multiformes en robotique et optronique, sur la cybersécurité (en phase avec le Forum international de la Cybersécurité) et les premiers résultats de la recherche sur la lutte contre les drones malveillants ont été présentés et publiés[10]. L'irruption de nouvelles technologies est bien au cœur de la recherche en France. En revanche les taux de succès des projets français dans le cadre du programme européen sur la sécurité H2020 sont plus décevants avec un taux de succès de la France pour l'appel européen 2015 à peine supérieur à 8%, derrière l'Espagne, l'Italie (supérieur à 14%), l'Allemagne et le Royaume -Uni (supérieur à 12%)[11].

(10) L'essentiel des contributions des chercheurs du workshop interdisciplinaire sur la sécurité globale (le WISG 2016) est en ligne sur le site de l'ANR : http://www.wisg.fr/programme.html

(11) Voir le site dédié : http://www.horizon2020.gouv.fr/cid73310/la-france-espace-europeen-recherche.html

Au niveau académique, l'articulation de la recherche et de l'enseignement sur les nouvelles technologies en matière de sécurité et de défense doit aussi être approfondie et généralisée. Les premières expériences initiées par le ministre de la Défense, en Bretagne, avec le Pôle

d'Excellence Cyber en sont un exemple. Sciences Po Rennes est l'un des participants[12] à cette aventure en expérimentant une offre de formation de niveau master en sécurité et défense ouverte à des ingénieurs en cybersécurité, en partenariat avec l'Université de Bretagne Sud.

(12) Comité de la *Filière industrielle de sécurité* (CoFIS) fort de l'association de grands groupes et d'un tissu dense et extrêmement dynamique d'ETI et de PME.

Cette offre de formation permet aux élèves d'apprendre à travailler dans un domaine où l'interdisciplinarité est forte. Elle s'appuie sur de nombreux partenariats régionaux dont celui avec la région de gendarmerie de Bretagne, initié en 2011 avec le général de corps d'armée Alain Giorgis, renouvelé depuis lors. La réforme de la mastérisation en cours renforcera également la poursuite possible en thèse de cette formation. La méthode du recours à des partenariats ciblés consolide l'approche globale de la sécurité et de la défense appliquée aux nouvelles technologies.

Au niveau européen

Le renforcement de l'approche globale de la Politique de sécurité et de défense commune (PSDC) est une réalité "de terrain" des principales opérations extérieures[13]. Le contexte politique est historique et unique: le ministre de la Défense a invoqué, sur la base de la déclaration de l'état d'urgence, pour la première fois dans l'histoire de l'Union européenne, le recours à l'article 42§7 du traité sur l'Union européenne permettant à un État qui serait l'objet d'une agression armée sur son territoire de demander aide et assistance par tous les moyens en leur pouvoirs aux autres États membres. Cette demande inédite intervient à un moment clé d'un renforcement juridique des règles européennes relatives au renforcement de la protection des droits fondamentaux applicables aux nouvelles technologies. Elles concernent, notamment, les nouvelles règles d'identification électronique et l'accord politique conclu le 28 janvier 2016 (enfin!) sur le règlement européen sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des ces données.

(13) Pour plus d'information voir notamment : https://www.telecom-bretagne.eu/recherche/reseaux_et_laboratoires/pole-d-excellence-cyber/

Sur l'identification électronique, le droit européen est une source forte de l'encadrement de l'usage des nouvelles technologies avec un règlement spécifique qui sera applicable le 1er juillet 2016[14]. Concernant les services de confiance, M. Pr. Bertrand Warusfeld, en soulignait très justement, dans le numéro précédent de cette même revue, la montée en puissance de l'ANSSI[15]. Mme Claire

(14) Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE : JOUE L 257/73 du 28 août 2014.

(15) Revue n° 254 P. 109

(16) Claire Levallois-Bart, "Les enjeux de 'l'identité numérique" revue de la Gendarmerie N° 248/2013 et Cahier n° 1 "Identités numériques" coordonné par Claire Levallois-Barth, Chaire Valeurs et Politiques des informations personnelles, mars 2016 téléchargeable très bientôt sur : www.informations-personnelles.org.

(17) Cette revue n° 254 P. 36.

Levallois-Barth, coordinatrice de la Chaire de recherches de l'Institut Mines-Télécom Valeurs et politiques des informations personnelles en a publié un mode d'emploi téléchargeable[16] très utile .

En discussion depuis le 25 janvier 2012, après des atermoiements interminables, un accord politique était enfin conclu le 28 janvier 2016 sur le règlement du Parlement et du Conseil sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des ces données (règlement général sur la protection des données). Dans cette revue, le général d''armée (2S) Wattin-Augouard soulignait que la donnée est désormais « *une donnée cible privilégiée des prédateurs* » pour en conclure de l'urgence d'une "divulgation maîtrisée[17]. C'est de cette divulgation maitrisée qu'il s'agit en faveur des données à caractère personnel ! Les technologies y sont abordées de manière progressiste « *devant faciliter la libre circulation des données au sein de l'Union européenne et leur transfert vers des pays tiers et des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel* » (§6).

En contrepartie de cette liberté, le choix de l'outil juridique qu'est le règlement devrait permettre une uniformisation de la protection des données à caractère personnel, au sein de l'Union européenne et se substituera à la directive européenne historique n° 95/46. Ce nouveau texte constitue une petite révolution en faveur de la protection des données à caractère personnel, en raison des contraintes qu'il impose à tous les acteurs utilisant des nouvelles technologies, pour le traitement de données à caractère personnel. On souligne, de manière non exhaustive, le principe de conformité qui s'imposera au responsable du traitement qui devra apporter la preuve de l'adoption de règles internes et de l'application de mesures qui respectent en particulier le principe de la protection des données dès la conception (*privacy by design*) et de la protection des données par défaut. Cette obligation se traduira notamment par la réduction au minimum du traitement des données à caractère personnel, leur pseudonomisation si possible et la transparence des fonctions et traitements des données (§61 du texte). Le *privacy by design* a vocation à s'étendre aux fabricants de produits et aux prestataires de service qui traitent de ces données, afin de les inciter à les intégrer dès la conception, et pourra même être pris en considération dans le cadre des marchés

publics[18]. Cette règle s'applique également au responsable de traitement de données, qui envisage un traitement de ces dernières avec un pays tiers, dont le niveau de protection n'est pas jugé comme étant adéquat. Il devra prendre, tout comme les sous-traitants, les garanties nécessaire pour le respect de la protection des données à caractère personnel.

(18) Pour une illustration de la première application en France du principe de privacy by design appliquée à l'imagerie active voir: Anne Cammilleri, Rémy Prouvèze, Isabell Büschel, Nouvelles technologies et défis juridiques en Europe - L'imagerie active au service de la sécurité globale, Bruylant, 2012, 260 p.

L'AUTEUR

Anne Cammilleri, professeure des Universités en droit public est actuellement en poste à Sciences po Rennes et à IODE-UMR CNRS 6262, où elle co-dirige avec le général Philippe Boone le Grade de Master Sécurité Défense et Intelligence Stratégique ; Elle est également en délégation auprès de l'Agence Nationale de la Recherche, où elle est coresponsable scientifique du défi 9 «Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents».

Dernières publications en lien avec le sujet

. un ouvrage : Anne Cammilleri, Rémy Prouvèze, Isabell Büschel, Nouvelles technologies et défis juridiques en Europe - L'imagerie active au service de la sécurité globale, Bruylant, 2012, 260p.

- un article : «Cybersécurité et cyberdéfense européenne... What else ?», Mélanges en l'honneur du François Hervouët, Entre Ordres Juridiques, LGDJ, 2015 Lextenso Editions n°70, Presses juridiques de Poitiers pp 31-5.

LE CONTINUUM SÉCURITAIRE OU L'OBLIGATION D'ACTIONS CONCERTÉES

L'interdépendance entre les domaines économiques et sociaux, la mondialisation des processus commerciaux et la libre circulation des personnes obligent à une approche globalisée de la sécurité européenne et nationale. Cette vision implique une collaboration franche, d'un niveau européen, entre les agences, qu'elles ressortent des sphères civile, militaire ou policière dans l'optique d'un décloisonnement des compétences.

L'émergence d'un monde numérique cautionne une sécurité adossée à un fort volet technologique qui puisse circonscrire les menaces polymorphes qui pourraient affecter les services essentiels des États. Dans ce cadre, les projets européens doivent favoriser des transferts de technologies et dotations, d'équipements et des formations intégrées au profit d'États de l'Union qui n'ont pas les moyens de les promouvoir. Ils doivent également faciliter la construction de programmes à forte valeur ajoutée qui permettent d'imposer des solutions rentables sur la scène mondiale (surveillance des frontières, transparence des mouvements financiers, protection des données, automatisation des processus urbains, *etc.*) qui assurent à l'Europe une primauté industrielle, sociétale et idéologique par rapport aux modèles asiatiques et nord-américains.

C'est l'enjeu de la préservation de nos sociétés démocratiques basées sur le libre-échange des personnes et des biens dans le respect des droits fondamentaux.

Continuum sécuritaire
et technologies au niveau européen

par **PIERRE BERTHELET**

Continuum sécuritaire et sécurité globale entretiennent des relations étroites. L'un et l'autre entendent dépasser les segmentations sectorielles pour apporter une réponse efficace à des menaces qui affectent les États et l'Union en tant que telle. L'esprit de la sécurité globale se matérialise par un ensemble d'actions sous la forme de subventions de l'Union dans divers domaines. Ses efforts s'orientent particulièrement vers une sécurité de nature technologique.

PIERRE BERTHELET
Chargé de cours à Sciences Po Lille
Chercheur au Centre de Documentation et de Recherches Européennes

La logique de la sécurité globale qui préside à l'action européenne permet de surmonter les réflexes sectoriels et cette logique tend à se retrouver dans le déploiement des fonds financiers européens. Concrètement, l'Union favorise, grâce aux subventions apportées, une démarche horizontale, concernant des domaines multiples, défense, police, douane, sécurité civile, tout en ayant une approche transverse, notamment en s'efforçant de multiplier les synergies entre acteurs issus d'horizons divers impliquant des États membres différents. Cette approche transcende les clivages existants en orientant les efforts autour de projets technologiques.

Sécurité globale et continuum sécuritaire : le sens des mots

Le continuum sécuritaire est un concept destiné à relier entre eux les différents secteurs de la sécurité ainsi que leurs menaces respectives : sécurité intérieure, extérieure, informatique, énergétique, environnementale, *etc*.[1] Il est étroitement imbriqué à un autre représentation : la sécurité globale[2].

Les dispositifs technologiques européens ont pu concrétiser une assistance maritime aux migrants victimes de passeurs relevant de la criminalité organisée.

La sécurité globale remonte à plusieurs décennies, même si elle trouve ses lettres de noblesse du fait des mutations que connaît le monde dans la deuxième moitié du XXe siècle. La sécurité s'élargit à de nombreuses sphères : protection sociale, environnement, travail, nucléaire, *etc.* Ces domaines sont reliés entre eux du fait des interdépendances croissantes en matière économique et sociétale. Aussi, s'il est possible d'avoir une approche sectorielle de la sécurité, il s'agit avant tout d'un effet de loupe afin de cerner un domaine particulier dans un ensemble plus vaste au sein duquel tous les éléments sont imbriqués.

Sur le plan de la menace, le continuum sécuritaire est une formule à double sens. D'un côté, il s'agit de rendre compte du phénomène de brouillage des repères, notamment l'effacement des frontières, avec pour corollaire une plus grande indistinction des menaces. Celles-ci, de nature polymorphe, sont en effet décrites comme se déplaçant et s'adaptant aisément. D'un autre côté, il faut faire état d'une mutation de la sécurité. Le continuum sécuritaire est étroitement lié à la sécurité globale, réponse à la métamorphose d'un contexte géopolitique, qui est autant un discours descriptif que mobilisateur. Il est question

(1) Sur le continuum sécuritaire, voir Watin-Augouard, M. « Le continuum », Armée d'aujourd'hui, n° 171, juin 1992, p. 32-35. Et plus récemment « Le continuum défense-sécurité intérieure », in Debove F., Renaudie O. (dir.), Sécurité intérieure. Les nouveaux défis, Paris, Vuibert, 2013.

(2) Voir notre ouvrage Chaos international et sécurité globale : la sécurité en débats, Paris, Éditions Publibook Université (EPU), 2014.

de dépeindre une mutation de la sécurité, mais aussi de l'appeler : sur le plan de la réponse abordée, la sécurité globale correspond à une manière de réagir de façon conjointe et coordonnée, chaque participant étant invité à œuvrer de concert avec les autres pour organiser une réaction collective efficace[3].

(3) Pour une analyse approfondie, voir Roche, J.-J., « Sécurité et défense globales. Des mutations en cours, un débat embryonnaire », Cahiers de la sécurité, n° 14, octobre-décembre 2010, p. 16-19 ; Coste, F., « L'adoption du concept de sécurité nationale : une révolution conceptuelle qui peine à s'exprimer », Note de la Fondation pour la recherche stratégique (FRS), n° 3, Paris, FRS, Série recherches et documents, 2011.

Les stratégies européennes en matière de sécurité sous le sceau de la sécurité globale

La logique de sécurité globale se retrouve également dans l'Union européenne. En effet, la Stratégie européenne de sécurité[4] décrit l'environnement et liste les défis majeurs. Il s'agit d'un document, directeur dans ce domaine, visant à orienter l'action politique et militaire de l'Union et de ses États membres sur la base d'une série de menaces identifiées : le terrorisme, la criminalité transnationale organisée et la cybercriminalité notamment[5].

(4) La stratégie européenne de sécurité est un document rédigé sous l'autorité du Haut représentant de l'UE pour la PESC, Javier Solana, et adoptée par le Conseil européen les 12 et 13 décembre 2003 à Bruxelles. http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV%3Ar00004

(5) Voir notre article : « La stratégie européenne de sécurité intérieure: un défi pour la gendarmerie », Revue de la Gendarmerie nationale, n° 235, juin 2010, p. 30-35.

Sa version, renouvelée pour la période 2015-2020, confirme cette vision selon laquelle « *la sécurité intérieure et la sécurité extérieure de l'Union européenne sont de plus en plus liées* ». Il importe de renforcer une action globale au niveau européen qui doit requérir une intervention impliquant les acteurs d'horizons divers, qu'ils soient publics ou privés, qu'ils soient rattachés à l'échelon national, infranational ou européen. Surtout, il importe que cette action soit décloisonnée[6].

(6) Voir notre article co-écrit avec le Colonel Gérin : « Où va la sécurité intérieure européenne ? », Revue de la Gendarmerie nationale, n° 250, septembre 2014, p. 6-13.

Il s'agit de mobiliser tant l'Union que ses États dans les efforts menés pour lutter contre des menaces qui s'adaptent à un environnement mouvant. La stratégie européenne en matière de cybersécurité en donne d'ailleurs un aperçu pour ce qui est des cybermenaces. Cette stratégie, adoptée en 2013, part d'un constat, à savoir le caractère polymorphe et hautement nocif des menaces. Elle note qu'« *au cours des dernières années, on a constaté que le monde numérique, s'il procure d'énormes avantages, est aussi très vulnérable. Les incidents de cybersécurité, d'origine malveillante ou accidentelle, se multiplient à un rythme inquiétant et pourraient perturber la fourniture de services essentiels que nous tenons pour acquis comme l'eau, les soins de santé, l'électricité ou les services mobiles. Les menaces peuvent avoir des origines diverses, notamment des attaques criminelles, à caractère politique, terroristes ou commanditées par un État, ainsi que des catastrophes naturelles et erreurs involontaires* ». C'est la raison

pour laquelle elle préconise un meilleur partage d'informations entre les autorités publiques nationales et le secteur privé, ainsi qu'une meilleure collaboration entre les agences, qu'elles viennent du monde civil (l'ENISA), du monde policier (Europol et notamment son unité EC3) ou du monde militaire (l'Agence européenne de défense - AED).

La stratégie européenne en matière de cybersécurité a donc une vision horizontale de la sécurité en adoptant une conception combinant la sécurité intérieure, la défense et la sécurité privée. Cette vision horizontale se retrouve dans des documents autres que des documents directeurs, notamment les textes européens instituant les fonds financiers. Ils préconisent des solutions technologiques face à des menaces, qu'il soit question de terrorisme, des flux migratoires, des trafics criminels et des catastrophes naturelles ou d'origine humaine. La protection des frontières extérieures de l'Union européenne en est une illustration.

Le soutien financier européen au projet maritime français SPATIONAV

La gestion des frontières extérieures européennes est une illustration de l'implication européenne dans des projets de sécurité et de défense destinés à renforcer les frontières à partir de technologies innovantes en collaboration avec le secteur privé. Instauré pour la période 2007-2013, le Fonds européen pour les frontières extérieures s'inscrit dans une logique de concrétisation d'un système européen commun de gestion intégrée des frontières. Pour rappel, ce projet, créé après les attentats de septembre 2001 de New York, vise à renforcer les frontières extérieures de l'Union. Une attention toute particulière est apportée aux frontières électroniques (smart borders). À cet égard, le Fonds a aidé les États membres à mettre en place ce système allant jusqu'à 92,82 % de l'investissement total pour certains États membres. Il a surtout servi à mettre sur pied le système européen Eurosur[7]. Dans ce cadre, 168 millions d'euros ont été mobilisés, soit près d'un tiers des ressources du fonds, pour la concrétisation de ce projet, en appuyant notamment la poursuite du déploiement de réseaux de radar français : SPATIONAV. Fondé sur un dispositif de surveillance maritime mutualisant les équipements de la marine nationale, de la douane et des Centres régionaux opérationnels de surveillance et de sauvetage en mer (CROSS), ce dispositif consiste en un déploiement (installations ou rénovations) de vigies et de sémaphores.

(7) Eurosur est destiné à assurer la surveillance aux frontières terrestres et maritimes de l'espace Schengen. L'objectif est de lutter contre l'immigration clandestine et les trafics illégaux, en particulier au large des côtes européennes. Suite au drame de Lampedusa, Eurosur a également une mission de sauvetage des migrants en perdition. Concrètement, ce dispositif, géré par l'agence européenne Frontex, consiste en une interconnexion des systèmes radar nationaux, un mécanisme d'échange d'informations entre les autorités nationales, l'objectif étant d'avoir un panorama aussi précis que possible de la situation en temps réel aux frontières, à partir d'informations fiables et constamment actualisées.

Les dispositifs technologiques européens ont pu concrétiser une assistance

maritime aux migrants victimes de passeurs relevant de la criminalité organisée

L'argent européen versé a permis l'achat d'équipements notamment des radars à haute fréquence, des drones, des véhicules terrestres sans pilote, des satellites géostationnaires ou encore des détecteurs. Ces éléments font partie d'une liste des éléments constitutifs d'Eurosur, allant d'une plate-forme d'échange d'informations à l'emploi de navires, en passant par des systèmes d'exploitation d'imagerie satellitaire ou d'outils d'analyses de risque.

À l'heure actuelle, le développement de SPATIONAV s'opère dans le cadre du Fonds de sécurité intérieure (FSI). D'après un rapport d'information publié par le Sénat, en février 2016, la France bénéficie d'un soutien de 177 millions d'euros au titre du FSI (soit 107 millions d'euros pour le volet frontières et visas, et 70 millions d'euros pour celui consacré à la police). Plusieurs projets ont été mis en place dans un tel contexte, en particulier ce projet SPATIONAV.

La recherche orientée vers les innovations technologiques au nom du continuum sécuritaire

Un registre varié d'investissements sur des contenus à forte valeur technologique

Dans un autre registre, le Fonds pour les frontières extérieures subventionne des projets variés à fort contenu technologique. Il a permis de financer l'équipement de certains États membres en matériel de surveillance, en particulier des moyens de transport (voitures, motos, hélicoptères, avions ou encore bateaux). Il les a aidés à acquérir du matériel opérationnel, tel que du matériel de vidéosurveillance par hélicoptère ou de traitement d'images satellite et des systèmes de camouflage ou de détection nocturne. Le Fonds a soutenu le déploiement d'équipements relatifs aux procédures de contrôle automatisé, tels que les portails électroniques. C'est le cas en France du développement du « SAS PARAFES », qui consiste à faciliter le passage des voyageurs munis de passeports biométriques.

Il a contribué, d'après un rapport sur l'évaluation du Fonds pour les frontières extérieures, à financer des formations ayant trait au pilotage d'engins de surveillance et à leur maintenance, à la lutte contre la fraude documentaire et à l'analyse de risque en matière migratoire.

Les programmes Horizon2020 entrent dans cette logique

Toujours en matière de gestion des frontières, les actions du programme Horizon 2020 complètent les actions réalisées par Frontex dans le domaine de la recherche et du développement, comme Dognose et All Eyes menés au début des années 2010. Le projet Dognose est destiné à améliorer l'action des garde-frontières concernant le contrôle des documents de voyage et l'évaluation du niveau de risque.

Le projet All Eyes est un projet visant à identifier les meilleures technologies en matière de surveillance des frontières. Faisant écho au projet Eurosur déjà en place, All Eyes englobe diverses technologies allant des capteurs à distance aux drones en passant par les véhicules terrestres sans pilote ou des aéronefs équipés de capteurs multi-renseignements. Les actions du programme Horizon 2020 ne se cantonnent pas à la sécurisation des frontières extérieures de l'Union. Entré en vigueur le 1er janvier 2014, ce programme est doté d'une enveloppe globale de plus 77 milliards d'euros. Une partie du programme, crédité de 1,695 milliard, est destiné à assurer la sécurité et prend la relève du septième programme-cadre pour la recherche (FP7)[8].

(8) le FP7 est un outil destiné à répondre aux besoins de l'Europe en matière d'emploi et de compétitivité ainsi qu'à la maintenir à la première place dans l'économie mondiale de la connaissance. Ces fonds sont dépensés sous forme de subventions accordées aux acteurs de la recherche, pour cofinancer des projets de recherche, de développement technologique et de démonstration. Les subventions sont accordées sur la base d'appels à propositions et d'une procédure d'examen par les pairs.

Horizon 2020 inclut les entreprises privées au nom d'une co-production de la sécurité dans une logique de sécurité globale. Il vise à renforcer la compétitivité et la position de l'Union européenne sur le plan international dans les domaines de la recherche, de l'innovation et des technologies, et à prendre en compte les préoccupations des citoyens au travers de réponses données à des défis sociétaux d'envergure. En matière policière, le programme entend mettre au point des équipements et des canaux de communication dans le contexte d'opérations menées par les services de police.

Dans le domaine de lutte anti-terroriste, le programme vise à déterminer et à analyser les principaux facteurs constitutifs d'un processus de radicalisation violente. Il entend se focaliser sur la détection de menaces internes à des infrastructures critiques, le but étant d'identifier des membres du personnel susceptibles de se livrer à des actions de sabotage.

Pour ce qui est de la protection civile, le programme vise à mettre au point des techniques de détection et de tri de personnes exposées à des substances NRBC[9]. Le but est de déterminer rapidement le nombre de personnes exposées et leur niveau d'exposition.

(9) NRBC : nucléaire, radiologique, biologique et chimique.

En matière de coopération douanière, le programme entend promouvoir des technologies destinées à contrôler rapidement de grands volumes de fret. Il s'agit en particulier de faire usage de procédés fondés sur la propriété atomique, en particulier pour détecter des menaces au sein de cargaisons denses, et de faire usage de procédés fondés sur l'évaporation.

Par ailleurs, le programme se donne pour objectif , parmi les mesures prévues en matière de gestion de l'ordre public, de modifier les tactiques de maintien de

l'ordre basées jusque-là sur le confinement et la dispersion par la force. Il propose de financer des outils technologiques permettant aux services de police d'identifier avec précision les éléments perturbateurs d'une foule agressive et de les extraire rapidement tout en opérant une intrusion minimale au sein de cette foule.

Au final, l'Union s'est largement investie dans le champ de la sécurité afin de mieux faire face à des menaces interconnectées. La vulgate politique et journalistique oppose les États à l'Union (dépeinte de manière caricaturale comme un « monstre technocratique » impotent, étouffant les États nations). Pourtant, la réalité est bien éloignée d'un tel cliché. L'Europe de la sécurité s'élabore avec le consentement des États, conscients que l'interconnexion des menaces appelle des solutions qui dépassent le cadre national. D'abord, les États sont les artisans de l'édification de cette Europe de la sécurité. Ensuite et surtout, ils sont les bénéficiaires des projets menés au plan européen, la France par exemple pour ce qui est du financement du programme SPATIONAV.

L'AUTEUR

Pierre Berthelet est un ancien conseiller ministériel auprès du Ministre de la Justice (Belgique). Enseignant à l'Institut d'Études politique de Lille, Chercheur au Centre de Documentation et de Recherches Européennes (CDRE), il est spécialisé sur les questions de sécurité intérieure européenne. Il anime le site securiteinterieure.fr.

Il est l'auteur de plusieurs études pour la Gendarmerie nationale (CREOGN) ainsi que de publications diverses :
. Paysage européen de la sécurité intérieure, New York, Oxford, Zurich, Vienne, PIE-Peter Lang, 2009, 573 p.
. Le droit institutionnel de la sécurité intérieure européenne, préambule de Pat Cox (Président du Parlement européen), Avant-propos de Jorge Hernandez-Mollar (Président de la Commission des Libertés publiques du Parlement européen), Préface de Gilles de Kerchove d'Ousselghem (Directeur à la Direction générale « Justice et affaires intérieures » du Conseil de l'Union), Postface d'Henri Labayle (Professeur des Facultés de droit), New York, Oxford, Zurich, Vienne, PIE-PeterLang, 2003, ISBN 978-90-5201-193-6 (324 pages)
. Le droit institutionnel de la coopération policière et judiciaire, Préface de Gilles de Kerchove d'Ousselghem (Directeur à la D.G.H. du Conseil de l'Union), Reviews de Souheil El-Zein (Directeur juridique d'Interpol) et de Constance Chevallier-Govers (Maître de conférences à Paris XII), Grenoble, Editions des Vignes, 2001, ISBN 2-914371-007-1 (191 pages)

Ouvrages collectifs

. « La sécurité intérieure européenne est-elle un invertébré juridique ? », in Mbongo, P., Latour, X. (dir.), Actes du Colloque « Sécurité, Libertés, Légistique. Autour du code de la sécurité intérieure » organisé à Poitiers le 15 mai 2012.
. « Europe's Internal Security and the Gendarmeries » (pp. 119-137), in Gendarmeries and the Security Challenges of the 21st Century, Dutch FIEP Presidency 2010 Seminar Project, FIEP Seminar Publication, Royal Marechaussee, 2011, ISBN :978-90-817734-0-9
. « L'Europe de la sécurité va-t-elle se construire ? » (p. 297–311), in En quête de sécurité. Causes de la délinquance et nouvelles réponses, sous la direction de Sebastian Roché, Paris, Armand Colin, 2003, 343 pages, ISBN-13 : 978-2200262839
. « Les attentats du 11 septembre ont-ils été une bonne ou une mauvaise chose pour la construction du troisième pilier ? », Actes du colloque du Centre d'Etudes sur la Sécurité Internationale et le Coopérations Européennes (CESICE) des 5, 6, et 7 décembre 2002), Grenoble, CESICE, 2003

DOSSIER

NOUVELLES TECHNOLOGIES ET SÉCURITÉ

Technologies de sécurité
et industrie : une filière pour aller plus loin

par THIERRY DELVILLE

La sécurité est souvent associée à l'idée d'un important marché de main-d'œuvre. Ceci est effectivement le cas tant d'un point de vue historique pour la sécurité publique que la sécurité privée. L'analyse des budgets de la gendarmerie nationale comme de la police nationale traduit cette prédominance avec un rapport qui s'établit selon les années entre +/-90% de budget pour la masse salariale et +/-10% pour le fonctionnement.. D'une certaine manière, ce rapport montre que les Français se sentent plus rassurés sous le regard des policiers et gendarmes que dans l'objectif d'une caméra !

THIERRY DELVILLE
Délégué ministériel aux industries de sécurité

Dans ce contexte il apparaît assez rapidement de nombreuses différences entre la sécurité et la défense, que ce soit du côté des donneurs d'ordre ou des fournisseurs. Le marché de la sécurité est un marché atomisé avec l'apparition régulière de nouveaux acteurs. Celui de la défense tourne autour d'une structure organisée de longue date avec un donneur d'ordre incontournable, le ministère de la défense et notamment la DGA. La défense a organisé un monopsone[1] permettant de disposer d'un acheteur unique très qualifié et un quasi-monopole de fait par grand secteur.

(1) Un monopsone est un marché sur lequel un seul demandeur se trouve face à un grand nombre d'offreurs.

La modernisation des forces de l'ordre repose sur des efforts d'organisation mais également sur l'introduction d'outils technologiques qui progressivement irriguent l'essentiel des activités et des spécialités. Une illustration en est le développement de la police technique et scientifique avec l'émergence à la fin des

années 2000 du concept de PTS de masse. Les techniques criminalistiques sortent de l'apanage de quelques experts de laboratoire vers l'ensemble des services. L'informatisation des grands fichiers a permis de mettre à disposition de tous les enquêteurs une ressource scientifique autrefois cantonnée.

La complexité galopante des infrastructures technologiques, le foisonnement des données, les cycles courts d'évolution nécessitent un dialogue nourri et permanent entre les acteurs opérationnels et le monde de l'industrie et de la recherche, d'autant plus que le délai d'appréhension durable d'un outil par les services de sécurité est notablement plus important que le temps nécessaire aux délinquants pour se l'approprier. Pour gagner du temps, les services doivent encore et toujours être plus efficaces et le rapprochement avec le monde industriel constitue une voie jusqu'à maintenant peu exploitée.

La création du conseil de la filière industrielle de sécurité

À l'occasion du dernier livre blanc pour la défense et la sécurité publié début 2013, le constat a été dressé que : « *Les conditions propices à l'industrialisation à plus grande échelle de solutions innovantes de sécurité, accessibles au juste coût et compétitives sur les marchés exports doivent être créées. En conséquence, une politique interministérielle visant à organiser une filière industrielle de la sécurité sera mise en place. Elle sera pilotée par un comité de filière, qui associera les principales parties prenantes au développement des technologies et du marché dans ce domaine.* »

Le conseil de la filière industrielle de sécurité (COFIS) a été installé par le Premier ministre le 23 octobre 2013. Il réunit les opérateurs de sécurité, les industriels du secteur constitués en Conseil des industries de la confiance et de la sécurité (CICS), le monde académique, les pouvoirs publics et des personnalités qualifiées comme la présidente de la commission nationale informatique et libertés.

Pour représenter le ministère de l'intérieur, par un décret en date du 28 février 2014, la délégation ministérielle aux industries de sécurité a été créée. Elle traduit un véritable changement dans la relation instaurée entre le ministère de l'Intérieur et les acteurs industriels du marché de la sécurité. Cette nouvelle délégation permet d'établir un lien entre les besoins opérationnels et les capacités industrielles.

La cartographie de la filière industrielle

Dans le cadre des travaux du COFIS, le SGDSN[2], la DGE du ministère de l'économie[3] et le ministère de l'Intérieur représenté par la délégation, ont lancé au second semestre 2014 une étude de

cartographie du marché et des acteurs de la filière française de sécurité, et notamment le volet industriel.

Elle s'inscrit dans les travaux du Pôle interministériel de prospective et d'anticipation des mutations économiques (PIPAME) de la DGE qui réalise des rapports sur l'évolution des principaux acteurs et secteurs économiques en mutation, en s'attachant à faire ressortir les menaces et les opportunités pour les entreprises, l'emploi et les territoires.

Les résultats de l'étude sortie fin juin 2015 ont permis de constater que le budget généré par cette filière en France était six fois plus important que prévu lors de son lancement fin 2013 : 58,9 milliards d'euros et 955.177 salariés. Inclut dans ces chiffres, le seul secteur marchand, s'élevant à 29,9 milliards d'euros et 302 142 emplois, comprend le secteur industriel avec 20,9 milliards d'euros de chiffre d'affaires et 125.222 emplois. Ce dernier secteur a généré un chiffre d'affaires de plus de 7 milliards à l'exportation.

La filière de la sécurité connaît une activité en constante progression depuis 2003, même si les services privés de sécurité ont connu un ralentissement de 2008 à 2013. Les secteurs les plus dynamiques restent ceux de l'électronique et des systèmes et de la cybersécurité. Les perspectives pour 2020 montrent que la croissance sera tirée par la cyber, avec un taux annuel de 10 %, et les produits électroniques, à 6 % (avec l'internet des objets à 18 %). L'ensemble de la filière croîtra de 5,1 % en rythme annuel moyen.

Les axes d'action du COFIS

Les axes d'action de la délégation s'articulent autour de plusieurs groupes de travail. Ils regroupent tous des représentants des différents partenaires du COFIS. Il s'agit des représentants des utilisateurs publics (police, gendarmerie, douanes, sapeurs-pompiers, administration pénitentiaire, collectivités locales,…) et privés (opérateurs, transporteurs,…), des mondes industriels (grands groupes et PME) et académiques (universités, organismes de recherche, pôles de compétitivité) et également des organismes régulateurs comme la CNIL.

Les différents groupes de travail visent à développer une offre industrielle performante et innovante en phase avec

(2) Secrétariat général de la défense et de la sécurité nationale. Ses missions intéressent l'ensemble des questions stratégiques de défense et de sécurité, qu'il s'agisse de la programmation militaire, de la politique de dissuasion, de la programmation de sécurité intérieure concourant à la sécurité nationale, de la sécurité économique et énergétique, de la lutte contre le terrorisme ou de la planification des réponses aux crises.

(3) La Direction Générale des Entreprises (DGE) a été créée par décret le 16 septembre 2014. Placée sous l'autorité du ministre de l'Économie, de l'Industrie et du Numérique, la DGE a pour mission de développer la compétitivité et la croissance des entreprises de l'industrie et des services. Ceci passe par le développement des nouveaux secteurs, notamment dans les services aux entreprises et à la personne, par le soutien et la diffusion de l'innovation et l'anticipation et l'accompagnement des mutations économiques, dans un objectif de croissance durable et d'emploi.

le besoin, compétitive vis-à-vis du marché international et respectueuse des contraintes juridiques, éthiques et sociétales qui fondent nos sociétés démocratiques.

Pour la période 2013-2014, sept axes de travail ont permis de mieux connaître la filière, de créer les relations de confiance entre acteurs, de lancer des initiatives à l'export ou de mettre en place les premiers démonstrateurs (cybersécurité des systèmes industriels, radio du futur et vidéo intelligente). Un des résultats importants est l'étude qui a cartographié la filière industrielle avec ses 125.000 emplois et 21 milliards d'euros de chiffre d'affaires, soit l'une des filières industrielles françaises les plus importantes. Mais l'essentiel réside aussi dans l'indicible, c'est-à-dire dans la relation de confiance, dans le dialogue qui s'est instauré entre les acteurs : l'administration échangeant sur les besoins futurs avec l'industrie, la CNIL évaluant les technologies les plus novatrices, les industriels et l'État allant de concert dans les démarches export.

Pour la période 2015-2017, quatre axes de travail visent à fédérer et valoriser tous les acteurs de la filière en particulier les PME et les acteurs locaux, à développer une offre innovante et adaptée, à développer la base industrielle de sécurité et à accéder au marché national et export. Après une phase de connaissance de la filière et de prise de conscience de son existence et de son importance, il s'agit maintenant de la développer alors que la concurrence mondiale est exacerbée.

Les technologies au cœur de la transformation du rapport à la sécurité

Après les attentats de janvier 2015, la délégation a proposé à la commission du Concours mondial de l'innovation (CMI) d'ajouter un volet sécurité. En lien avec le CMI, le COFIS et le Ministère de l'enseignement supérieur, la délégation a assuré une large information sur cette initiative ce qui a assuré un succès en termes de propositions reçues (3e domaine souscrit après la santé et le numérique).

Dans le domaine des achats innovants, en lien avec la DEPAFI[4], la délégation a assuré une première rencontre entre acheteurs du ministère et des entreprises de la région lyonnaise dont de nombreuses PME du cluster EDEN[5]. Cette rencontre a permis au ministère de préciser ses futurs besoins et les

(4) La direction de l'évaluation de la performance, des affaires financières et immobilières est une direction de pilotage, d'expertise et de service. Responsable déléguée de la fonction financière ministérielle (RFFiM), elle prépare, négocie et suit l'exécution du budget du ministère et assure une prestation de service, d'expertise et de conseil en matière budgétaire et comptable.

(5) EDEN, Cluster de sûreté et de sécurité, a été fondée en 2008 par six hommes d'affaires de Rhône-Alpes. En 2011, EDEN est devenu une Fédération nationale combinant quatre associations régionales : Rhône-Alpes, Bretagne, Bourgogne et Provence-Alpes-Côte d'Azur (PACA).

procédures d'acquisition utilisées, mais aussi de présenter son action en termes de soutien à l'export.

La délégation assure le suivi et la plupart du temps, dans les faits, impulse et coordonne les activités sur les démonstrateurs lesquels visent à développer une synergie entre les centres de recherche, les industriels, les services de l'État et des collectivités en matière de sécurité et de sûreté. Ces démonstrateurs concernent le Big Data, la PMR (radio sécurisée), la Sûreté aéroportuaire, les « Smart and safe cities », la Vidéoprotection intelligente, pour ne citer que ces thèmes. Cette activité permet la rencontre entre les utilisateurs publics et privés, la coordination du suivi des groupes de travail, l'analyse des projets, la coordination avec le groupe des financeurs et l'information du cabinet du ministre.

L'importance de démontrer : l'exemple du démonstrateur « VOIE »

Notre société est marquée par la révolution de l'image. Le domaine de la sécurité n'échappe pas à cette tendance avec la multiplication des capteurs et avec la diffusion généralisée des images.

Pour développer de nouvelles solutions d'exploitation en temps réel ou en temps différé de grands volumes d'images, un démonstrateur baptisé « VOIE » regroupe deux groupes industriels et une dizaine de PME autour de quatre cas d'usage.

Le premier, porté par la Préfecture de police, consiste à mettre en place des outils d'interopérabilité en temps réel entre les systèmes de vidéo protection afin de permettre, par exemple, à une salle de commandement de prendre la main sur le réseau de caméras d'un partenaire de l'État comme un centre commercial.

Deux autres cas d'usage permettront de mieux tirer profit des systèmes de vidéo dans les systèmes de transport pour anticiper les actes malveillants, criminels ou terroristes. La SNCF et la RATP animent chacune un démonstrateur dans leur environnement spécifique.

Enfin, dernier cas d'usage, la police judiciaire regroupe autour d'elle des services d'investigation pour développer des logiciels, « analytics » , de traitement vidéo.

Tous ces outils permettront de valoriser les images et donc de valoriser les investissements importants concédés par les « vidéosurveilleurs » dans un cadre juridique et éthique clairement défini.

La sécurité est plus que jamais au cœur des préoccupations individuelles et collectives. Le développement d'une société de plus en plus digitale fait apparaître de nouvelles menaces et transforme également la nature et le périmètre de la réponse apportée. Cette course en avant impose aux acteurs privés et publics de la sécurité de s'organiser pour mieux réfléchir aux besoins futurs et les anticiper. Dans ce cadre le rôle de l'État agissant comme prescripteur mais aussi régulateur de l'offre de sécurité est plus déterminant que jamais.

L'AUTEUR

Avant d'occuper ses fonctions à la DMIS, Thierry Delville a alterné des postes à dominante techniques (télécommunications et informatique) avec des postes opérationnels. Directeur des services techniques et logistiques de la Préfecture de Police de Paris (DOSTL) (2009 – 2014) - Chef du Service des Technologies de la Sécurité Intérieure (2005 – 2008) - Adjoint puis Chef du bureau des systèmes d'informations et des télécommunications à la direction centrale de la Sécurité Publique (DCSP) (1998 – 2005) - Chef de la Circonscription de Sécurité Publique de BONDY (93) (1996 1998) - Chef de la Circonscription de Sécurité Publique de BEZONS (95) (1994 – 1996) - Elève commissaire puis stagiaire à l'ENSP de St Cyr au Mont d'Or (69) (1992 – 1994) - Chef de l'unité informatique au service des voyages officiels et de la sécurité des hautes personnalités (SVOSHP) (1989 – 1992) - Analyste programmeur à la direction des transmissions et de l'informatique (DTI) au Ministère de l'Intérieur. Chargé des projets micro informatiques au BAMIB (bureau des applications micro informatiques et bureautiques) (1987 – 1989)

Le management de l'innovation ou comment relier innovation participative et innovation institutionnelle

par **FRANÇOIS BRÉMAND**

L'innovation apparaît aujourd'hui comme le remède miracle à bien des difficultés rencontrées par les entreprises, les administrations ou la société. La gendarmerie n'échappe pas à cette mode mais elle a su imaginer et construire, en une dizaine d'années, un véritable écosystème de l'innovation. Arrivé aujourd'hui à maturité, il permet d'envisager sereinement sa valorisation.

L'innovation ne se décrète pas

FRANÇOIS BRÉMAND

Colonel de Gendarmerie
Bureau de la qualité et de l'appui à la performance
Mission du pilotage et de la performance
Direction générale de la gendarmerie nationale

Remède miracle, l'innovation au sens large est déclinée en de multiples concepts : technologique, sociale, de rupture, spontanée, provoquée, participative, collaborative, et même... frugale que l'on apparente souvent à de l'innovation *low cost*. Hélas, elle ne se trouve pas en pharmacie et encore moins sur l'étagère d'une officine de consultant, pour la simple et bonne raison qu'elle ne se décrète pas. Un dirigeant peut taper du poing sur la table ou se démener, rien ne se passe si ses personnels n'ont pas d'idées ou du moins peu ou pas innovantes ! Pourquoi ? Parce que l'innovation n'est pas seulement un résultat, c'est d'abord « *un processus qui se déroule depuis la naissance d'une idée jusqu'à sa matérialisation* »[1]. Il convient donc de construire le meilleur processus pour faire naître les idées, susciter l'innovation puis créer les conditions favorables à son développement, l'accompagner, la tutorer et enfin matérialisée, la faire connaître, reconnaître et la diffuser. Simple à présenter, la mise en œuvre de

(1) Définition du Larousse

Une WebApp, développée par l'adjudant Olivier Favre PGHM du Versoud (38), qui sauve des vies par une géolocalisation de victimes par leur téléphone

ce processus est compliquée dans une organisation géographiquement éclatée et très hiérarchisée comme la gendarmerie. En effet, notre institution est marquée par une empreinte hiérarchique forte et par un dispositif territorial d'environ 4 000 emprises. Dans ces conditions, vouloir mettre en place un dispositif de management de l'innovation du jour au lendemain peut s'avérer illusoire.

Une construction méthodique

L'innovation peut être divisée en deux grandes catégories : l'innovation institutionnelle et l'innovation participative.

L'innovation institutionnelle se décide en haut lieu, elle s'inscrit dans une démarche "top down" (du haut vers le bas), et s'impose aux échelons inférieurs. Elle est généralement cantonnée à des bureaux d'étude et conduite à partir du siège de l'entreprise avec des chefs de projets.

L'innovation participative se décide sur le terrain, elle s'inscrit dans une démarche "bottom up" (du bas vers le haut), et se propose aux échelons supérieurs. C'est « *une démarche de management structurée qui vise à stimuler et à favoriser l'émission, la mise en oeuvre et la diffusion d'idées par l'ensemble du personnel en vue de créer de la valeur ajoutée et de faire progresser l'organisation* »[2].

(2) Définition donnée par l'association "Innov'acteurs"

Une énergie renouvelable

Cachée, diffuse, l'innovation participative existe partout, tout le temps et elle est parfois bien plus puissante que l'innovation institutionnelle. Il est donc impératif de pouvoir créer les conditions favorables à son émergence. Il faut

souvent détecter les innovations dans les structures les plus reculées des cantons le plus excentrés, puis extraire ces innovations et les acheminer au siège de l'organisation. Il est enfin nécessaire de les analyser, les raffiner, avant de les distribuer à d'autres structures qui en trouveront l'utilité.

En un sens, l'innovation participative est une énergie renouvelable si les conditions de son existence sont régulièrement entretenues. Les cadres de contact ont, à cet égard, un rôle essentiel. Ils doivent savoir créer les conditions favorables à l'émergence des innovations, adapter à leur bénéfice celles qui proviennent d'autres territoires et détecter les personnels innovants.

L'enjeu pour le management de l'innovation est de prendre en compte les deux grandes composantes de l'innovation et d'établir des passerelles entre elles, l'innovation participative nourrissant l'innovation institutionnelle et cette dernière pouvant orienter l'innovation participative à son profit.

L'enjeu étant clairement fixé, la DGGN a donc construit méthodiquement, en une dizaine d'années, un écosystème harmonieux de pilotage de l'innovation.

10 % d'innovation institutionnelle

L'innovation institutionnelle a toujours été peu développée en gendarmerie, cette dernière n'ayant pas vocation à être un centre de recherches. Elle a souvent reposé sur les capacités d'entités spécialisées comme le pôle judiciaire de la gendarmerie nationale et notamment l'Institut de recheches criminelles, le groupe d'intervention de la gendarmerie nationale[3], le service des technologies et des systèmes d'information de la sécurité intérieure, ou le centre de recherche de l'EOGN...

(3) Deux ingénieurs de l'armement servent aujourd'hui au sein du service recherche et développement du GIGN

Jusqu'en 2013, cette innovation institutionnelle n'était pas optimisée et canalisée. L'arrivée, auprès du directeur général d'un conseiller scientifique, issu de la direction générale de l'armement, et de deux chargés de missions "prospective et préparation de l'avenir" au sein du cabinet, ainsi que la création du comité de pilotage ART (Anticipation Recherche Technologie) ont permis de mieux orienter les projets institutionnels et de se placer comme force de proposition au sein du ministère de l'Intérieur, que ce soit sur des projets comme l'analyse prédictive conduite par le service central de renseignement criminel, la création de l'observatoire central des systèmes de transport intelligents, ou encore le projet de gendarme connecté NEOgend... La force du comité de pilotage ART réside également dans la prise en compte des innovations issues de l'innovation participative et leur éventuelle intégration dans l'innovation institutionnelle, ce qui constitue une première passerelle entre les deux formes d'innovations.

90% d'innovation participative

L'essentiel de l'innovation en gendarmerie, plus de 90 %, repose sur l'innovation participative avec un dispositif solide et cohérent mais qui n'est pas encore utilisé à plein régime. Pourtant, ce qui semble aujourd'hui une évidence a été difficile à mettre en œuvre et il reste encore ça et là quelques résistances. En provenance directe du terrain, conçue par des hommes et des femmes dont l'innovation est d'abord une passion en plus de leur métier de gendarme, l'innovation participative doit se frayer un chemin entre les réticences au changement, le manque de temps, l'engagement intense au service de nos concitoyens, les freins hiérarchiques, réels ou supposés, les contraintes financières, le manque d'audace, la peur de l'échec...

Une innovation participative à deux faces

L'innovation participative peut être déclinée en deux branches : l'innovation participative provoquée et l'innovation participative spontanée.

Encore peu développée en gendarmerie, l'innovation participative provoquée consiste pour le commandement qui se trouve face à un problème précis, à solliciter l'ensemble du personnel sous son autorité afin de recueillir des solutions. La gendarmerie a expérimenté ce dispositif en 2015, en lançant conjointement avec le ministère de la défense, un défi participatif "Drone", dont le thème était "vos idées face aux drones malveillants". Ce défi a permis de recueillir, au sein de l'Institution, 150 idées en deux mois et d'identifier des personnels particulièrement qualifiés, en mesure de composer un futur vivier de télépilotes.

Fer de lance du management de l'innovation en gendarmerie, l'innovation participative spontanée est celle qui s'est le plus développée depuis une dizaine d'années. Dans ce type d'innovation, le commandement ne demande rien et, d'initiative, des personnels de terrain imaginent de nouveaux outils, de nouvelles applications, de nouveaux processus, de nouveaux modes d'action...souvent pour résoudre leurs problèmes du quotidien, pour faire disparaître des irritants, pour combler les lacunes de matériels parfois inadaptés ou mal conçus.

Ce dispositif est aujourd'hui composé de trois briques qui prennent en compte les idées élaborées, les bonnes pratiques et les idées brutes.

La prise en compte des idées élaborées remonte à 1988, avec le soutien de la mission pour le développement de l'innovation participative de la défense (MIP). Malgré son rattachement au ministère de l'Intérieur, la gendarmerie

(4) Annexe 33 de la délégation de gestion cadre entre le MINDEF et le MININT

Sirpa-gendarmerie

La gendarmerie a remporté le premier prix du secteur « service public » au Podium de la Relation Client BearingPoint – TNS Sofres 6 – 9 février 2016.

bénéficie toujours de ce précieux soutien[4] qui permet de financer les innovations de ses personnels jusqu'à 90 000 euros et d'apporter un soutien en matière de propriété intellectuelle, via le bureau de la propriété intellectuelle de la DGA.

Les Ateliers de Performance, fleuron de l'innovation participative

La prise en compte des bonnes pratiques remonte à 2007 et à la création des ateliers de performance (ADP). Ils permettent de recueillir des bonnes pratiques et non simplement des idées. Elles doivent avoir été mises en oeuvre localement et le bénéfice doit en être mesuré sur un périmètre et une période. Le succès des ateliers de performance repose sur trois facteurs :

la simplicité du dispositif, tout personnel (gendarme, militaire du corps de soutien, civil) pouvant faire remonter une bonne pratique à la DGGN/MPP (mission du pilotage et de la performance) via une fiche de performance dématérialisée, sans avis hiérarchique ;

la confiance accordée aux concepteurs, qui ont le droit à l'erreur ;

la liberté laissée aux bénéficiaires : les unités restent libres de mettre en oeuvre les bonnes pratiques retenues dans le répertoire annuel des ateliers de perfomance.

Après 10 ans d'existence, 550 bonnes pratiques et leur documentation sont actuellement disponibles sur le Wik'innovation de la gendarmerie[5]; 20 % des bonnes pratiques annuelles sont reprises en central, notamment dans le cadre de la Feuille de route (FdR) de la gendarmerie ; 20 bonnes pratiques par an sont reprises par un tiers des régions et le retour sur "investissement créatif" est estimé entre un et trois millions d'euros par an pour un coût de 20 000 euros et 1 ETP. Les potentialités des ADP sont loin d'être épuisées puisqu'après dix ans d'existence, seulement 1 % des personnels y a participé.

(5) Conçue à l'été 2014, le wik'innovation est la plate-forme collaborative de l'innovation en gendarmerie

En 2012, le comité de suivi des ateliers de performance a vu le jour afin d'inciter les directions de la DGGN à étudier plus précisément l'impact de certaines bonnes pratiques, en vue de leur éventuelle généralisation. Piloté par le bureau de la qualité et de l'appui à la performance, ce comité est composé des deux chargés de missions "prospective et préparation de l'avenir" du cabinet et des référents "feuille de route" des directions et services. Après le comité de pilotage ART, le comité de suivi des ADP constitue la seconde passerelle entre l'innovation institutionnelle et l'innovation participative.

Enfin, à compter de juin 2013, la mise en œuvre de la Hotline feuille de route (FdR) a permis de prendre en compte les idées brutes en provenance du terrain. Ces propositions sont analysées dans les directions puis transmises au cabinet pour éventuellement nourrir la Feuille de route (FdR) de la gendarmerie. Depuis 2013, cela a été le cas pour chaque phase de la FdR.

Quelle reconnaissance ?

Pour créer un climat propice à la naissance de l'innovation, à sa captation, à son analyse puis à sa diffusion, la gendarmerie nationale a donc construit, brique après brique, un écosystème global de management de l'innovation, en concentrant ses efforts sur l'innovation participative. Pionnière dans ce domaine au sein de la sphère publique, la gendarmerie a été récompensée dès 2009 par le prix de la modernisation de l'Etat avec la démarche des ateliers de performance, reconnue en interministériel comme à l'étranger. Elle est aujourd'hui récompensée à travers tous les prix reçus par ces innovateurs à l'extérieur de l'Arme : prix IntériEurékâ jusqu'en 2012, prix de l'Audace remis par la fondation Leclerc de Hautecloque, prix de de la résilience sociétale (HCFDC), prix Bearing Point TNS Sofres de la relation client, reçu en 2016, sur le thème de la simplification...

En marge de ces prix, La DGGN tient particulièrement à la reconnaissance des innovateurs. Elle se traduit par des témoignages de satisfaction, des lettres de félicitations et des présentations[6], par des récompenses pécuniaires, mais surtout par la participation régulière des innovateurs à la mise en œuvre de leurs innovations généralisées par l'administration centrale.

(6) Comme celle qui s'est tenue le 23 mars 2016, à l'hotel de Beauvau où une dizaine d'innovations gendarmerie issues du terrain ont été présentées au ministre de l'Intérieur.

Dans l'esprit de la Feuille de route, l'organisation du management de l'innovation en gendarmerie vise aujourd'hui à décharger le gendarme innovateur d'un maximum de contraintes que ce soit en termes de remontée des innovations, de propriété intellectuelle, de valorisation... La DGGN est désormais au service de ces innovateurs afin de les accompagner au mieux dans la réalisation de leur projet. C'est pourquoi deux

circulaires internes récentes, sur l'innovation en gendarmerie[7] et sur la protection et la valorisation des innovations[8], sont venues encadrer ces nouvelles pratiques.

Les fondations du management de l'innovation étant désormais solides et stabilisées, la gendarmerie peut dorénavant s'engager sur deux voies d'avenir, le partenariat avec des centres de recherche ou des écoles d'ingénieurs et la commercialisation de ses meilleures innovations.

(7) Circulaire n°88 000 GEND/MPP du 12 octobre 2015 relative à l'innovation en gendarmerie.

(8) Circulaire n°4 000 GEND/DSF/SDAF/BADM du 17 décembre 2015 relative à la protection et à la valorisation des inventions en gendarmerie.

(9) L'ONERA est le centre de la recherche aéronautique, spatiale et de défense.

(10) Ecole nationale supérieure de techniques avancées.

(11) Ecole internationale des sciences du traitement de l'information.

Des partenariats innovants

En 2014, la DGGN a signé une convention de partenariat avec l'ONERA[9] et elle devrait très prochainement signer une convention avec l'ENSTA ParisTech – université Paris Saclay[10]. Les échanges avec les écoles d'ingénieurs se sont déjà traduits concrètement par la réalisation des applications smartphone grand public "stop cambriolage" avec Epitech Montpellier ou Vigicambri 64 avec l'EISTI[11] de PAU.

Cette coopération avec les écoles d'ingénieurs peut également prendre des formes originales comme l'organisation prochaine d'un hackathon au siège de la DGGN en avril 2016. Co-organisé par la MPP, le STSI[2] et l'APIE[12], cet hackathon réunira sept écoles d'ingénieurs (Epitech Montpellier, Nantes, Nice, Ecole 42, EPITA, EISTI Pau et ENSTA ParisTech) et visera à développer, à partir de l'application Gendloc[13], des solutions techniques afin de mieux interagir avec une personne en détresse à partir de son smartphone, à mieux appréhender son environnement à partir des smartphones qui l'entourent et enfin à faciliter la collecte d'informations de masse utiles aux interventions en cas de situation exceptionnelle (attentats, catastrophe...).

(12) Agence du patrimoine immatériel de l'Etat

(13) Conçue par l'adjudant Olivier Favre du PGHM de Le Versoud (38), Gendloc est une web app permettant de géolocaliser précisément une personne égarée à l'aide de son smartphone, sans l'installation préalable d'une application

(14) Sous-direction administrative et financière/Bureau administration

La commercialisation des meilleures innovations

Chaque année, deux à trois innovations issues de l'innovation participative sont brevetées par la gendarmerie. En 2014, à l'initiative du conseiller scientifique du DGGN, et avec l'appui de la MPP et de la SDAF/BADM[14], la gendarmerie s'est engagée dans la commercialisation de ses meilleures innovations. Cette démarche a été initiée en 2014, suite au dépôt du brevet d'ADN rapide conçu par le chef d'escadron Sylvain Hubac de l'IRCGN. Cette démarche de commercialisation a été élargie en juin

2015 avec le dépôt de la marque "gendarmerie nationale" et prochainement le dépôt de marques filles "GIGN", "Garde républicaine", "IRCGN", "PGHM" et "FAG", afin de pouvoir commercialiser des licences de marque, à partir d'innovation gendarmerie. L'objectif est d'obtenir des retours sur "investissements créatifs", afin de pouvoir financer de nouvelles innovations issues de l'innovation participative ou de l'innovation institutionnelle.

Dans le même esprit, des contacts ont été établis en 2016 avec la SATT Lutech[15] afin de lui confier la valorisation d'innovations issues de l'institution.

(15) Accélérateur de transfert de technologies, SATT lutech est une des 14 sociétés créées par le programme d'investissement d'avenir et spécialisées dans la maturation et la commercialisation d'innovations issues de la recherche

De la détection des innovations jusqu'à leur commercialisation, la gendarmerie a mis en place un management total de l'innovation comme on parle de management total de la qualité. Elle est désormais solidement armée pour récolter les fruits de son engagement stratégique dans ce domaine.

L'AUTEUR

Colonel de gendarmerie, François Brémand sert, depuis 2010, à la mission du pilotage et de la performance, où il est chargé de l'innovation participative, de la qualité et du suivi de la feuille de route. St cyrien (promotion Maréchal Lannes), il a servi en gendarmerie mobile (EGM Nantes), en école (EOGN), en gendarmerie départementale (compagnie de Ploermel) et au bureau de la sécurité publique de la DGGN. Il prendra, au 1er août 2016, le commandement de la gendarmerie de l'Oise.

Pourquoi la gendarmerie mise-t-elle sur les réseaux sociaux ?

par SUZANNE FERRET et FRÉDÉRIC ALLAMAND

« Conquérir » les réseaux sociaux permet à la gendarmerie de disposer de vecteurs de communication modernes s'affranchissant des médias, dans une vraie démarche de proximité numérique avec la population. L'Institution peut ainsi « produire ou coproduire de la sécurité » en fonction des événements, notamment en cas de crise, auprès d'un public "connecté" grandissant. Mieux, les publications atteignent une audience beaucoup plus large que celle des abonnés grâce au principe de "viralité" des réseaux sociaux, renforcé par leur perméabilité avec les médias traditionnels et l'essor des NTIC[1].

SUZANNE FERRET

Chef de la section des publications électroniques SIRPA – Gendarmerie

FRÉDÉRIC ALLAMAND

Chef de la section des médias sociaux Sirpa-Gendarmerie Community manager de la gendarmerie

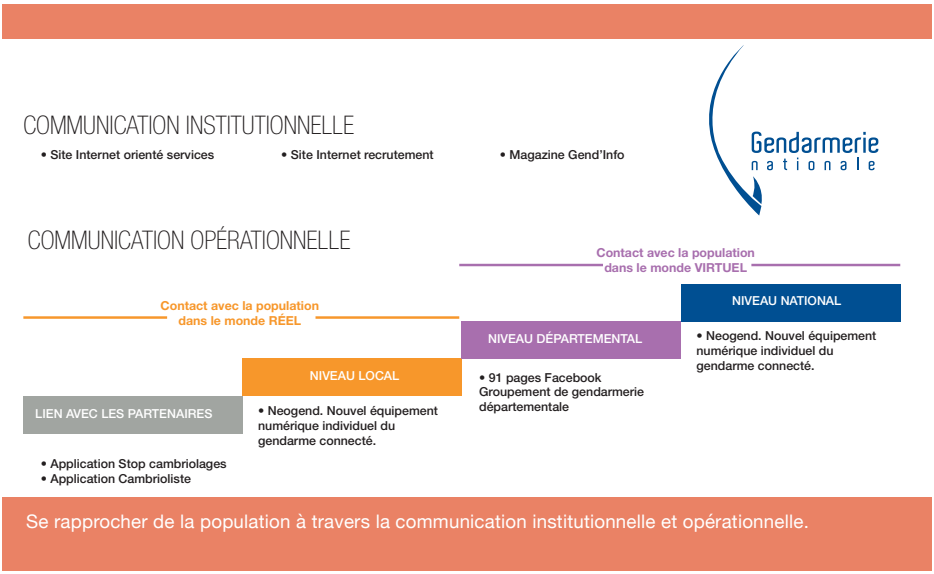
(1) Nouvelles technologies de l'information et de la communication : ensemble des techniques utilisées pour le traitement et la transmission des informations (câbles, téléphone, Internet, etc.) Larousse.

(2) Les Tweetos sont les utilisateurs de Twitter.

Avec 5 millions de Tweetos[2] en France et 25 millions de Français sur Facebook, le monde de l'information et de la communication a basculé dans l'ère des Réseaux sociaux (RS), devenus incontournables à bien des égards.

Consciente des changements induits par cette révolution numérique, la gendarmerie nationale a très vite compris l'importance d'inclure ces RS dans sa stratégie globale de communication. Mais à quel dessein ?

L'institution n'amorce pas un « virage numérique » à compter de 2010 pour céder à un effet de mode ou seulement



Se rapprocher de la population à travers la communication institutionnelle et opérationnelle.

faire moderne. L'ambition affichée est de créer une nouvelle proximité numérique avec la population en diffusant de l'information utile et concrète, qui « produit » de la sécurité.

Cumulant aujourd'hui plus d'1,2 million d'abonnés sur Facebook et Twitter[3], la gendarmerie dispose d'un dense maillage territorial virtuel qui reçoit, partage et diffuse à son tour jusqu'au cœur des territoires, dans le réel, les messages qu'elle publie. Comme le souligne le général d'armée Denis Favier : « *Avec le numérique, nous avons développé une nouvelle logique de proximité, celle d'une gendarmerie en phase avec son temps* ». Cette révolution numérique ne s'est pas faite du jour au lendemain et comme toute révolution, elle s'est heurtée à des résistances.

(3) Nombre d'abonnés : Twitter @Gendarmerie 204 000 ; Facebook GN 535 000 ; Somme des pages groupement 500 000.

I La conquête des réseaux sociaux : une prise de risque indispensable ?

Comment sommes-nous passés du « gendarme de Saint-Tropez » au gendarme 3.0, totalement connecté ?

Disposant d'une image favorable dans l'opinion publique[4], la gendarmerie aurait pu se contenter d'exister dans le paysage médiatique à travers les articles de presse ou les reportages qui lui sont quotidiennement consacrés, d'autant qu'elle dispose déjà, en termes de communication, de ses

(4) Selon un sondage IFOP pour l'Essor de la gendarmerie réalisé en 2012, un an avant que le gendarmerie ne mette en place une véritable stratégie numérique, 83 % des personnes interrogées avaient une « bonne opinion » des gendarmes

propres outils de publications écrites (GEND'info, Revue de la gendarmerie nationale) et numériques (sites web). Mais le développement progressif des NTIC et l'émergence spontanée des RS ont bouleversé la façon de communiquer, le monde des médias et les attentes de la population. Nous vivons dans une société de l'information immédiate, avec une diffusion en continu, sans temps mort. Or, les médias sociaux permettent précisément une communication instantanée, plus directe et plus proche. L'émetteur diffuse l'information voulue, au moment voulu, sans aucun intermédiaire. Il « touche » même l'abonné partout et surtout n'importe où grâce aux NTIC.

Tiraillée entre l'attrait et l'intérêt de ces outils d'un côté et une certaine circonspection de l'autre, la gendarmerie saute finalement le pas en ouvrant une page nationale Facebook en 2010. C'est la première étape exploratoire vers le monde des réseaux sociaux.

Facebook : la puissance d'un réseau « amical »

En 2010, la gendarmerie réalise un coup d'essai avec la création d'une page groupe. Une expérience concluante qui conduit à la création d'une « fan page officielle » un an plus tard. Son rôle : promouvoir l'image de la gendarmerie en amont de l'événement du Tour de France. Elle attire rapidement de nouveaux membres, notamment de jeunes Internautes intéressés par ses carrières et métiers.

Très fort vecteur de communication virale, fonctionnant sur les réseaux de connaissances et d'amis, Facebook assure alors à la gendarmerie une présence renforcée durant la campagne de recrutement et au-delà, complétant les dispositifs classiques. Les publications de la page reçoivent un bon accueil mais la stratégie est loin d'être aboutie : la ligne éditoriale se limite à la duplication sur Facebook des informations mises en ligne sur le site internet.

L'année 2013 voit la création d'une section des publications numériques au sein du SIRPA-G. Le chef SIRPA-G lui confie la mission d'impulser une nouvelle dynamique, de « dépoussiérer la com » et de concevoir une véritable ligne éditoriale propre à Facebook. Style direct, articles vivants, thèmes variés et actions opérationnelles sont privilégiés. Des rendez-vous hebdomadaires sont aussi proposés aux fans avec des photos légendées et des vidéos. L'effet est net et sans appel : les abonnés passent de 60 000 à 530 000 en 3 ans.

Fort de ce succès et désirant rapprocher les gendarmes de terrain de la population, le SIRPA-G expérimente les pages Facebook au

5) Selon un sondage IFOP pour l'Essor de la gendarmerie réalisé en 2012, un an avant que le gendarmerie ne mette en place une véritable stratégie numérique, 83 % des personnes interrogées avaient une « bonne opinion » des gendarmes

niveau départemental, dans le cadre de la « feuille de route »,[5] puis généralise bientôt cette pratique à tout le territoire métropolitain et à l'outre-mer. Progressivement et pour de multiples raisons, Facebook ne suffit plus à occuper l'espace des médias sociaux. Pour livrer bataille et prendre toute sa place dans le "concert des institutions présentes sur les RS", la gendarmerie décide d'étendre son « offre » avec un compte Twitter.

Twitter, un défi en 140 caractères mais pas un gadget !

Souvent précurseurs en matière de communication, les dirigeants politiques ont très tôt mesuré l'intérêt de disposer d'un maximum de "canaux" pour valoriser leur action. Twitter, par la brièveté de son contenu, son côté « flash info » ou « fil AFP » et sa simplicité, est devenu très vite après sa création, en 2006, le réseau social idoine. En 2008, le chercheur Dominque Wolton affirmait : « *les hommes politiques qui sont déjà sous pression s'imaginent qu'avec de nouveaux moyens de communication comme Twitter, ils vont échapper à la tyrannie journalistique et instaurer un lien direct avec le public* ». Or d'après la journaliste Marie Maurisse, multiplier les tuyaux ne signifie pas toujours mieux communiquer mais expose au contraire au risque de saturation. Libérée par nature des contraintes électorales et des ambitions personnelles, la gendarmerie voit son horizon s'étendre aussi loin que porte sa vocation de service public. Renforcée par sa légitimité, son autorité et sa crédibilité en matière de sécurité et de défense, l'institution dispose a priori de tous les atouts pour s'inscrire dans cet univers inconnu, sensible, presque risqué. Les autres acteurs publics ne s'y aventurent d'ailleurs que dans une optique institutionnelle.

Le 21 janvier 2014, sous l'impulsion du général d'armée Denis Favier, directeur général de la gendarmerie nationale, le SIRPA-G lance donc le compte Twitter de la gendarmerie nationale, assumant d'emblée, par le choix d'un ton innovant et la publication d'informations opérationnelles, une véritable prise de risque.

Dès lors, quel sens donner à l'utilisation par la gendarmerie des réseaux sociaux ?

La stratégie numérique s'appuie sur une éthique professionnelle et une #GendarmerieEnOpérations

Une communication responsable, utile, toujours respectueuse du droit

L'esprit qui a présidé à la stratégie d'ensemble est le suivant : Il apparaît nécessaire, voire indispensable, de créer du lien dans l'espace « virtuel » en collant toujours au « réel ». Sur Facebook et Twitter, la gendarmerie nationale fait le choix de développer une stratégie numérique à vocation opérationnelle, sans

négliger le volet institutionnel, chaque réseau bénéficiant d'une animation spécifique en fonction de ses possibilités.

Pour y arriver, la gendarmerie s'est donc mise en ordre de marche. L'enjeu est de construire une structure adaptée à ses ambitions. La réussite de cette initiative a reposé d'abord sur l'adhésion et l'engagement de petites équipes en charge de l'animation des RS, puis sur la gratuité des outils et enfin sur le nombre limité d'ETP dédiés à la mission[6].

(6) Au niveau central, l'animation de la page Facebook puis le lancement du compte Twitter ont été faits sous plafond des effectifs. A l'été 2014, 3 ETP ont été créés pour pérenniser l'animation de Twitter. Au niveau départemental, il appartient au commandant de groupement d'organiser la publication sur sa page Facebook avec les effectifs dont il dispose.

Des principes clairs doivent guider en permanence l'action des membres des équipes de publication. Une information ne peut être publiée que si elle répond à 4 critères :

Utilité : concrète et opportune pour l'abonné, l'information doit donc être publiée dans le bon tempo. Par exemple, une coupure d'autoroute un jour de départ en vacances ne vaut qu'à l'instant ;

Véracité : l'information est factuelle, conforme à la réalité ;

Validation : l'information n'est pas publiée sans autorisation préalable de l'autorité compétente (magistrat, autorité administrative) et des chefs opérationnels qui sont au fait de la sensibilité locale. Selon la nature de l'information, un tweet est validé à différents niveaux : chef du bureau médias, chef du SIRPA-G, voire DGGN ;

(7) Au niveau central, l'animation de la page Facebook puis le lancement du compte Twitter ont été faits sous plafond des effectifs. A l'été 2014, 3 ETP ont été créés pour pérenniser l'animation de Twitter. Au niveau départemental, il appartient au commandant de groupement d'organiser la publication sur sa page Facebook avec les effectifs dont il dispose.

Légalité : aucune information ne doit contrevenir au droit[7].

C'est sur ce « quadriptyque éthique » qu'est fondée la crédibilité de la gendarmerie sur les RS. Par ailleurs, une communication toujours responsable renforce le SIRPA-G et surtout les chefs opérationnels.

Produire de la sécurité via les réseaux sociaux

La stratégie numérique de la gendarmerie est à son image : opérationnelle. Elle repose sur une structure militaire, pyramidale ascendante : toutes les informations émanant des unités du terrain remontent par la chaîne des officiers communication ou lui parviennent via le centre d'opération et de renseignement de la gendarmerie. Bien entendu, pour être dans le temps de l'action et répondre à l'exigence de l'immédiateté imposée par une communication sur les RS, les unités peuvent également saisir directement le SIRPA-G pour relayer une information urgente, à l'exemple des appels à

témoins. Grâce à son « maillage territorial numérique » (91 pages Facebook départementales), la gendarmerie dispose en outre d'un puissant outil de communication "au cœur des territoires" : rien n'est plus facile qu'un post pour informer la population locale au plus près de ses préoccupations, voire échanger et recueillir des informations.

Ainsi, la gendarmerie diffuse des informations opérationnelles à visée sécuritaire. Elle informe ses abonnés, en fonction des problématiques locales, sur les nouvelles formes de délinquance observées par les unités, leur rappelle les actions de prévention mises en œuvre près de chez eux, comme l'opération tranquillité vacances, ou relaye l'existence d'application smartphone, comme « cambrioliste » qui permet de lister ces biens et de faciliter les procédures en cas de vols. Cette action offensive *via* les réseaux sociaux est-elle suffisante pour « imposer » aux autres la vision d'une gendarmerie opérationnelle, utile voire moderne et connectée ?

La puissance et l'influence en question !

Osons faire un parallèle avec la définition de la puissance telle que Raymond Aron la concevait en matière de relations internationales. Dans quelle mesure la gendarmerie impose-t-elle aux médias, aux institutions, voire aux abonnés influents les thèmes qu'elle choisit et l'agenda de son actualité ?

Un réel retour en termes de sécurité

Soyons clairs : le compte Twitter et les pages Facebook ne sont que des outils et ne peuvent pas, à eux seuls, dicter le « je veux » de la gendarmerie à ceux qui sont chargés de faire l'actualité.

Toutefois, à défaut de s'imposer par la force, la gendarmerie attire les « influenceurs » en faisant passer des messages pertinents et adaptés aux codes des RS. Ainsi, « *en croissance continue depuis son lancement, le compte @Gendarmerie s'est imposé comme une référence, tant sur le fond de ses messages (actualité opérationnelle de la gendarmerie, prévention, informations relatives aux questions de sécurité publique) que dans la forme de ses publications (attractivité et originalité), faisant l'objet de très fréquentes reprises et citations dans les médias* »[8]. Il est d'ailleurs classé aujourd'hui au 7e rang des comptes institutionnels les plus suivis. Plusieurs milliers de journalistes nationaux ou issus de la presse quotidienne régionale sont abonnés à @Gendarmerie pour capter les infos exclusives que la gendarmerie annonce. De nombreuses personnalités publiques suivent aussi le compte. Les messages émis bénéficient d'une visibilité assez forte et de relais efficaces, y compris chez Twitter France, ce qui

(8) Citation du colonel Gwendal Durand, chef du bureau médias au moment du lancement du compte Twitter.

démultiplie les effets attendus. Surtout, « faire le buzz » n'a qu'un seul but : augmenter le nombre d'abonnés pour accroître la portée des messages d'information, en particulier en cas de crise.

Car la présence sur les RS prend tout son sens en temps de crise où les abonnés sont avides d'informations fiables et de messages officiels qu'ils ne peuvent trouver ailleurs que sur les comptes institutionnels, les médias ayant parfois tendance à privilégier le « scoop » au détriment du factuel.

La communication de crise revêt alors un intérêt politique majeur puisqu'il s'agit pour les pouvoirs publics d'informer, de rassurer, de conseiller, de prévenir et d'accompagner la population. Les retours en termes de sécurité, voire de recueil d'informations sont bien réels pour les forces de l'ordre. L'organisation territoriale de la gendarmerie et le caractère opérationnel de la DGGN sont des atouts pour suivre en temps réel l'évolution d'une situation complexe sur le terrain. Le bureau médias est en mesure de projeter des personnels en qualité de journaliste reporter d'images, sous l'égide ou non de la délégation interministérielle à la communication du Ministère de l'intérieur, pour récupérer de la matière et enrichir les publications (photos, vidéos, *etc.*).

À titre d'exemple, au lendemain des attentats du 13 novembre 2015 à Paris, le tweet : « #EtatdUrgence Des contrôles ont lieu partout en France. Ne signalez pas la position des forces de l'ordre #Attentats » a été vu par plus de 800 000 personnes. Sur Facebook, le même post a atteint 6 millions de personnes. Cette information faisant appel à l'esprit citoyen de la population a donc été « plébiscitée » pour son utilité !

Au-delà de cette analyse, quel peut être l'impact des réseaux sociaux sur la réputation ou l'image de la gendarmerie, en externe comme en interne ?

Une gendarmerie décomplexée

L'influence des réseaux sur la réputation ou l'image d'une institution (e-réputation[9]), une entreprise, une marque ou une personne, n'est pas linéaire et difficilement quantifiable. Les effets sont variables et l'on ne peut finalement se limiter à observer l'e-réputation de la gendarmerie, car elle dépasse les réseaux sociaux.

(9) L'e-réputation est l'image véhiculée par une marque (société, personne ou institution) sur tous les types de supports numériques (médias, réseaux sociaux, forums, messagerie instantanée…).

La présence de l'Institution sur les RS s'accompagne d'un retour positif en termes d'image et donc de recrutement. Difficilement quantifiable, ce retour est néanmoins réel et il suffit pour s'en convaincre de lire les commentaires, d'observer la croissance du nombre de fans ou les reprises médiatiques (télévisuelles, presse écrite ou radio).

Humaniser l'Institution, montrer que l'action des gendarmes a du sens, et concurremment donner des outils de compréhension aux internautes sur cette action suscitent l'adhésion grandissante des abonnés. Aujourd'hui, la gendarmerie existe et évolue au-delà de sa fonction même de gardienne de la loi et force de sécurité. Elle ne se contente plus d'offrir des bénéfices concrets à la population. En partageant sur les RS ses « coups de cœur » ou ses « coups de gueule » mais aussi ses réussites (belles affaires de police judiciaire), la gendarmerie construit avec ses fans ou followers toute une histoire émotionnelle et collective.

De même, en dévoilant « l'envers du décor », comme les coulisses de la formation des gendarmes, elle joue sur une dimension d'identification et stimule ainsi son attractivité.

Soucieuse de s'inscrire en permanence dans une démarche de service public, l'Institution produit de la sécurité grâce aux réseaux sociaux en informant la population au plus près de ses préoccupations, spécialement en temps de crise. Ses publications valorisent l'action collective de ses personnels civils et militaires, de l'échelon central à celui de la brigade.

Alors que la gendarmerie a conquis Facebook et Twitter, trouvera-t-elle un intérêt à investir d'autres réseaux sociaux ?

LES AUTEURS

Le chef d'escadron Frédéric Allamand est chef de la section des médias sociaux au Sirpa-G et community manager de la gendarmerie. Il a occupé le poste de commandant de la compagnie de Bonneville (74) après avoir été cadre de contact puis officier communication à l'École des officiers de la gendarmerie nationale et commandant de l'escadron départemental de sécurité routière de la Haute-Loire.

Titulaire d'une maîtrise de droit, Suzanne Ferret est attachée d'administration du ministère de l'Intérieur, où elle sert actuellement en qualité d'ajointe au community manager de la gendarmerie. Elle a notamment occupé le poste de rédactrice en chef-adjointe du magazine GEND'info, puis de rédactrice en chef de la Revue de la gendarmerie nationale avant d'être chef de la section des publications électroniques au Service d'informations et de relations

L'émergence des nouvelles technologies dans l'univers de la sécurité

par **SERVAN LÉPINE**

La prise en compte de l'évolution des problématiques de sécurité liées aux mouvements migratoires européens et à la répétition des attentats terroristes provoque l'ajustement de nouvelles réponses pour lutter contre cette situation sociétale dont les conséquences peuvent être lourdes. Face à ces événements, nous observons une réelle prise de conscience et une vraie volonté de transférer certaines missions régaliennes à la sécurité privée dans un cadre juridique établi.

SERVAN LÉPINE
Président d'EXCELIUM SAS

Toutefois, l'inventaire des solutions de sécurité actuelles peut apparaître aujourd'hui limité au regard de l'étendue des environnements et des amplitudes horaires à surveiller, de la rapidité de déplacement des individus, ou des moyens techniques mis en œuvre pour réaliser ces exactions. De nouveaux défis se présentent donc ouvertement à l'ensemble des acteurs publics, privés et citoyens pour maintenir la sérénité nécessaire aux populations, aux entreprises et aux États.

Nous pouvons reconnaître que nous retrouvons dans ce cadre de nouvelles formes de complexité qui imposent très clairement une approche particulière pour identifier les solutions de sécurité adaptées à chaque situation. Le premier principe est de mettre en œuvre une démarche d'analyse dynamique des moyens et des actions qui permettra ensuite d'ajuster la situation en fonction des résultats obtenus. L'analyse spécifique de l'évolution de la problématique impliquera ensuite de déclencher de nouvelles actions et moyens jusqu'à l'obtention d'une

Des réseaux qui permettront de raccorder des millions d'objets du fait des caractéristiques des émetteurs.

situation plus ou moins stable et maîtrisée. Dans ce contexte, on distinguera les actions qui seront réversibles de celles qui ne le seront pas et qui nécessitent en cas d'échec de trouver une nouvelle solution. Il s'agit donc d'une manière générale d'imposer un schéma d'action heuristique imposant un apprentissage par actions successives sans retour, parfois, à l'état d'origine.

Face aux problématiques de sécurité de demain, nous devons remettre en cause nos postulats historiques en nous appuyant sur l'émergence des nouvelles technologies et les évolutions sociétales, comme les nouvelles formes de participation collaborative, pour développer de nouveaux moyens de vigilance, d'analyse et de communication de l'information.

Une révolution numérique aboutie

Au regard de l'évolution des systèmes informatiques depuis une trentaine d'années et des pratiques qui l'ont accompagnée, nous pouvons imaginer celles qui sont à même d'émerger au regard des problématiques de sécurité et de sûreté que nous rencontrons.

En se référant à la technologie de la vidéosurveillance, dont on observe l'évolution des performances techniques et la baisse des prix depuis 20 ans, nous pouvons discerner le chemin et la performance des systèmes de sécurité qui vont se développer dans un contexte fortement stimulé. Nous pouvons prendre conscience du chemin déjà parcouru en rappelant que certaines caméras sont à présent capables de restituer une image en couleur dans la pénombre, de voir à plus de 500 mètres dans une obscurité totale et sur un périmètre de 360°.

La problématique du stockage des données ou des images est maintenant banalisée au regard du développement de la performance des systèmes d'enregistrement qui se sont accrus de plus d'un million de fois en 20 ans tout en se miniaturisant par 10. Le Big data s'impose du fait du rapport entre la quantité d'informations susceptible d'être recueillie et son faible coût de stockage. En même temps, les systèmes de compression de données se sont eux aussi perfectionnés pour compenser le

poids toujours plus important des données à véhiculer.

En parallèle, la facilité et les capacités de communication de ces données se sont de la même manière accrues à travers les réseaux filaires ou hertziens. La fibre optique a supplanté la traditionnelle liaison téléphonique de cuivre. L'Internet Protocol (IP) s'est définitivement affirmé comme le standard de communication s'imposant à des vitesses de transmission impressionnantes entre tous les équipements électroniques. La vitesse de dialogue entre les différents systèmes informatiques disséminés sur la planète présente aujourd'hui des temps de réponses impressionnants au regard d'anciens équipements de communication comme le Minitel ou les premières connexions ADSL.

La révolution numérique s'est bel et bien imposée dans ce domaine et celui des télécommunications. Dans celui de la sécurité des biens et des personnes, la révolution ne fait que commencer !

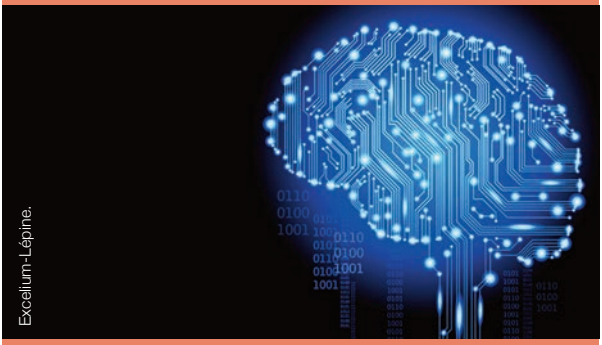
Des réseaux pour une géolocalisation des objets connectés.

En se projetant sur les dernières technologies qui sont sur le point de se généraliser sur le plan mondial, nous prenons conscience qu'il reste de nombreuses choses à inventer dans le domaine de la sécurité des biens et des personnes.

Nous évoquerons en premier lieu le développement des réseaux de communications basses fréquences (LoRa, SigFox, Quowisio, …) qui permettent de communiquer de petites quantités d'information sur des distances très importantes. Cette technologie va bientôt permettre de relier n'importe quel objet connecté qui aura été équipé d'un capteur. Ces nouveaux réseaux, en cours de déploiement sur le territoire français, vont donc permettre à très brève échéance de raccorder des millions d'objets à moindres coûts (1 €/an) du fait de la puissance des émetteurs et de l'étendue de leur rayonnement.

Il faut savoir aussi que ces réseaux peuvent arriver à capter un signal plusieurs mètres en profondeur et dans certaines conditions jusqu'à 5 niveaux de parkings souterrains. De ce fait, tout déplacement d'objet équipé sera identifié et géolocalisé en temps réel, permettant de détecter toute évolution anormale dans l'espace ou dans le temps en générant une alarme et, le cas échéant, de le localiser en temps réel. Bien plus encore, les techniques employées faciliteront l'envoi d'informations sur le fonctionnement des équipements et permettront de relever toutes sortes d'informations complémentaires (température, état des équipements, niveau sonore…).

Il est évident que d'ici peu, nous pourrons protéger contre le vol tout objet équipé de ce type d'émetteur. Si l'on prend en compte la miniaturisation de ces capteurs qui va s'opérer en parallèle, nous pouvons être rassurés sur une évolution très favorable pour la lutte contre le vol.



Excelium-Lépine.

Des algorithmes évolués qui comportent l'acquisition d'une intelligence en matière d'événements anormaux.

Le développement des applications mobiles associées à ces technologies va permettre à chacun d'assurer de manière plus active la surveillance de son environnement et développer des missions collaboratives qui permettront à d'autres de réaliser des missions de surveillance partagées dans l'espace et dans le temps.
« L'uberisation » de certaines prestations de sécurité risque de se développer, permettant de mutualiser des moyens de surveillance et d'en réduire les coûts.

Une vigilance technologique différenciée pour acquérir un contexte

Des applications mobiles comme CityLity permettent dès aujourd'hui d'identifier dans son environnement urbain ou domestique tout dysfonctionnement technique ou environnemental mais aussi de relever toute problématique relative à la sécurité des biens et des personnes.

N'importe quel utilisateur est dès à présent en mesure, à tout moment, de relever un incident et de le porter à la connaissance de tous pour permettre de réagir ou de développer telle ou telle vigilance par rapport au risque identifié. Un historique dynamique des événements se constitue progressivement, permettant aux acteurs concernés (publics et privés) de mettre en place des actions ou des solutions ponctuelles ou définitives dans les espaces concernés.

Dans d'autres environnements plus sensibles, la sécurité intégrera de façon marquée les problématiques de protection des données, des réseaux et de l'accès à l'information.

Certains équipements électroniques de sécurité avec une forte autonomie électrique ont développé des capacités

de déplacement à travers des systèmes de pilotage automatiques qui s'adaptent en temps réel à l'environnement (vent, état du terrain, dénivelés…) et des capacités d'analyse des données qui faciliteront la surveillance d'environnements sensibles.

Les algorithmes d'analyse des données se seront tellement développés que tout comportement suspect sera identifié et analysé avec une réponse immédiate renvoyée à l'environnement ou aux agents chargés de la surveillance. Ces algorithmes vont se perfectionner pour analyser des comportements suspects, des mouvements de foule, l'identification de certains objets (armes, explosifs, …) qu'il sera possible de neutraliser plus rapidement. L'apprentissage artificiel ou « Deep Learning » basée sur l'analyse répétée d'images ou d'informations permet à présent à la machine de développer des fonctions d'apprentissage autonomes. Facebook l'utilise déjà pour reconnaître un individu figurant sur des photos postées et de l'identifier même en second plan. Cette technologie permet, par rapport à des technologies traditionnelles, de développer des fonctions d'apprentissage autonomes au niveau informatique sur des caractéristiques plus abstraites qu'elle va elle-même construire.

Associées au Big data, ces technologies vont permettre d'assister les agents de sécurité dans l'analyse des environnements, limiter les fausses alarmes et détecter des comportements anormaux ou violents. Les caméras vont développer des fonctions nouvelles. Outre le suivi automatique d'une personne, de caméras en caméras, lors de son déplacement ou l'identification d'un objet abandonné derrière un emplacement non visible, il sera possible de repérer un individu circulant à contre-sens ou présentant un comportement anormal dans une file d'attente ou durant un embarquement.

Il sera possible demain, d'associer la reconnaissance faciale en 3 dimensions au rapprochement de données externes d'origine diverses (personnelles, géographiques, historiques…) sur l'individu et d'établir des corrélations particulières permettant de justifier l'appréciation d'un comportement douteux. En rapprochant ces données, l'informatique sera à même de faire des associations inattendues, sans même avoir été programmée. Par exemple, identifier un individu qui passerait systématiquement à proximité d'un endroit sensible ou qui y resterait un peu trop longtemps, pourra générer une alerte.

Les moyens d'action seront alors pilotés, en local ou à distance, pour permettre une réaction adaptée et efficace à chaque situation identifiée mais sans déployer d'importants et coûteux moyens humains.

Excelium-Lépine.

Les robots dotés d'une intelligence artificielle vont partager le champ de la sécurité en renforçant l'acquisition de phénomènes.

Nous ne sommes pas loin de retrouver certains éléments de science-fiction qui ne nous paraissent pas aussi éloignés aujourd'hui de ce que l'on pouvait imaginer il y a 20 ans !

Les prochains acteurs de la sécurité seront-ils des robots ?

En France, depuis 5 ans, les premiers drones ou aéronefs civils ont fait une apparition avec le soutien de la Direction générale de l'aviation civile qui a fait preuve d'audace dans un domaine déjà extrêmement sensible et réglementé.

Aujourd'hui accessibles en termes d'investissement, ils permettent de surveiller de grands espaces avec précision et efficacité pour protéger des infrastructures sensibles ou des agents de sécurité lorsqu'ils sont confrontés à des actions de lutte contre les incendies ou des manifestations violentes.

L'autonomie de ces drones va progresser de manière évidente comme les moyens embarqués d'analyse d'images qui vont permettre d'accroître leur utilisation dans la sécurité notamment dans le cadre d'escortes sensibles, de surveillance de foules ou de protection de grands espaces naturels (forêts, montagnes, bords de mer…).

En parallèle, les travaux réalisés sur l'intelligence artificielle, la précision des automatismes, la captation de signaux sonores et visuels, vont permettre la présence de robots de sécurité aux côtés des équipes de sécurité. Certainement pas sous la forme d'engins aux formes humanoïdes mais plutôt sous des formes plus ludiques et plus acceptables sur le plan humain. Serons-nous capables de présenter notre carte d'identité numérique à un robot présent à l'entrée d'un aéroport, d'une gare ou d'un site sensible ?

L'environnement s'adaptera pour nous permettre d'entrer dans ces lieux avec une certaine liberté sachant qu'au préalable un certain nombre de

vérifications aura été réalisé pour nous permettre d'y accéder.

Protéger les libertés fondamentales dans un contexte critique et mouvant

La question essentielle qui se pose, à travers l'émergence de ces nouvelles technologies tournées vers la sécurité, concerne la préservation des libertés individuelles ou collectives. Resteront-elles identiques pour tous ? Varieront-elles en fonction des territoires et des circonstances ? Quelle autorité sera en charge d'en ajuster les droits et le périmètre ?

N'oublions pas les réticences rencontrées hier par les populations et les politiques lors de l'émergence des caméras de vidéosurveillance. Même dans des situations de tensions sécuritaires fortes, il faudra toujours veiller à maintenir un environnement qui soit propice à l'autonomie et à la responsabilisation des individus.

Il est évident qu'à travers les grands bouleversements que le monde rencontre à présent au niveau climatique, sociologique, migratoire et économique, les appréciations risquent d'évoluer. L'Organisation Interanationale pour les Migrations (OIM) indique que plus de 250 millions de personnes risqueraient de migrer de leur pays d'origine, d'ici 2050, du fait de contraintes climatiques. Lorsque l'on observe les conséquences en Europe de la migration de 4 millions de personnes issues du Moyen-Orient et d'Afrique en 2 ans, nous pouvons imaginer les conséquences plus massives de ces contraintes migratoires.

Ce sont des questions auxquelles chacun d'entre nous doit dès à présent réfléchir afin que les technologies n'aliènent pas les libertés pour lesquelles nos aïeux se sont battus et auxquelles aspire profondément l'espèce humaine.

L'AUTEUR

Servan LÉPINE, président et fondateur d'EXCELIUM SAS, société française de sécurité. Ingénieur en Économie et Gestion des Entreprises Agroalimentaires (ENITA Clermont-Ferrand) Il a travaillé pendant 7 ans dans des missions d'hygiène alimentaire, assurance qualité, puis dans la gestion de restaurants d'entreprises à la Défense. Après 4 ans dans un Groupe International de Sécurité, il crée EXCELIUM en 2003. Au sein du Syndicat national des entreprises de sécurité (SNES), il occupe actuellement les missions de Responsable Régional Ouest et de vice-président en charge de la Commission « Hommes & Technologies ».

ALLER PLUS LOIN

EXCELIUM : Société Française de Sécurité (Nantes, Paris, Lyon, Toulouse, Rennes, La Roche/Yon) - Services & Solutions de Sécurité - Certifications ISO 9001, APSAD P3 & Intrusion. Cette société propose une offre GLOBALE de Sécurité à travers des solutions temporaires ou définitives de sécurité basée sur l'émergence des nouvelles technologies. EXCELIUM réalise actuellement la surveillance de la construction de la LGV Tours-Bordeaux et du métro de Rennes.
EXCELIUM est membre fondateur du « Consortium Sécurité Privée » regroupant 13 Entreprises Françaises de sécurité pour proposer une offre globale nationale.
Il représente avec 4.500 salariés, 140 M€ de chiffre d'affaires et 40 agences sur le plan national, le 5e acteur français de la Sécurité Privée.

Les systèmes de drones
au cœur de la transformation numérique de la gendarmerie nationale

par JÉRÔME BISOGNIN

Institution séculaire, en charge de la sécurité de 95 % du territoire et de la protection de 50 % de la population, la gendarmerie nationale s'est toujours donné les moyens de mettre les nouvelles technologies au service de l'accomplissement de ses missions. Aujourd'hui, tel est encore le cas, notamment avec les systèmes de drones aériens[1].

Apanage jusqu'à présent d'unités spécialisées (GIGN, SRTA, IRCGN)[2], la territorialisation des drones est désormais possible en raison de leurs facilités accrues de mise en œuvre et des progrès de la miniaturisation. Combinant capacités d'évolution dans la 3e dimension et d'appui au profit des personnels déployés au sol grâce aux charges utiles (caméra embarquée par exemple), ils sont un facteur de modernisation du service public que rend la gendarmerie nationale. Il convient cependant de les inscrire dans l'organisation plus vaste des moyens aériens dont elle dispose et pour lesquels un haut niveau d'exigence en termes de sécurité aéronautique est l'un des principes cardinaux. Après avoir présenté les modalités d'insertion des systèmes de drones aériens de la gendarmerie nationale dans l'architecture aéronautique d'État, l'auteur se propose de décrire combien ils permettent d'optimiser l'action des unités opérationnelles et d'ouvrir des perspectives capacitaires mais aussi de

JÉRÔME BISOGNIN

Colonel de Gendarmerie
Chargé de mission
DGGN
Direction de l'organisation et de l'emploi

(1) L'appellation ''systèmes de drones aériens'' est privilégiée sur celle de drones en raison de l'association indissociable de l'aéronef, du système de télépilotage, du télépilote qualifié et des liaisons de vol et de charge utile.

(2) GIGN : groupe d'intervention de la gendarmerie nationale, SRTA : section de recherche de la gendarmerie des transports aériens, IRCGN : institut de recherches criminelles de la gendarmerie nationale.

Le drone est inséré dans le dispositif après une concertation entre les chefs opérationnels et la vérification du contexte légal.

positionnement pour la gendarmerie nationale.

Conquérir une place légitime dans l'environnement aéronautique de la gendarmerie nationale

Annonciateurs d'une 3D pour tous, relayés par les médias sous l'effet des succès de leaders mondiaux du drone civil, les systèmes de drones ont suscité des interrogations avant que ne soit décidé d'étendre leur déploiement au sein de la gendarmerie nationale.

L'expérimentation, comme facteur de connaissance et d'adhésion aux systèmes de drones

En premier lieu, la DGGN a fait le choix d'en démontrer la pertinence en ayant recours à des Évaluations technico-opérationnelles (ETO). En tant que démarche expérimentale, ces ETO ont permis de mettre en évidence les atouts tactiques et techniques des systèmes de drones, leurs limites objectives et un certain nombre d'impératifs à satisfaire dans leur emploi. Elles ont mobilisé des experts métier et technique afin de susciter une indispensable approche pluridisciplinaire et de favoriser les synergies attendues. Pour les réaliser, la DGGN s'est inscrite dans une démarche partenariale auprès des fleurons de la filière du drone qui ont été des gages de progrès mutuellement bénéfiques et d'interconnaissances indispensables dans le cadre d'une ambition commune.

Le travail d'équipe pour fédérer

Les voies et moyens d'une cohérence nationale, entre les unités déjà détentrices de systèmes de drones et celles pouvant le devenir, ont du être définis afin de faire sens et concevoir un objectif de portée institutionnelle. Ainsi, un groupe de travail a été constitué par la DGGN afin de rédiger une doctrine d'emploi, de mettre en place un plan d'équipement et d'élaborer une formation centralisée. Il est apparu logique, dans ce contexte, de faire du Commandement des forces aériennes de la gendarmerie nationale (CFAGN) l'organe pivot du dispositif en raison de son expérience inestimable du milieu aérien.

L'encadrement juridique des systèmes de drones

La démarche globale entourant un tel projet d'entreprise a mis en lumière le besoin d'un encadrement strict par des normes supérieures. Ainsi, les systèmes de drones de la gendarmerie nationale

relèvent de l'édifice réglementaire relatif à la conception des aéronefs télépilotés d'État[3] et à leur utilisation de l'espace aérien[4]. Il en résulte un niveau élevé d'exigence au plan de la sécurité aéronautique, condition de l'autorisation des vols par le directeur général de la gendarmerie nationale en tant qu'autorité d'emploi[5]. La mise en œuvre de systèmes de drones, par ailleurs, doit s'effectuer hors cadre judiciaire dans le respect de la vie privée et de l'inviolabilité du domicile[6]. Les dispositions de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés doivent en outre être respectées dans la mesure où des données individuelles seraient recueillies par les caméras embarquées. Sauf besoin tenant à la procédure pénale ou à l'exploitation pour la formation dans le cadre du retour d'expérience, ces données ne seront pas conservées plus de trente jours. Le respect du cadre d'emploi de la vidéoprotection mobile[7] est donc un point d'ancrage lors du recours aux systèmes de drones.

(3) Arrêté du 24 décembre 2013 fixant les règles relatives à la conception et aux conditions d'utilisation des aéronefs militaires et des aéronefs appartenant à l'État et utilisés par les services des douanes, de sécurité publique et de sécurité civile qui circulent sans aucune personne à bord.

(4) Arrêté du 17 décembre 2015 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord en particulier.

(5) Arrêté du 3 mai 2013 sur les attributions de la direction de la sécurité aéronautique d'État, de l'autorité technique et de l'autorité d'emploi.

(6) Article 9 du code civil.

(7) Note express N°29301 GEND/DOE/SDSPSR/BSP/DR du 11 avril 2012 relative au cadre d'emploi de la vidéoprotection mobile.

Faciliter la préparation et la conduite de l'action

Le développement d'une capacité nationale de drone va permettre de mettre à la disposition des unités de la gendarmerie nationale un moyen supplémentaire pour mener une manœuvre de renseignement qui contribue à l'accomplissement d'autres missions.

Un nouvel appui du CFAGN aux unités

Tout commandant d'unité de la gendarmerie nationale pourra demander le concours d'un système de drone. Il est donc une évidence de capitaliser sur les savoirs-faire du CFAGN afin d'assurer l'efficacité et la proximité sur la base du meilleur choix de capteur aérien d'informations. Pour gérer les demandes de recours au système de drone, la DGGN a institué un processus de dialogue entre les chefs opérationnels et les commandants locaux des forces aériennes de la gendarmerie nationale. Cet échange est la clé de la réussite de la mission confiée à un système de drone. Elle comprend un effet à produire sur un adversaire ou sur un terrain mais aussi une insertion fiable au sein d'un dispositif commandé à partir du sol et l'observation de règles d'utilisation en sécurité de l'espace aérien.

Un vaste éventail de missions

Un système de drone est un outil qui se caractérise par sa polyvalence. Il est une

aide à la décision pour tout personnel en charge d'un commandement, notamment grâce à la retransmission d'images en temps réel qui permet l'appréciation exhaustive de la situation et l'expression rapide d'ordres en retour.

Renseigner les autorités d'emploi prend un autre sens, par ailleurs, car il est possible de leur donner une meilleure vision des conditions d'engagement opérationnel des moyens et de les aider de ce fait à formuler leurs directives. C'est dans l'appui des moyens au sol que les systèmes de drones démontrent toute leur pertinence. La liste des possibles est vaste : surveiller un objectif, dissuader des malfaiteurs d'agir, appuyer un poste de contrôle, faciliter la manœuvre au maintien de l'ordre, protéger un site, soutenir les opérations criminalistiques, aider à une interpellation sur la voie publique, renseigner sur des infractions flagrantes...L'emploi au profit du soutien est aussi envisageable pour la préparation de travaux en hauteur dangereux ou encore dans le cadre de la communication institutionnelle.

Une organisation adaptée aux besoins

De telles opportunités opérationnelles pourront se concrétiser sur l'ensemble du territoire national. Les acquisitions échelonnées de systèmes permettront d'établir, en effet, une couverture drone en métropole et en outre-mer. Elle sera déployée principalement dans les unités

Les pilotes des drones, issus de toutes les subdivisions de l'arme, suivront une formation qualifiante dispensée par le CFAGN.

du CFAGN. Ainsi, les commandants territoriaux verront s'accroître leur capacité de manœuvre grâce au recours à des moyens aériens complémentaires dans leur emploi ou subsidiaires pour certaines circonstances. Des personnels ressources, issus des unités du CFAGN comme de la gendarmerie départementale ou de la gendarmerie mobile, en seront les servants après avoir suivi une formation qualifiante au groupement d'instruction du CFAGN. Les ''précurseurs'' de la capacité nationale de drones de la GN (GIGN, SRTA, PJGN) conserveront leurs compétences. D'autres unités spécialisées (PI2G, GOS, GPI notamment) en seront aussi détentrices pour satisfaire des besoins spécifiques.

Ouvrir de nouvelles perspectives

Les systèmes de drones sont au cœur d'une révolution numérique qui irrigue les

mondes privés et régaliens. La gendarmerie nationale doit accompagner cette dynamique afin d'en maîtriser les répercussions pour ses propres processus mais aussi dans le but de déceler les facteurs d'adversité qu'ils pourraient porter en germe.

Sirpa-gendarmerie

La profondeur du projet quant à son terme, l'évolution des matériels et des doctrines impose une synergie, au niveau ministériel entre opérateurs et partenaires majeurs du projet.

Des travaux bénéfiques sur les drones malveillants

Les survols de sites sensibles par des drones entre l'automne 2014 et le printemps 2015 en sont une illustration. Ils ont conduit la DGGN à prendre à bras le corps la menace des drones malveillants. Une réponse globale y a été apportée, recouvrant tous les champs d'action de la gendarmerie nationale. Elle a permis l'arrestation de télépilotes de drones grâce aux capacités d'investigation qui ont été développées par la gendarmerie des transports aériens et la sous-direction de la police judiciaire de la DGGN. La mise en œuvre de contre-mesures maîtrisées et proportionnées est aussi désormais possible. La DGGN s'est engagée, en outre, dans des travaux interministériels de longue haleine sous l'égide du secrétariat général de la défense et de la sécurité nationale qui ont permis de bâtir des coordinations innovantes. Cette mobilisation a contribué à enrichir les connaissances sur les systèmes de drones, sous l'angle de leurs atouts pour le service de la gendarmerie mais aussi à la lumière d'un certain nombre de risques qui ne peuvent être ignorés (en particulier les vulnérabilités liées à l'environnement électromagnétique). Les concours de l'Office national des études et recherches aérospatiales (ONERA) et de la division des applications militaires du commissariat à l'énergie atomique (CEA/DAM) ont été à ce titre précieux. Cette apprentissage par l'étude de l'adversité a vocation paradoxalement à se prolonger au regard des potentialités duales des systèmes de drones au profit des univers civils et sécuritaires. Elle permet, de même, de positionner les systèmes de drones de la gendarmerie nationale au bon niveau.

Le progrès par la globalisation des objectifs

La DGGN s'est dotée d'une méthode pour avoir une vision exhaustive sur les objectifs capacitaires à atteindre. Pour être progressifs et soutenables, les travaux sur les systèmes de drones doivent être enrichis par une veille permanente, présenter un cadre pluriannuel, se caractériser par leur approche holistique (technique, opérationnelle, juridique, financière, partenariale, sociologique, universitaire, ...) et capitaliser sur des ETO. Ils présentent également une dimension de coopération internationale. Un partenariat avec des gendarmeries sœurs permet d'avoir des retours d'expérience, d'échanger sur des bonnes pratiques, voire de rechercher des appuis. Le premier lot de 4 microdrones de la gendarmerie nationale a bénéficié d'une subvention du Fond de Sécurité Intérieure de l'Union européenne, ce qui atteste de la portée continentale du projet.

De nouveaux défis à l'horizon

Cette dynamique de projet et de progrès doit d'inscrire dans le long terme. La miniaturisation des aéronefs, le développement de l'intelligence artificielle dite faible, l'amélioration des traitements de données recueillies et leur numérisation au sein d'un cloud de sécurité intérieure sont des jalons déjà perceptibles. Le projet n'est pas autonome en soi et « coagulera » sûrement avec d'autres ambitions structurantes pour la gendarmerie nationale comme l'équipement NEOGEND. Il est un moteur, enfin, d'une dynamique plus vaste visant à doter certaines des composantes du ministère de l'Intérieur de tels systèmes de drones.

L'AUTEUR

Le colonel Jérôme Bisognin est chargé de mission à la direction des opérations et de l'emploi de la DGGN. Il a exercé des postes de commandement en unités opérationnelles et en écoles ainsi que des temps de responsabilité en tant qu'aide de camp du secrétaire général de la défense nationale et en état-major central. Il est diplômé et breveté d'état-major. Il est la cheville ouvrière depuis deux ans du projet ''drones'' de la DGGN.

La Structure d'accueil mobile déployable (SAMD), un indispensable outil d'aide au commandement

par **FABIEN MILLIASSEAU**

Ce mercredi 25 mars 2015, la quiétude de la petite commune de Seyne-les-Alpes dans les Alpes de Haute-Provence (04) est durablement troublée par la présence de plusieurs centaines de gendarmes. La veille, un Airbus A320 de la compagnie Germanwings s'est écrasé en montagne avec à son bord 150 personnes de 19 nationalités différentes.

Les plus hautes autorités françaises et étrangères se déplacent sur site, des familles de victimes affluent, des journalistes du monde entier épient les forces de l'ordre qui doivent gérer cette crise dans sa globalité, de l'ordre public à l'enquête.

FABIEN MILLIASSEAU

Chef d'escadron de gendarmerie officier planificateur DGGN

S'appuyant sur les principes de subsidiarité et de complémentarité, la montée en puissance du dispositif hors norme de la gendarmerie est rapide et complète. Les moyens locaux sont renforcés par les moyens nationaux et la manœuvre est coordonnée au sein d'un poste de commandement central reposant sur la structure modulaire du Centre de planification et de gestion de crises (CPGC).

La SAMD devient *de facto* l'exosquelette d'un poste de commandement de crise autour duquel s'articule un ensemble de structures et de forces.

Au cœur de la crise, la recherche et l'emploi de moyens opérationnels performants

La crise est un processus dynamique complexe initié après une période d'incubation ou d'accumulation d'incidents, s'amplifiant dans le temps et qui, lors de l'occurrence d'un événement déclencheur, éclate et se modifie sous

Un outil projetable au plus près d'un lieu de crise pour une posture opérationnelle efficiente.

l'action de facteurs aggravants. Dès lors et pour ne pas la subir, il faut anticiper les mesures de précaution, de prévention et d'organisation permettant d'en atténuer les effets et particulièrement la surprise, facteur principal de l'effet de sidération.

Si, d'après Platon, « *ce ne sont pas les murailles mais les hommes qui font les remparts protecteurs de la cité* », ces hommes, confrontés au stress, à la fatigue psychique et psychologique, doivent pouvoir s'appuyer sur des pratiques réflexes éprouvées, une logistique simple, peu contraignante, obéissant à un formalisme précis et être dotés d'outils opérationnels performants.

Dans ce cadre, en complément de moyens déjà détenus, le CPGC devait disposer d'un outil déployable et projetable afin d'accueillir, au plus près d'une zone de crise et dans une structure de circonstance et autonome, un état-major de planification et/ou de conduite des opérations avec tous les moyens nécessaires à leur fonctionnement (stations de travail, communications, énergie, éclairage, *etc.*).

En 2013, après une période de prospection, d'audits et d'analyse de produits auprès des industriels régulièrement amenés à concevoir des solutions au profit de la Défense, un marché est passé avec la société Cegelec Défense en vue de fournir à la gendarmerie un shelter à ses couleurs répondant aux besoins spécifiques de l'institution. La gendarmerie acquiert donc sur fonds propres cette SAMD permettant la mise en place d'un poste de commandement lors d'une crise majeure mais également son déploiement à

l'occasion d'événements de grande ampleur.

Un véritable couteau suisse

Les capacités techniques détenues par le CGPC lui garantissent son indépendance matérielle vis-à-vis de l'autorité bénéficiaire et lui permettent de compléter les moyens de commandement locaux.

La SAMD s'intègre dans ce concept d'autonomie, de résilience et s'avère adaptée aux divers théâtres d'opérations sur lesquels la gendarmerie est appelée à intervenir dans des conditions climatiques parfois extrêmes.

Il s'agit d'un poste de commandement projetable qui s'articule autour d'un conteneur ISO de 20 pieds aérotransportable de près de 10 tonnes, d'un poids lourd porteur à plateau (SCANIA), d'un poids lourd PREMIUM dédié au transport du lot d'accompagnement (soit quatre tonnes de matériels divers) et d'un groupe électrogène de plus de deux tonnes.

Au plus près de la zone de crise, une fois l'emplacement identifié, à savoir un terrain mesurant 15 mètres par 25 au minimum et présentant une déclivité de 5 % au plus, cette structure en alliage léger, issue des technologies aéronautiques, se déploie sans moyen de levage complémentaire en quatre heures tel un accordéon par un jeu de glissières. Une fois ouvert, le shelter offre alors deux espaces distincts. Le premier, "réservé", accueille les baies techniques sur lesquelles se greffent les différents moyens de communication. Le second est un espace "ouvert" qui offre une surface de 80 m^2 aménageable à la demande par le mouvement de cloisons amovibles et pouvant accueillir jusqu'à 28 postes de travail pré-équipés.

Plusieurs configurations internes sont également possibles, offrant à son bénéficiaire un espace de travail adapté au cas d'espèce, de l'*open space* aux espaces cloisonnés indépendants.

L'ensemble est alimenté électriquement soit *via* un raccordement direct au réseau local soit par son groupe électrogène disposant d'une autonomie de 12 heures.

Au sein de la SAMD, les moyens radios, informatiques, de téléphonie ou d'information permettent d'émettre en toutes circonstances.

Des bulles tactiques de plusieurs kilomètres de rayon peuvent être créées et raccordées entre elles par l'emploi de Relais indépendant portable (RIP) et des valises GATEPRO ou DESC permettant également une interopérabilité avec les réseaux radio des autres administrations (ACROPOL, ANTARES, *etc.*).

Le réseau Topaze ou Projectable Tactical Network (PTN) offre quant à lui la couverture d'une bulle d'environ 4 000 km^2, permettant les échanges voix et données et l'interopérabilité avec les autres réseaux radio. Une messagerie tactique et une connexion Intranet (pour 20 postes) sont également accessibles au

Un espace modulaire connecté et autonome permettant des configurations adaptées aux crises.

sein du shelter par l'utilisation de paraboles, de clefs 3G ou encore d'une antenne satellite.

Le système audiophonique est complété par la mise en service de centraux téléphoniques de petite capacité, des GSM et en situation dégradée des moyens satellitaires (IRIDIUM, ISATPHONE, BGAN, EXPLORER, *etc.*).

Enfin, les moniteurs et écrans de projection permettent de visualiser les chaînes d'information télévisées, les images retransmises en direct des hélicoptères ou des véhicules de la CNOEIL[1] (*via* les boîtiers VEMOTION) ou encore les images en provenance des quatre caméras IP pouvant être connectées entre elles. Cette structure climatisée, particulièrement complète dans son offre à l'utilisateur, peut se voir greffer des modules annexes à savoir des tentes UTILIS, en toile PVC suspendue à une charpente en profilés d'aluminium, pouvant offrir des surfaces de travail de 18 à 54 m².

(1) Cellule Nationale Observation et Exploitation de l'Imagerie Légale.

Un déploiement sollicité et régulier

Confrontée à des situations de crise de plus en plus nombreuses et complexes faisant peser des risques sur les populations et les enjeux vitaux, la gendarmerie est régulièrement amenée à recourir à cette structure. Au cours de l'année 2015, le shelter a ainsi été déployé à six reprises que ce soit à l'occasion de crises inopinées ou bien dans le cadre de la conduite d'événements planifiés s'inscrivant souvent dans le temps.

Lors de la catastrophe aérienne de la Germanwings au mois de mars, la SAMD et les tentes d'appoint ont été particulièrement utilisées en tant que PC de commandement, de conduite et d'enquête s'intégrant dans un dispositif plus large en coordination avec l'IRCGN et offrant des conditions de travail optimales aux militaires engagés sur cette opération à résonance internationale.

Fin avril, dans le cadre du traditionnel TEKNIVAL du 1er mai, le shelter a été mis à disposition de la région Nord-Pas-de-Calais et implanté sur la base aérienne 103 à Cambrai (59). Sur un site totalement désaffecté, sans aucune ressource électrique, ni réseau de communication, la structure a été particulièrement appréciée et a permis une conduite optimale des opérations.

Quelques semaines plus tard, le SCANIA a déposé la SAMD sur l'emprise de l'ex-base aérienne de l'OTAN à Grostenquin (57) devant accueillir le rassemblement estival annuel "Vie et Lumières" de la mission évangélique des Tziganes de France auquel participent entre 20 et 30 000 personnes de cette communauté. Enfin, sur fonds de crise migratoire et en vue d'interdire toute intrusion à l'intérieur du tunnel Transmanche, la gendarmerie est mandatée pour contrôler la zone Eurotunnel à Calais (62). Un important dispositif de gendarmes mobiles assure cette mission. Au mois d'octobre et pour plusieurs semaines, dans l'attente de structures plus pérennes, la SAMD a donc été déployée au profit du GOMO comme poste de commandement avancé. Si l'emploi de la structure d'accueil mobile se fait de plus en plus régulier, le CPGC ne dispose actuellement que d'un moyen et non d'une capacité.

Un moyen et non une capacité qui oblige à la prospective

Ne disposant que d'une seule structure, la gendarmerie doit parfois procéder à un arbitrage et un choix doit être réalisé quant aux missions à privilégier.

Par ailleurs, une fois par an et pour une période d'un mois, le shelter fait l'objet d'une remise en condition auprès de l'industriel. Cette obligation contractuelle conjuguée au caractère unitaire de ce moyen obère la capacité opérationnelle de manière momentanée et pourrait s'avérer préjudiciable en cas de déclenchement de crises simultanées.

C'est pour pallier le risque d'indisponibilité de la structure que des études sont actuellement menées par les militaires du CPGC afin d'acquérir un moyen intermédiaire entre la SAMD et les tentes UTILIS en mesure de déployer rapidement un PC de circonstance.

Un Véhicule Porte-Berce (VPB), muni d'un bras hydraulique et permettant de charger un container équipé des matériels spécifiques[2] pourrait

(2) La berce offre un espace de travail de près de 30m² et peut accueillir jusqu'à 20 postes de travail. Dotée d'équipements modernes en informatique (écran tactile interactif, écran extérieur, visio-projecteur, etc.), en transmission (réseau Intranet, Internet, satellitaire, etc.) et en moyens (mâts pneumatiques, climatisation, éclairage LED, etc.), elle est opérationnelle en mois de cinq minutes, agrège et valorise les moyens existants.

ainsi répondre aux besoins de la gendarmerie. Cette structure mobile polyvalente de commandement, projetable sans préavis au plus près de la crise, interopérable (Police nationale, DGSCGC, armées) et immédiatement opérationnelle constituerait alors l'élément de projection rapide permettant d'offrir un PC de commandement à l'échelon local concerné par l'événement. À terme, ces différents moyens pourraient par ailleurs être complétés par des modules dits de vie des militaires permettant leur couchage, la restauration ou encore l'hygiène élémentaire et offrant dès lors une parfaite autonomie au PC de commandement déployé sur tout type de théâtre.

Enfin, dans un esprit proactif visant à une amélioration constante des produits nécessaires en temps de crise, plusieurs militaires de l'unité travaillent sur le déploiement de moyens complémentaires au sein de la SAMD.

Le temps est souvent une contrainte importante et l'acquisition d'images actualisées de la situation et d'une cartographie associée est primordiale pour la conduite des opérations. Le système de cartographie de crise SC2, encore à l'état de prototype, permet en moins de quatre heures d'obtenir et de diffuser une mosaïque d'orthophotographies, sur-couchée de données cartographiques et opérationnelles. Ce système pourra être déployé au sein du shelter et offrir une véritable plus-value opérationnelle pour planifier, préparer ou conduire les opérations.

Enfin, si le système d'information et de projection d'images répond aux actuels besoins, il est perfectible et la recherche du produit le plus adapté est en cours. La réflexion porte sur l'acquisition d'un mur d'images sous forme d'un moniteur LCD aérotransportable qui permettrait, outre un gain de temps substantiel dans son déploiement, de disposer d'une résolution parfaite d'images.

Par ailleurs, il s'agit d'une structure évolutive capable d'accueillir tous les développements technologiques adaptés aux situations de crises. La SAMD apparaît donc comme un moyen rare, adapté à tout type de crise permettant, dans les meilleures conditions, de conduire les opérations et d'assurer la circulation de l'information.

L'AUTEUR

Le chef d'escadron Fabien Milliasseau, occupe les fonctions d'officier planificateur du Centre de Planification et de Gestion de Crise depuis le mois août 2014.
Officier sous contrat, titulaire d'une maîtrise de droit privé et d'un DESS d'analyse des systèmes stratégiques, le chef d'escadron Milliasseau a été précédemment affecté au Comgend de Mayotte comme officier adjoint renseignement et à la région de gendarmerie d'Aquitaine et pour la zone de défense sud-ouest comme chef de la section analyse renseignement ordre-public.

Un sonar en gendarmerie,
un moyen unique au service de tous

par NICOLAS KÜNKEL

La gendarmerie nationale dispose depuis 2006 d'un système de détection sonar à balayage latéral permettant de cartographier les fonds aquatiques et de procéder à des recherches de police judiciaire à partir d'une embarcation. Adapté de matériels du milieu naval militaire, ce moyen de haute technologie est détenu à Strasbourg par la compagnie fluviale de gendarmerie du Rhin . Il a été acquis grâce à des financements tri-nationaux (France, Allemagne, Suisse) et européens (fonds INTERREG).

NICOLAS KÜNKEL

Chef d'escadron de gendarmerie
Commandant la gendarmerie des voies navigables

Un outil technique à forte valeur ajoutée

La pièce maîtresse de cet équipement complexe est le sonar lui même, surnommé “poisson” mais dont la forme évoque plutôt celle d'une torpille. Il est équipé de transducteurs émettant et recevant des ondes acoustiques de courte fréquence. Les signaux sont alors transmis par le câble de traction à l'interface informatique installée à bord de l'embarcation qui génère les images. Aisément mis en œuvre, le matériel s'adapte sans difficulté à tout type de moyen nautique du petit semi-rigide à la vedette lourde. Par ailleurs, un capteur GPS permet de localiser précisément les échos détectés et d'en recueillir les coordonnées avec une grande précision. Les données stockées sur une carte externe permettent à la fois la lecture instantanée aux yeux aguerris des militaires formés et une lecture plus attentive à l'issue de la mission. Il s'agit d'un ensemble complet composé de plusieurs torpilles, d'une caméra de type ROV et de tous les équipements annexes nécessaires entreposés en permanence dans un véhicule de grande

Sirpa-gendarmerie

Une technologie qui met en œuvre des outils de détection et de cartographie.

capacité dédié. Les sous-officiers les plus expérimentés dispensent en interne une formation à la mise en œuvre du moyen et à l'analyse des données collectées qui était initialement réalisée par le fabricant. Les sous-officiers qualifiés assurent une permanence 24h/24 depuis Strasbourg et sont en mesure de répondre à toute sollicitation opérationnelle.

L'originalité tient également de ses conditions d'emploi

En 2005, à l'initiative de la France, un séminaire a été organisé à Strasbourg permettant la rencontre des différentes unités de police fluviale au niveau européen. Cet événement a permis de présenter les atouts de chaque participant sur le plan de la police judiciaire subaquatique et a mis notamment en lumière l'intérêt marqué de certains moyens spéciaux.

L'idée de départ s'appuyait donc sur la mise en œuvre de technologies modernes, en matière d'investigations subaquatiques, en portant effort sur la sécurité du personnel engagé dans des conditions physiques souvent risquées. De plus, les unités fluviales engagées sur le Rhin, se connaissant bien, avaient déjà enclenché une dynamique avancée de coopération facilitée par des textes normatifs (Accords de Schengen - Décision de Prum -Accord de Vittel) de plus en plus efficients. Ainsi, assez naturellement, l'idée d'acquérir en commun un sonar avec les partenaires les plus proches était née.

Ce projet tri-national consistait à intensifier la coopération transfrontalière sur les cours d'eau du Rhin supérieur en matière d'investigations subaquatiques. Ce projet devait également permettre d'améliorer et de développer la coopération dans les domaines juridique et administratif entre les différents partenaires en entraînant une harmonisation des procédures et un échange de savoir faire appliqué à des problématiques communes. Par le biais de la mise en commun de matériel de haute technicité, un transfert et surtout une synergie se sont développés entre les services de police dans le domaine des connaissances liées aux investigations dans le milieu aquatique.

En 2012, l'unité disposant du sonar a changé de configuration en devenant la

Sirpa-gendarmerie

Une permanence opérationnelle qui permet un engagement immédiat pour dispenser une expertise spécifique.

compagnie de gendarmerie fluviale franco-allemande. Cet équipement est mis en œuvre, dans le cadre des leurs enquêtes et recherches dans la région du Rhin supérieur, par des personnels spécialement formés : gendarmes français et policiers allemands ainsi que des personnels de la police des cantons suisses de Bâle-ville et Bâle-campagne.

Il s'agit donc d'un moyen utilisé depuis l'origine sur le plan international et d'un vecteur majeur de la coopération transfrontalière entre forces de police du bassin rhénan.

Jusqu'au 1er janvier 2016, les frais relatifs à l'engagement du moyen étaient à la charge des unités et des formations administratives qui en faisaient la demande. Dans un contexte budgétaire contraint, il avait été constaté une baisse significative des demandes de concours. Pour lever ce frein à l'emploi, en s'inscrivant dans le cadre de sa mission de coordination des unités fluviales et nautiques intérieures, le commandement de la gendarmerie des voies navigables basé à Conflans Sainte Honorine (78) prend à sa charge les frais induits par l'emploi du sonar en dehors du périmètre de la région ACAL (Alsace- Champagne-Ardenne-Lorraine).

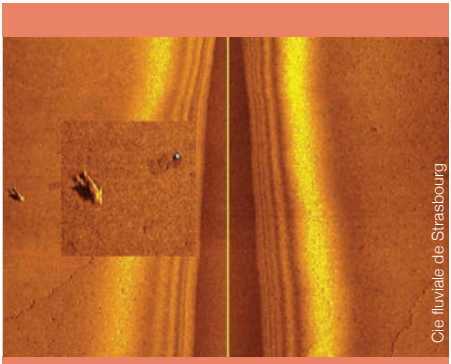
Un “système d'armes” intégré qui a d'ores et déjà fait la preuve de son utilité

Depuis sa mise en œuvre opérationnelle le 1er janvier 2007, les résultats obtenus au cours de plus de 453 missions réalisées en France et à l'étranger dans le cadre d'enquêtes judiciaires sont particulièrement révélateurs et ont un impact médiatique souvent important.

Les chiffres sont éloquents et témoignent de la pertinence du concept : 25 corps, 1097 VL, 351 embarcations, 25 objets divers principalement des coffre-forts ont pu être découverts grâce au sonar.

Il semble opportun de relever que sur 450 missions réalisées, près de la moitié d'entre elles l'a été au service de coopération transfrontalière.

En outre, non content d'être engagé à la demande d'unités territoriales, le sonar est utilisé à intervalles réguliers pour procéder à des cartographies de certaines voies navigables. De cette manière, il est aisé de constater les évolutions en découvrant de nouveaux objets immergés depuis le passage précédent. Il peut être employé indifféremment en eaux intérieures



Une lecture qui demande un expertise malgré une grande précision de l'image des résultats.

comme en mer sans limite technique véritable autre qu'une mise en œuvre à partir d'une embarcation.

Ce spectre missionnel varié permet de compléter l'action judiciaire des unités territoriales dans le cadre de l'atteinte aux biens en s'insérant dans le dispositif global de production de sécurité. Cet équipement unique au sein de la gendarmerie nationale apporte non seulement une plus-value significative dans l'engagement (rapidité, précision, zone étendue, préservation de la ressource en enquêteurs subaquatiques) mais permet également de retrouver des corps et des objets dans le cadre de dossiers d'enquête non solutionnés depuis longtemps ou à fort retentissement national ou international (par exemple affaire Lætitia Perrais à Pornic, engagements à Abidjan en soutien de l'OCRVP, aux Pays-Bas, en Hongrie ou en Guyane).

Une compétitivité qui repose sur une remise à niveau

Aujourd'hui, cet équipement n'est plus commercialisé par son fabricant américain sous sa forme initiale. Il utilise notamment une interface obsolète fonctionnant sous Windows XP qui n'est plus mise à jour par Microsoft. Le maintien en condition opérationnel via l'importateur français en devient particulièrement problématique.

Par ailleurs, l'évolution de la technologie en matière de sonar à balayage latéral et de caméra sous-marine de type ROV a conduit à la mise sur le marché de nouveaux produits beaucoup plus modernes, pratiques d'emploi et utilisant des systèmes d'exploitations actuels. Un projet de modernisation et de remise à niveau pourrait s'inscrire en conséquence dans une volonté de renouvellement d'un matériel à haute valeur ajoutée qui a fait la preuve de sa performance sur le plan opérationnel et dont la médiatisation des résultats permet à la gendarmerie d'afficher une avance indéniable dans le domaine de la police judiciaire subaquatique.

L'apport des fonds européens pour un projet par nature international permettrait assurément de conserver à cette technologie toute son acuité et à l'institution de conserver ce pôle d'excellence reconnu.

Les métiers de la sécurité évoluent, leurs technologies aussi

par GRÉGORY LEBOURDAIS

Depuis plusieurs années la robotique commence à se développer et à intégrer notre vie quotidienne. Après les robots d'intervention en milieu dangereux ou les robots aspirateurs, c'est maintenant dans la sécurité que la robotique vient améliorer le travail des agents.

Il s'appelle e-vigilante, c'est un robot de surveillance qui a été conçu pour effectuer des rondes autonomes à l'intérieur des entrepôts et sites industriels. Né suite à une étude de marché de plusieurs mois, avec plus de 150 personnes rencontrées dans le domaine de la sécurité, e-vigilante répond tout d'abord à trois grandes problématiques du milieu de la sécurité : un besoin constant de surveillance, une nécessité de réactivité en cas d'incident et la possibilité d'agir à distance et en temps réel.

GRÉGORY LEBOURDAIS

Directeur communication EOS Innovation.

La sécurité 2.0

La sécurité occupe une part de plus en plus importante au sein des entreprises. À l'heure du big data et des objets connectés, il était nécessaire de développer un nouveau produit en cohérence avec les avancées technologiques. Misant sur la robotique, EOS Innovation a cherché à savoir comment une plateforme mobile et autonome pouvait améliorer la sécurité des sites sensibles. Afin de déceler si un besoin commun émergeait, l'équipe a parcouru la France pendant plusieurs mois à la rencontre d'un grand nombre d'acteurs de ce milieu, allant des agents de sécurité sur le terrain aux directeurs de sites et d'entreprises de sécurité.

EOS innovation

Un outil conçu à partir d'une expression des acteurs de la sécurité en entreprise.

Cette étude a permis de valider l'intérêt du milieu de la sécurité pour ce type de solution et d'en définir les principales fonctionnalités: effectuer des rondes automatisées, détecter des intrusions et être capable de faire des levées de doutes à distance.

Après deux ans de développement, le résultat est e-vigilante: un outil de surveillance connecté permettant d'avoir une surveillance active et adaptable à la typologie de son site. Il fonctionne en totale autonomie et veille sur le site en effectuant des rondes préventives afin de signaler en temps réel un potentiel danger mettant en péril la sécurité. Toutes les données sont enregistrées pour analyser les failles, revoir les incidents et disposer de preuves.

Les agents de sécurité ne pouvant que rarement pénétrer à l'intérieur des entrepôts, e-vigilante est un outil efficace complétant leur travail, tout en évitant le risque humain, particulièrement lors de situations dangereuses (personnes mal intentionnées ou départ de feu).

C'est une extension de l'agent de sécurité, qui lui permet d'agir à distance, mais aussi de suivre l'intervention d'une personne en direct sur le site, en enregistrant de précieuses informations en cas de problème.

Enfin c'est un système non intrusif, e-vigilante opère ses rondes en dehors des heures d'activités et reste dans sa base lorsqu'il ne fonctionne pas, évitant toute interférence dans l'activité du site surveillé.

Comment fonctionne e-vigilante

Après son installation, qui prend moins d'une journée, la première étape pour le robot est d'intégrer la carte du site. Pour cela, il doit parcourir toute la zone pour enregistrer l'environnement (il faut environ une heure pour mémoriser un espace de 6 000 m²). Par la suite la personne en charge de la sécurité pourra, par le biais de l'interface administrateur dédiée, créer ses propres chemins de ronde et définir les horaires de fonctionnement, une formalité qui prend moins de 10 minutes. Tous ces paramètres, et bien d'autres, sont modifiables à n'importe quel moment en se connectant à l'interface administrateur et e-vigilante les appliquera lors de sa prochaine ronde.

Une fois ces opérations achevées le robot est autonome, il effectuera ses rondes aux heures demandées et ira se recharger automatiquement sans aucune

intervention extérieure. Sa première ronde lui permettra de mettre à jour les changements de l'environnement puis il effectuera ses rondes de surveillance.

Lorsqu'e-vigilante est en phase de travail, le télésurveilleur ou la personne en charge du site doit juste se connecter à l'interface utilisateur pour disposer du retour des informations en temps réel. Scannant son environnement à la recherche d'incidents de différents types (départ de feu, intrusion, porte n'ayant pas été fermée, palette déplacée...), le robot préviendra automatiquement la personne en charge de la sécurité lorsqu'il rencontrera une anomalie pouvant nuire à la sécurité du site. Cette dernière peut alors, en temps réel, qualifier l'incident grâce aux caméras et micros intégrés. Même si le site est plongé dans le noir absolu, les caméras à vision nocturne et les projecteurs infrarouges rendent la qualité du retour vidéo toujours optimale. La levée de doute devient quasi instantanée permettant de réagir immédiatement à un événement avec le maximum d'informations.

L'interface intègre tous les outils dont le télésurveilleur a besoin: retour vidéo en temps réel, position du robot sur le site, outils de rédaction d'une main courante, des moyens de dissuasion comme l'alarme ou la possibilité de parler et d'écouter ce qui se passe sur le site. Il suffit de cliquer sur l'endroit désiré sur la carte du site et le robot s'y rend automatiquement, en empruntant le chemin le plus court.

L'interface entre le robot et le télésurveilleur permet une levée de doute directe.

Un outil fiable

Une grande importance a été donnée à trois aspects cruciaux qui conditionnent la réussite d'un produit de ce type. Ce robot fonctionnant environ 400 heures par mois, sa fiabilité est un point clé.

L'industrialisation a été pensée, dès la conception, pour fiabiliser les processus et disposer d'un produit robuste. Ainsi tous les composants du robot ont été durcis et ont déjà prouvé leur efficacité sur le long terme. De plus e-vigilante est testé en permanence au sein d'un entrepôt dédié pour être constamment amélioré.

Le second point est la simplicité d'usage. L'interface administrateur permet de créer, modifier ou supprimer aisément les chemins de ronde et les horaires de fonctionnement du robot à n'importe quel moment. L'administrateur peut aussi gérer les utilisateurs et leurs accès en quelques clics. L'utilisateur dispose, quant à lui, d'une interface intuitive, où toutes les fonctions importantes sont en accès direct. Conscient que beaucoup d'entreprises utilisent déjà un logiciel de téléprésence, les protocoles nécessaires ont été développés pour que le contrôle du robot soit disponible sur une grande majorité de ces logiciels.

L'AUTEUR

Diplômé de Strate College Designer en 2009, Grégory Lebourdais rencontre David Lemaitre en mars 2010, lors de la création d'EOS Innovation. Il rejoint rapidement l'équipe et travaille notamment sur le design des produits ainsi que sur l'image de l'entreprise. Directeur de la Communication, il supervise les relations presse, la stratégie marketing et la cellule design d'EOS Innovation.

ALLER PLUS LOIN

Créée en mars 2010 par David Lemaitre, EOS Innovation est une entreprise spécialisée dans la robotique de surveillance. Elle conçoit, fabrique et commercialise e-vigilante, le premier robot de surveillance destiné aux entrepôts et sites industriels. Récompensée par plusieurs prix de l'innovation, l'entreprise a accueilli Scientipôle Capital à son capital en 2013. Début 2014, elle effectue une seconde levée de fonds auprès de la société Parrot pour accélérer son développement.

www.eos-innovation.eu

Le dernier point est la sécurisation du système. Il serait contradictoire de proposer un outil de surveillance qui ne soit pas lui-même sécurisé. Le système de communication est donc crypté et change toutes les 5 minutes, les informations sont transmises via un VPN sécurisé et les vidéos sont enregistrées sur trois supports différents.

Un potentiel prometteur

Aujourd'hui e-vigilante est capable de répondre aux besoins premiers en matière de sécurité. Il fonctionne dans plusieurs entrepôts et les perspectives de développement, notamment à l'international, sont très prometteuses. Nous travaillons pour demain afin de proposer des évolutions du système qui permettront beaucoup d'autres applications que ce soit en matière de sécurité ou dans des domaines complémentaires, faisant d'e-vigilante un outil d'une grande polyvalence.

NEOGEND au cœur
d'une démarche participative

par YVES MARZIN et THIBAUT LAGRANGE

La société connaît depuis plusieurs années un véritable bouleversement numérique. Le rythme des évolutions semble même s'accélérer et ouvre toujours davantage le champ des possibles. De très nombreuses solutions (équipements et applications) sont actuellement développées. Convaincu de l'apport déterminant que représentent ces nouvelles technologies, le Directeur général de la gendarmerie nationale (DGGN) a fixé, dès septembre 2014, un objectif ambitieux, au carrefour des démarches participatives de simplification ("feuille de route") et d'innovation ("ateliers de la performance") : doter chaque gendarme d'un smartphone ou d'une tablette sécurisée lui permettant d'accomplir, en tout temps, tout lieu, l'ensemble de ses missions.

Ces équipements, et plus largement l'environnement numérique associé, constituent bien plus qu'un outil de mobilité. Ils viennent transformer les modes d'action du gendarme et ouvrir des fonctionnalités et perspectives nouvelles. Au-delà, ils créent une nouvelle proximité avec la population en offrant de nouveaux services et en accélérant la capacité de réponse immédiate aux sollicitations par la multiplication des points de contact : le gendarme devient brigade.

YVES MARZIN

Colonel de gendarmerie
Cabinet du directeur général de la gendarmerie nationale
Pôle stratégie et conduite

THIBAUT LAGRANGE

Colonel de gendarmerie
Cabinet du directeur général de la gendarmerie nationale
Pôle stratégie et conduite

Le plan ministériel pour la sécurité

Le projet numérique de la gendarmerie est mené dans le cadre du Plan ministériel pour la sécurité (PMS) qui comporte cinq défis destinés à moderniser non seulement les équipements, mais aussi les modes d'action des forces de sécurité intérieure. Ces défis sont les suivants :

- la proximité numérique qui vise à simplifier les démarches administratives des citoyens, à leur offrir de nouveaux services numériques, à relayer l'action des forces de sécurité et à développer les échanges opérationnels et interactifs avec la population ;
- la modernisation et l'unification des plates-formes d'appels d'urgence pour améliorer le service offert aux usagers et assurer une meilleure coordination entre les services. Deux pistes sont examinées avec la mise en place d'une plate-forme commune pour la région parisienne et le lancement d'une expérimentation en province ;
- la mobilité qui doit permettre de mettre à disposition des forces de sécurité des terminaux (tablettes, ordiphones) et des applications adaptées pour améliorer la réponse opérationnelle et la sécurité des primo-intervenants ;
- les réseaux radio dont les équipements et le fonctionnement sont modernisés pour faire face aux nouveaux et futurs besoins opérationnels, tout en faisant converger les systèmes existants pour garantir une cohérence ministérielle et interministérielle ;
- les outils géodécisionnels et prédictifs qui, à partir des données collectées par les services ou disponibles en sources ouvertes, développent des solutions informatiques pour aider à la décision et à l'analyse. La détection, l'analyse et la finesse du suivi de certains phénomènes permettent d'optimiser la gestion des moyens et ainsi de lutter plus efficacement contre la délinquance.

Le projet NEOGEND

S'inscrivant dans le projet mobilité du ministère, le projet NEOGEND a suscité, dès son annonce et au regard des solutions existantes sur le marché, de très fortes attentes et exigences, en interne comme en externe. Pour y répondre au mieux, une nécessité s'est immédiatement imposée : associer pleinement les gendarmes à la conception et au développement de l'outil qui leur est destiné. Quelles fonctionnalités leur paraissaient incontournables, utiles, secondaires ? Quels nouveaux usages professionnels pouvait-on imaginer?...

Le DGGN a donc souhaité une démarche collaborative et participative animée par une équipe pilote au niveau national, s'appuyant sur l'ensemble des directions de la DGGN mais aussi sur des groupes utilisateurs issus de différentes unités opérationnelles. Cette conduite de projet

innovante correspond à l'esprit de la feuille de route de la gendarmerie : valoriser les gendarmes et faire de chacun d'entre eux un acteur du changement, une force de proposition pour renforcer l'action opérationnelle, pour alléger et simplifier les process et les fonctionnements.

Imaginé et élaboré après une réflexion participative sur les usages professionnels, NEOGEND a démarré à titre expérimental en septembre 2015 dans le département du Nord, avec le déploiement de 1200 équipements individuels. L'expérimentation se poursuit en 2016 avec la région Bourgogne (environ 2000 équipements avant l'été). Les militaires de ces unités sont équipés de smartphones Samsung Galaxy S5 et de tablettes Sony Xperia Z2, des équipements modernes et de grande qualité mis en dotation à titre individuel.

Dans le même temps, 6 500 tablettes collectives sont déployées au sein de toutes les unités élémentaires opérationnelles afin de familiariser les gendarmes à l'utilisation d'un outil dont la généralisation est attendue pour l'année 2017.

La démarche participative mise en place lors de la conception se poursuit pour le développement : les gendarmes du Nord et de la région de Bourgogne, collaborent de manière active au développement de NEOGEND. Un forum de discussion a spécialement été mis en place et donne satisfaction. Les échanges permanents et réguliers entre l'équipe pilote et les gendarmes dotés permettent et permettront encore, tout au long de l'expérimentation et de la préfiguration, d'améliorer et d'optimiser les solutions retenues avant leur généralisation nationale.

Des fonctionnalités diverses

À ce stade du projet, toutes les fonctionnalités permises de manière collective par les Terminaux informatiques embarqués (TIE)[1], sont proposées aux gendarmes dotés d'un équipement numérique individuel NEOGEND. Les gendarmes disposent également de toutes les informations opérationnelles avec la messagerie tactique et d'un accès sécurisé à tous les types de fichiers via une application. Parmi les nouveautés très appréciées du terrain, figure la lecture optique, via l'appareil photo, des bandes MRZ de certains titres officiels (carte nationale d'identité, carte grise...)[2].

(1) Pour assurer ses missions de sécurité publique et de police judiciaire, la gendarmerie dispose, à bord de ses véhicules, d'un système de transmission de données couplé au système de radiocommunication numérique RUBIS.

(2) La MRZ est une zone, lisible lorsque l'on passe le document dans un lecteur optique, qui permet de transmettre à un ordinateur les informations d'identité du porteur.

En un clic, le gendarme récupère automatiquement et sans erreur de saisie les données. Pour les passages aux fichiers, cela représente un gain de temps et d'efficacité certain, pour le gendarme comme pour la personne contrôlée.

D'autres applications ont également été développées comme l'Opération tranquillité vacances (OTV), qui facilite le suivi des usagers inscrits à cette

Les applications donnent un confort d'usage qui profite tant à l'opérateur qu'à l'usager.

opération de prévention des cambriolages. Plus encore, les patrouilles de gendarmerie visualisent sur une carte les résidences concernées et notamment, via un code couleur, celles qui n'ont pas fait l'objet d'une surveillance au cours des derniers jours. Cela permet d'orienter le service et de renforcer l'efficacité opérationnelle des patrouilles.

Un accès à la messagerie interpersonnelle est également offert aux gendarmes, ainsi qu'un espace individuel réservé dans un cloud privé de la gendarmerie. Chaque militaire peut ainsi y stocker, à partir du terrain, les documents qu'il souhaite (fichiers, photos, *etc.*), les partager au besoin, et surtout les récupérer sur sa station de travail Intranet dès son retour à l'unité. Les photos prises sur le terrain, lors de constatations par exemple, sont ainsi automatiquement stockées sur l'espace de stockage personnel et sécurisé et rendues immédiatement accessibles. D'autres fonctionnalités et applications sont enfin en cours de développement avec l'aide des programmeurs du service des technologies et des systèmes d'information de la sécurité intérieure (ST(SI)²) qui sollicitent au besoin l'appui de sociétés ou partenaires extérieurs (écoles d'ingénieurs...).

L'application "prise de note" facilitera demain la réutilisation des informations et renseignements recueillis sur le terrain. Dès le retour de service, ces éléments pourront venir alimenter les pièces de procédures ou compte rendu à rédiger. Les notes prises par le militaire sur le terrain viendront intégrer automatiquement de nombreux champs figurant dans le logiciel de rédaction de procédure. C'est une véritable plus-value.

L'application de cartographie opérationnelle permettra notamment la géolocalisation des patrouilles environnantes et les événements en cours. Déjà en phase de développement, elle constituera un outil supplémentaire d'aide à la décision et facilitera la gestion opérationnelle des interventions.

Toutes les applications sont ou seront mises en ligne sur un magasin privé de la gendarmerie, à l'instar des banques d'applications que l'on retrouve sur nos terminaux mobiles privés.

Ces applications doivent être accessibles en tout lieu, en tout temps, quel que soit le théâtre d'engagement des gendarmes. C'est pourquoi l'outil NEOGEND est

Sirpa Gendarmerie

Les interfaces proposées permettent un accès à toutes les informations opérationnelles.

capable de se connecter à l'aide des réseaux 3G/4G des opérateurs, à tout accès WIFI à Internet. Dans les cas où les réseaux de téléphonie mobile ne seraient plus disponibles, NEOGEND peut aussi s'appairer, en mode bluetooth, à un véhicule de patrouille pour réutiliser, en mode dégradé, le réseau radio RUBIS de la gendarmerie. Les accès au système d'information de la gendarmerie à partir de NEOGEND répondent aux mêmes conditions de sécurité et de traçabilité que depuis tout poste de travail au bureau. Les diverses utilisations prévues (messagerie tactique et interpersonnelle, interrogations de fichiers...) ou à venir (au vu des formidables opportunités d'applications qui s'ouvriront), ont nécessité la sécurisation des équipements et la traçabilité des usages pour répondre aux obligations légales prévues (déontologie, CNIL...). Basée sur un ANDROID libre de droit qui a été profondément modifié, la solution sécurisée SECDROID retenue pour l'expérimentation a été développée par le ST(SI)² conjointement avec l'Agence nationale de sécurité des systèmes d'information (ANSII). Elle garantit la sécurité des équipements ainsi que des informations contenues et transmises. Une dotation individuelle des smartphones et des tablettes facilite ensuite la gestion des certificats de sécurité et la traçabilité des actions réalisées.

La conduite du changement : une véritable transformation digitale de la gendarmerie

Le projet NEOGEND impacte fortement les usages habituels et les méthodes de travail. Il offre donc une occasion idéale pour réviser dans le même temps les procédures actuellement en place, en les modernisant et les simplifiant. La participation active et continue de représentants d'unités opérationnelles au sein des groupes utilisateurs garantit la prise en compte permanente des souhaits des gendarmes de terrain. Les diverses propositions sont ensuite analysées par le comité de pilotage de la direction générale et les directions contribuent aux éventuelles évolutions nécessaires : évolution des usages, de la doctrine ou des textes, diffusion de bonnes pratiques. L'idée n'est pas de calquer les processus actuels sur l'outil, mais bien de les identifier, de trouver les sources d'amélioration possibles et de profiter des forces de la nouvelle technologie pour simplifier, automatiser et ainsi optimiser les méthodes de travail. À l'image des ateliers de performance et de la

Les personnels peuvent connecter leurs matériels en cybersécurité quelle que soit leur position.

démarche de la feuille de route, il convient de tirer tous les bénéfices possibles de l'utilisation des nouvelles technologies et de la dotation individuelle des smartphones et tablettes numériques. La gendarmerie nationale est ainsi engagée dans une véritable transformation digitale.

Les applications développées prennent en compte l'architecture, l'ergonomie et le design nécessaires à des usages en mobilité sur des équipements de type smartphone ou tablettes. La dotation personnelle et individuelle des équipements permet de répondre à tous les besoins opérationnels, y compris les plus particuliers. Des applications destinées par exemple de manière plus spécifique à certains types d'unités (brigades fluviales, formations aériennes....) pourront être aisément développées et mises en fonction sur les équipements, dans le respect du cadre de cohérence technique nécessaire à la sécurité générale des équipements et des réseaux. Les applications indispensables au service quotidien seront intégrées aux équipements et mises à jour automatiquement à distance. Les applications disponibles seront accessibles via un portail de téléchargement permettant à chaque gendarme de personnaliser son environnement numérique opérationnel et de l'adapter à des besoins plus ponctuels ou spécifiques. La prise en main de ces nouveaux outils professionnels apparaît intuitive et très comparable à celle des tablettes et smartphones privés aujourd'hui très répandus. Les séances de formation nécessaires seront mises en place ou proposées directement sur les équipements.

Le projet NEOGEND, intégré aux défis du plan de modernisation de la sécurité, est naturellement mené en liens étroits et réguliers avec la Direction Générale de la Police Nationale (DGPN), les autres services ou directions du Ministère de l'Intérieur et, plus largement, en interministériel. Les équipements sécurisés smartphones et tablettes serviront aux différentes forces et les applications développées partagées, renforçant ainsi la coopération au sein du ministère. L'allégement et la simplification des procédures contribuent aussi à la modernisation de l'action publique.

Conduit en intégrant de façon itérative les utilisateurs, le projet NEOGEND positionne la gendarmerie comme un des acteurs les plus innovants en matière de technologies numériques.

Les textiles techniques
comme solutions de protection

par FRANÇOIS BOUSSU

Les textiles techniques peuvent apporter une réponse aux problématiques des impacts en tant que solution de protection souple (gilet pare-balles) ou en tant que renfort de matériaux composites pour des solutions dures (blindage de véhicule).

La compréhension du mode de déformation, lors de nos travaux expérimentaux de recherche d'impacts sur des structures tissées, nous a permis de révéler l'influence sur la performance balistique de certains paramètres du tissu. Forts de cette connaissance, nous avons proposé des solutions innovantes pour répondre aux besoins de protection des gilets pare-balles sous impacts de différentes munitions à des vitesses variées.

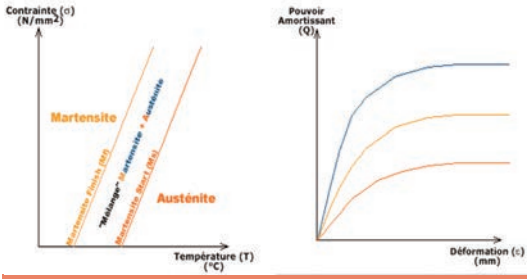
FRANÇOIS BOUSSU
Enseignant chercheur à l'ENSAIT
Laboratoire GEMTEX

La protection souple à l'impact se définit principalement par différents niveaux de performance répondant aux diverses menaces balistiques, répertoriées dans la norme NIJ 0101-06[1], tout en respectant trois critères principaux : la performance, l'ergonomie (poids, flexibilité) et le coût total[2]. Dans une étude récente et très complète sur les différents brevets existants de protection souple à l'usage de la personne[3], ainsi que dans le cadre de nos différents travaux de recherche[4], l'optimisation de ces trois critères, selon les configurations de menaces et d'utilisation, a nécessité le

(1) "Ballistic Resistance of Body Armor," Office of Science and Technology, National Institute of Justice, Washington, DC, NIJ Standard–0101.06 NCJ 223054, July 2008.

(2) C.A. Couldrick, "A systems approach to the design of personal armour for explosive ordonance disposal," Cranfield University, College of Defence technology, engineering systems department, Cranfield, UK., Engineering Thesis November 2004.

(3) B.Z. Haque Gama, M.M. Kearney, and J.W. Gillepsie, "Advances in Protective Personnel and Vehicle Armors, ," Recent Patents on Materials Science, vol. 5, pp. 103-134, 2012.



(gauche) Représentation des différentes transitions de phase de fil métallique à mémoire de forme de type Nickel-Titane - (droite) Évolution du pouvoir amortissant des différentes phases de transition du matériau à l'état solide en fonction de la déformation.

développement de nouvelles solutions pour mieux absorber l'énergie cinétique d'impact du projectile, rendre plus proche du corps la protection souple et minimiser les coûts des matériaux fibreux.

Les applications de protection souple, présentées dans cet article, s'orientent principalement vers des gilets pare-balles pouvant s'adapter à la morphologie du corps humain, notamment la partie supérieure comprenant l'ensemble des organes vitaux tels que les appareils digestif, respiratoire et le système de circulation sanguine. Cette adaptation est nécessaire pour assurer un contact permanent entre la solution de protection souple et la partie supérieure du corps humain, permettant ainsi la déformation lors d'un impact et l'absorption de son énergie sans provoquer de perforation du gilet pare-balles.

Les gilets pare-balles intégrant des fils à mémoire de forme

Initialement, le fil à mémoire de forme[5] à base de Nickel-Titane (Nitinol[6]), inséré dans une structure composite rigide à base de fils graphites résinés époxy, a montré une bonne capacité d'absorption à l'énergie d'impact faible vitesse[7], ainsi que dans des structures composites à base de fils de verre E résinés époxy[8]. Dans le cadre de nos premiers travaux de

(4) S. Taing, "Amélioration des performances d'un gilet discret contre les balles et coups de couteaux et diminution du trauma arrière," PROTECOP, Bernay, France, Projet de fin d'études ENSAIT 2007.
Koncar and F. Boussu, "Flexible Displays on Textiles for Personal Protection," in Intelligent Textiles for Personal Protection and Safety NATO security through science series. D: information and communication security, S. Jarayaman, P. Kiekens, and A.M. Grancaric, Eds.: IOS press, 2006, vol. 3, pp. 65-88.
J. Codina, "Développement d'une tenue pare-coups pour le maintien de l'ordre," Groupe MARCK, Argenteuil, France, Projet de fin d'études ENSAIT 2011.
J. Van Roey, "Étude du comportement dynamique des matériaux granulaires et tissés: approche expérimentale et simulation numérique," Ecole Royale Militaire, Bruxelles, Belgique, Thèse de doctorat 16/12/2011.

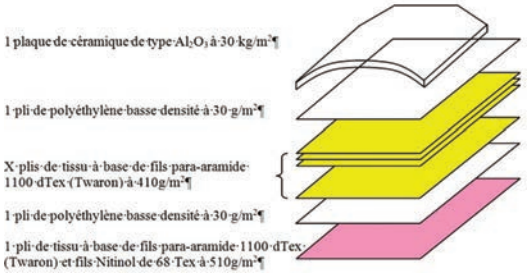
(5) E. Patoor and M. Berveiller, Technologie des alliages à mémoire de forme, Traité des Nouvelles Technologies – série matériaux ed.: Hermes, 1994.

(6) Niti Alloy Company. (2014, June) Shape memory alloy wire. [Online]. http://www.sma-mems.com

(7) T.C. Kiesling, "Impact failure modes of graphite expoxy composites with embedded superelastic Nitinol," Mechanical Engineering Deparment, VPI & SU, Blackburg, VA, USA, Master Thesis 1995.
T.C. Kiesling, Z. Chaudhry, J.S.N Paine, and C.A. Rogers, "Impact failure modes of thin graphite epoxy composites embedded with superelastic Nitinol," in 37th AIAA/ASME/ASCE/AHS/ASC structures, strucural dynamics, and materials conference, Salt Lake City, Utah, USA, April 15-17, 1996, pp. 1448-1457.

(8) S. Merlier and J-L. Petitniot, "Caractérisation et modélisation de l'amortissement de fils d'alliages à mémoire de forme," Université de Lille 1, Lille, France, Rapport de stage MST Juin 1997.
S. Bourasseau, S. Merlier, and J-L. Petitniot, "Caractérisation et modélisation de l'amortissement de fils d'alliage à mémoire de forme," ONERA, DMSE/RCS, Rapport technique RT n°99/42, Octobre 1999.
D. Joly and J-L. Petitniot, "Etude de l'effet amortissant de fils d'AMF dans des poutres en composite verre-époxy," ONERA, DMSE/RCS, Rapport Technique RT n°99/29, Août 1999.

recherche sur les protections souples de type gilet pare-balles[9], nous avons exploité la capacité d'absorption du matériau à mémoire de forme dans la phase de transition martensitique - austénitique lors d'un impact balistique[10]. Pour répondre aux impacts balistiques de niveau III et IV de la norme NIJ 0101-06[11], deux types d'armures de tissu ont été réalisés à partir d'un quadrillage de fils à mémoire de forme à base de Nickel-Titane (Nitinol) de 68 Tex (diamètre 0,25 mm) dans les directions chaine et trame des tissus et des fils para-aramides de 1100 dTex (Twaron). Ces deux types de tissus ont été positionnés en face arrière des cibles, comme préconisé par Ellis[12], composées d'un assemblage de différents matériaux (Figure 2) pour subir une cuisson en autoclave à 125 °C sous 15 bars pendant 3 heures.



Description des différents composants de la cible à base de tissu para-aramide et Nitinol.

Les performances balistiques des cibles, à base de tissu de para-aramide et de Nitinol positionné en face arrière, ont permis d'arrêter les projectiles de type 7,62 mm non perforantes (9,7 g à 838 m/s) lors de multi-impacts (niveau III) et la munition 7,62 mm perforante (10,8 g à 868 m/s) lors d'un mono-impact (niveau IV) (Tableau 1). Cependant, les déformées dynamiques des cibles mesurées après impact, sur l'empreinte du cratère laissé sur la plastiline lors de l'essai balistique ainsi que sur les cibles elles-mêmes, révèlent une hauteur de pénétration du projectile supérieure à la valeur autorisée de 44 mm prévue par la norme NIJ 0101-06.

(9) S. Lecomte, "Etude de matériaux composites à base de tricots et d'un tissu mixte alliage à mémoire de forme et Aramide," MS COMPOSITES, Liévin, France, Projet de fin d'études ENSAIT 2004.

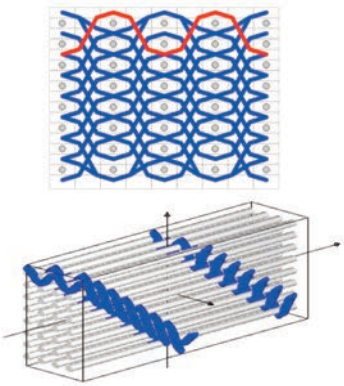
(10) J.V. Humbeeck, J. Stoiber, L. Delaey, and R. Gotthardt, "The High Damping Capacity of Shape Memory Alloys," Z. Mettallkd, vol. 86, pp. 176-183, 1995.
L. Planckaert, J-L. Petitniot, and E. Deletombe, "Optimisation des structures aéronautiques par déformations réversibles et préprogrammées – Etude numérique et expérimentale d'éléments structuraux en alliage à mémoire de forme," ONERA, Lille, France, Rapport Technique RT n°98/51, décembre 1998.
N. Koeda et al., "Damping Properties of Ductile Cu-Al-Mn-Based Shape Memory Alloys," Materials Transactions, vol. 46, no. 1, pp. 118-122, 2005.

(11) "Ballistic Resistance of Body Armor," Office of Science and Technology, National Institute of Justice, Washington, DC, NIJ Standard–0101.06 NCJ 223054, July 2008.

(12) M.R.L. Ellis, "Ballistic impact resistance of graphite epoxy composites with shape memory alloy and extended chain polyethylene spectra hybrid components," Mechanical Engineering, Blackburg, VA, USA, Master's Thesis December 1996.

Type d'essais selon la norme NIJ 0101-06	Masse de la cible (kg)	Performance balistique	Vue en face arrière de la cible après impact
Niveau 3: multi-impacts (6 projectiles) de balles de 7,62 mm non perforantes de 9,7 g vitesse à 838 m/s	3,35	Arrêt des projectiles Déformée dynamique supérieure à 44mm pour les deux derniers tirs.	
Niveau 4: mono-impact d'une balle de 7,62 mm perforante de 10,8 g vitesse à 868 m/s	3,33	Arrêt du projectile Déformée dynamique supérieure à 44mm.	

Observation des cibles à base de tissu para-aramide/ Nitinol après impact balistique de niveau III et niveau IV de la norme NIJ 0101-06.



Représentations 2D et 3D du tissu Interlock A - liage L 1-2-8 avec fils de chaine de surface.

(13) R.L. Ellis, F. Lalande, H. Jia, and C.A. Rogers, "Ballistic Impact Resistance of SMA and Spectra Hybrid Graphite Composites," Journal of Reinforced Plastics and Composites , vol. 17, pp. 147-164, 1998.

(14) A. Purushothaman, G. Coimbatore, and S.S. Ramkumar, "Soft Body Armor for Law Enforcement Applications," Journal of Engineered Fibers and Fabrics, vol. 8, no. 2, pp. 97-103, 2013.

(15) A. Mohd Rozi, Y. Wan, A. Wan, S. Jamil, and S. Azemi, "Effect of fabric stitching on ballistic impact resistance of natural rubber coated fabric systems," Materials and Design, 2007.

Comme l'a constaté ultérieurement Ellis et al. [13], les fils à mémoire de forme de type Nickel-Titane ne contribuent pas à absorber l'énergie d'impact aux vitesses des projectiles des niveaux III et IV de la norme NIJ 0101.06 en raison de leur faible valeur de réactivité sous déformation dynamique rapide.

Les gilets pare-balles intégrant des hybridations de structures textiles

Dans le cadre des travaux de Purushothaman et al.[14], le recours à l'assemblage de matériaux de nature différente, tels que du cuir, du non tissé aiguilleté et des multi-couches de tissus, permet de répondre à la fois à la protection balistique et à la protection à la coupure. De la même façon, l'assemblage par couture en losange de multi-couches de tissus secs et enduits de caoutchouc naturel a permis d'obtenir de meilleures performances à l'impact balistique pour des tirs au niveau IIIA de la norme NIJ 0101.06 (407 à 420 m/s) et de réduire la valeur de la déformée dynamique après impact par rapport à des assemblages de tissus non cousus [15].

Ainsi, dans le cadre de nos travaux de recherche[16] ont été assemblées différentes structures textiles (non tissé et tissus), dont un tissu 3D interlock chaine à base de fils para-aramide de 840 dTex (Twaron) de type Interlock A -Liage L 1-2-8 avec fils de chaine de surface (Figure 3), pour les soumettre à deux types d'impacts (balle de 9mm et FSP 5,4 mm) selon la norme STANAG 2920[17] et de

(16) J. Maillet, "Développement d'une nouvelle solution balistique souple dans le cadre du projet EPIDARM," OUVRY, Lyon, France, Projet de fin d'études ENSAIT 2008.
J. Maillet, M. Lefebvre, F. Boussu, and M. Pirlot, "Innovative 3D textile structure for soft body armor protection, EPIDARM project," in Intelligent Textiles and Clothing for Ballistic and NBC Protection. Split, Croatia: ASI NATO, August 31, 2011, p. 350.
F. Boussu and J. Maillet, "Innovative 3D textile structure for soft body armour protection," in NATO Advanced Study Institute "Defence Related Intelligent Textiles and Clothing for Ballistic and NBC (Nuclear, Biological, Chemical) Protection, Split, Croatia, Tuesday 6th April to Friday 16th April 2010.

(17) NATO Standardization Agency, "NATO STANAG 2920 PPS:2003 Ballistic Test Method for Personal Armour Materials and Combat Clothing. 2nd ed.," Brussels, Belgium, 2003.

(18) D.J. Finney and F. Tattersfield, "Probit Analysis: A Statistical Treatment of the Sigmoid Response Curve," Journal of the American Statistical Association, vol. 47, no. 260, pp. 687-691, 1952.
H.J. Langlie, "A Reliability Test Method for "One-Shot" Items," Ford Aerospace Communications Corporation, Aeronautronic Division, 1965.

mesurer les performances balistiques par la vitesse V50 (la probabilité estimée de perforation est de 0,5) et la déformée dynamique des cibles ou BFS (Back Face Signature)[18].

L'assemblage de matériaux à propriétés mécaniques et physiques différentes lors d'une sollicitation dynamique de type impact apporte à la cible finale un comportement hybride d'absorption d'énergie, segmenté par les différentes couches de matériaux utilisées. Nous avons donc considéré différents matériaux textiles souples, tels que :

- le non tissé à base de fibres de para-aramides pour la valeur de son module en compression dans l'épaisseur nous permettant de diminuer la valeur de la déformée dynamique après impact[19].

- l'assemblage de 5 couches de tissus de para-aramide Kevlar 29 par couture suivant un quadrillage de cm dont le nombre de couches, la forme et la dimension du type de couture a permis de révéler un meilleur comportement à l'impact de munitions de type 9 mm de niveau IIIA de la norme NIJ 0101.06 par rapport à d'autres types de couture (Cf note 16).

- un tissu 3D interlock chaine à base de fils para-aramide de 840 dTex (Twaron) de type Interlock A -Liage L 1-2-8 avec fils de chaine de surface présentant une meilleure perforation à l'impact d'une bille de 10mm de diamètre (5,04 g) à 900 m/s que les deux autres types : Interlock O - liage T 1-7-7 avec fils de chaine de renfort et Interlock A - Liage T 9-5-5 avec fils de chaine de renfort et base sergé façonné de 10 effet trame cordon à droite[20].

A partir de ces matériaux, différents assemblages ont été réalisés pour aboutir à une masse surfacique de 5,07 kg/m^2.

Référence des cibles	Composition des cibles
PW DQ + Felt	X_1 plis de 5 couches de tissus de para-aramide Kevlar 29 cousus selon un quadrillage de cm (PW DQ) Y_1 plis de non tissé de fibres para-aramides (Felt)
PW DQ + 3D LtL + Felt	X_2 plis de 5 couches de tissus de para-aramide Kevlar 29 cousus selon un quadrillage de cm (PW DQ) Y_2 plis de tissu Interlock A - liage L 1-2-8 avec fils de chaine de surface à base de fils de para-aramide 840 dTex (Twaron) (3D LtL) Z_2 plis de non tissé de fibres para-aramides (Felt)
3D LtL + PW DQ + Felt	X_3 plis de tissu Interlock A - liage L 1-2-8 avec fils de chaine de surface à base de fils de para-aramide 840 dTex (Twaron) (3D LtL) Y_3 plis de 5 couches de tissus de para-aramide Kevlar 29 cousus selon un quadrillage de cm (PW DQ) Z_3 plis de non tissé de fibres para-aramides (Felt)
PW DQ + 3D LtL + Felt + PW DQ	X_4 plis de 5 couches de tissus de para-aramide Kevlar 29 cousus selon un quadrillage de cm (PW DQ) Y_4 plis de tissu Interlock A - liage L 1-2-8 avec fils de chaine de surface à base de fils de para-aramide 840 dTex (Twaron) (3D LtL) Z_4 plis de non tissé de fibres para-aramides (Felt) Q_4 plis de 5 couches de tissus de para-aramide Kevlar 29 cousus selon un quadrillage de cm (PW DQ)

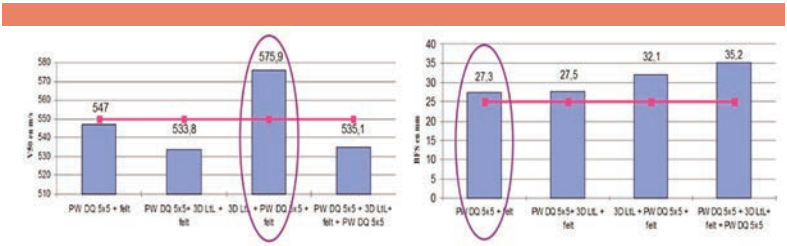


Figure 4 : Comparaison des 4 cibles selon : (gauche) la vitesse V50 en m/s d'un FSP de 20 mm - (droite) la déformée dynamique après impact (BFS) en mm.

(19) Maillet, "Développement d'une nouvelle solution balistique souple dans le cadre du projet EPIDARM," OUVRY, Lyon, France, Projet de fin d'études ENSAIT 2008.

(20) Cf note 16

(21) J. Singletary and A. Bogdanovich, "3-D Orthogonal Woven Soft Body Armor," Journal of Industrial Textiles, vol. 29, no. 4, pp. 287-305, January 2000.

Nous pouvons constater (Figure 4 - gauche) que seule la cible référencée (3D LtL + PW DQ + Felt) possède une valeur de V50 de 575,9 m/s sous impact FSP 5,4 mm (masse 1,1 g) selon la norme STANAG 2920, supérieure à l'objectif initial de 550 m/s, par le positionnement en face avant du tissu Interlock A - liage L 1-2-8 avec fils de chaine de surface à base de fils de para-aramide 840 dTex (Twaron) (3D LtL), montrant ainsi une performance balistique supérieure par rapport aux autres cibles.

Par contre la valeur de la déformée dynamique après impact (BFS) de cette même cible référencée (3D LtL + PW DQ + Felt) est de 32,1 mm (valeur supérieure à l'objectif initial de 25 mm) montrant ainsi plus de déformation sous sollicitation dynamique que la cible plus rigide référencée (PW DQ + Felt) de valeur de BFS égale à 27,3 mm (Figure 4 - droite).

L'hybridation de matériaux textiles face aux différentes menaces (FSP de 5,4 mm et munition de 9 mm) contribue plus ou moins, selon les critères utilisés (V50 ou BFS), à l'amélioration de la performance balistique pour une même masse surfacique de cible dans le développement de nouvelles solutions de protection de type gilet pare-balles; mais reste néanmoins difficile à identifier en raison du nombre important d'essais à réaliser pour comprendre la part de chaque matériau dans le mécanisme d'absorption de l'énergie cinétique d'impact.

Les gilets pare-balles adaptés à la morphologie féminine

Dans les travaux de Singletary et al.[21], les performances balistiques des tissus 3D interlock chaine par rapport aux multi-couches de tissus cousus dans l'épaisseur ont été révélées, notamment par la contribution des fils de chaine de

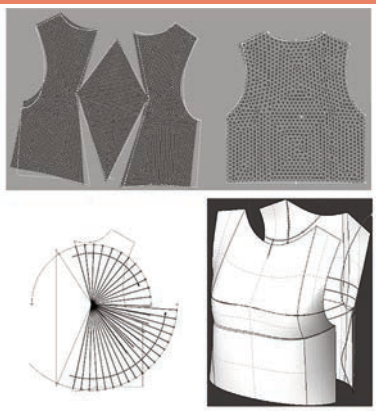


Figure 5 - (haut) plastrons avant et arrière découpés à plat avant assemblage - (gauche) rotation de la ligne de découpe pour chaque pli de tissu autour de la pointe avant de la poitrine - (droite) mise en forme 3D des plastrons avant et arrière du gilet pour un pli de tissu.

liage et leur nombre par unité de volume. Selon ces mêmes auteurs, ce type de tissu 3D interlock chaine peut s'avérer être une solution nouvelle pour la confection de gilet par balles à morphologie féminine, évitant ainsi les coutures d'assemblage ou l'ajout d'implant rigide. En complément de cette proposition, Chen et Yang[22], ont souligné l'intérêt de la déformabilité multidirectionnelle du tissu 3D interlock chaine pour la réalisation de gilets pare-balles à morphologie féminine et ont proposé un modèle de découpe géométrique des tissus à plat pour une mise en forme en 3D[23] à partir des dimensions relevées sur la poitrine. Cependant, les découpes nécessaires à la conception des plastrons issus des tissus 3D interlock chaine à plat engendrent des zones de déchet de 20 à 30 % de la surface totale, ce qui augmente considérablement la part du coût des matériaux fibreux dans le coût total du gilet.

Ainsi, dans le cadre de nos travaux de recherche[24], nous avons réalisé des gilets pare-balles à base de multi-couches de tissus 2D de para-aramides découpés et assemblés selon une disposition nouvelle des points de couture, afin de minimiser les découpes et le poids du gilet final par la réduction du nombre de plis de tissus, permettant une même performance à l'impact balistique d'une balle de 9 mm FMJ RN à 350 m/s de niveau II de la norme NIJ 0101.06.

Chaque couche de tissu a fait l'objet d'une découpe selon la forme avant et

(22) X. Chen and D. Yang, "Use of 3D Angle-Interlock Woven Fabric for Seamless Female Body Armor: Part 1: Ballistic Evaluation," Textile Research Journal, vol. 80, no. 15, pp. 1581–1588, September 2010.

(23) X. Chen and D. Yang, "Mathematical Modeling Use of Three-dimensional Angle-interlock Woven Fabric for Seamless Female Body Armor: Part II," Textile Research Journal, vol. 80, no. 15, pp. 1589-1601, September 2010.

(24) F. Boussu and P. Bruniaux, "Customization of a lightweight bullet proof vest for the female form," in Advances in military textiles and personal equipment.: Woodhead Publishing, 2012, ch. Part II, pp. 167-195.
P. Bruniaux, I. Cristian, and F. Boussu, "State of the art and new perspective on ballistic vest design," in Technical Textiles – Present and Future Symposium, Iasi, Romania, 21-22 October 2011.
A. Cichocka, M. Kulinska, P. Bruniaux, and F. Boussu, "Ballistic Body Armor Project for Women," in AUTEX 2009 World Textile Conference, Izmir, Turkey, May 26-29, 2009, pp. 773-778.
J. Maillet, M. Kulinska, A. Cichocka, P. Bruniaux, and F. Boussu, "A ballistic vest for women," in LWAG 2009 Conference, Security and use of innovative technologies against terrorism, Aveiro, Portugal, May 18-19, 2009.
F. Boussu, A. Ragot, M. Kulinska, X. Legrand, and P. Bruniaux, "Customization of a lightweight ballistic vest," in Futurotextiel 08, 2nd International scientific conference "Textiles of the Future", Kortrijk, Belgium, 13 – 15 november 2008.

Figure 6 : (gauche) face avant du gilet pare-balles avec la localisation des 6 points d'impact - (milieu) visualisation des zones déformées en face arrière du gilet - (droite) empreintes des déformées dynamiques aux 6 points d'impact dans la plastiline Roma n°1.

arrière du plastron (Figure 5- gauche), puis la ligne de découpe de la forme avant du plastron a subit une rotation d'un angle de 8,92° à chaque nouvelle couche de tissu autour du centre situé à la pointe avant de la poitrine (Figure 5 - milieu), ce qui a permis de réaliser un assemblage par couture pour relier les plastrons avant et arrière pour chaque couche de tissu (Figure 5 - droite). Par la suite, les différents plastrons assemblés ont été enfilés les uns sur les autres pour former un gilet à base de multi-couches dont les lignes de couture des plastrons avants et arrières ne s'alignent pas suivant l'épaisseur, répartissant la zone de rupture des coutures lors de l'impact sur une surface plus importante.

Par le biais de cette répartition des zones de couture, nous avons pu enlever deux plis de tissu par rapport au nombre initial de plis préconisé par Tong et al.[25] pour la réalisation d'un gilet pare-balles soumis à un impact de 9 mm FMJ à 350 m/s de niveau II de la norme NIJ 0101.06. Nous pouvons localiser les 6 points d'impacts sur la face avant du gilet (Figure 6- gauche) et visualiser les zones endommagées résultantes des points d'impact en face arrière du gilet (Figure 6- milieu), dont les empreintes des cônes de déformation du gilet peuvent être mesurées sur la plastiline de la cible de type Roma n°1 ayant une résilience sous déformation dynamique quasiment identique à celle de la chair humaine[26] (Figure 6- droite).

Les résultats des tirs balistiques ont montré que 5 tirs sur 6 ont été stoppés à différentes valeurs du nombre de couches de tissus pour différentes vitesses d'impact mesurées, et ont permis de mesurer les profondeurs de pénétration ainsi que le diamètre à la base du cône de déformation du tissu en face arrière du gilet sur la plastiline (Tableau 3).

(25) B.P. Kneubuehl and M.J. Thali, "The evaluation of a synthetic long bone structure as a substitute for human tissue in gunshot experiments," Forensic Science International, vol. 138, no. 1–3, pp. 44–49, 17 December 2003.

(26) L. Tong, A-P. Mouritz, and M-K. Bannister, 3D fibre reinforced polymer composites.: Elsevier science, 2002.

Numéro impact	Vitesse d'impact mesurée (m/s)	Arrêt du projectile	Profondeur (mm)	Diamètre (mm)	Nombre de couches perforées
1	355	No			
2	358	Yes	21	60	2
3	352	Yes	30	70	4
4	356	Yes	32	70	4
5	351	Yes	30	60	3,5
6	362	Yes	30	70	7,5
7	358	Yes	35	45	5

Résultat des essais de tirs de balles de 9 mm FMJ RN à 350 m/s du niveau II de la norme NIJ 0101.06 et mesures des déformées dynamiques dans la plastiline Roma n°1.

La valeur moyenne de la profondeur d'impact est de 30 mm ce qui constitue une valeur bien inférieure à la valeur de la norme NIJ 0101.06 de 44 mm, montrant ainsi la capacité d'absorption d'énergie à l'impact plus élevée de cette conception de gilet pare-balles. Néanmoins, ce premier prototype de gilet adapté à la morphologie féminine nécessite de nombreuses améliorations, notamment en termes de maintien des couches de tissus sur les bords du gilet afin d'éviter les glissements des plis conduisant à la perforation du gilet lors du premier impact. Une amélioration du système de pression, appliquée sur le corps humain par le gilet, peut réduire les zones de non contact, ce qui favorise l'utilisation de la totalité de la surface du corps humain lors de l'impact et contribuerait à réduire de quelques millimètres la valeur de la profondeur de la déformée dynamique.

Conclusion sur les solutions de protection souple à l'impact

Dans le cadre des travaux de recherche menés sur les solutions de protection souple à l'impact utilisant un matériau textile seul ou couplé avec un matériau céramique, nous avons identifié différentes architectures textiles, et notamment les tissus 3D interlocks chaines, pour répondre à l'impact des diverses menaces à différentes vitesses. La solution de l'empilement de tissus 2D à base de fils de para-aramide et de fils de Nickel-Titane, positionnés en face arrière d'une partie dure en céramique, a permis de révéler la capacité d'amortissement de la structure tissée lors de multi-impacts de projectiles de type 7,62 mm non perforante (9,7 g à 838 m/s) et mono-impact d'une munition de type 7,62 mm perforante (10,8 g à 868 m/s). Cependant, les valeurs de la déformation arrière après impact se sont révélées supérieures à 44 mm, et donc non conformes aux valeurs requises par les niveaux III et IV de la norme NIJ 0101-06. Pour une menace de type balle de 9 mm FMJ RN à 350 m/s du niveau II de la norme NIJ 0101-06, la solution d'assemblage par couture des différentes plastrons de tissu 2D à base de fils para-aramides a permis d'y répondre, tout en apportant une solution d'adaptation d'un gilet pare-balles à la morphologie

féminine. Enfin, l'hybridation de solutions textiles comprenant notamment des tissus 3D interlocks chaines à base de fils para-aramides 840 dTex a permis de répondre à la menace d'un FSP de diamètre 5,4 mm (masse 1,1 g) selon la norme STANAG 2920 à une vitesse V50 de 575,9 m/s (supérieure à la valeur de référence de 550 m/s). Par contre, la valeur de la déformation arrière après impact de la solution textile obtenue est de 32,1 mm (valeur supérieure à l'objectif initial de 25 mm) ce qui tend à montrer la difficulté à identifier des solutions ayant des capacités d'absorption de l'énergie d'impact, tout en ayant une capacité de déformation dynamique limitée, pour minimiser la hauteur de pénétration autorisée de l'ensemble projectile/protection souple dans le corps humain, en tant que solution de protection de type gilet pare-balles.

L'AUTEUR

BOUSSU François, professeur des universités enseigne à l'ENSAIT. Ingénieur, il a travaillé en Tunisie (société JBT) puis en France (Société Victor Machu). Il est membre du laboratoire GEMTEX. Il est un spécialiste des technologies du tissage, de la modélisation des structures tissées et des armures fondamentales (tissus 3D interlocks chaines). Outre un encadrement doctoral, il dirige des recherches à l'Université de Valenciennes et du Hainaut-Cambrésis. Il participe à des programmes de recherche nationaux, internationaux et privés. 2 programmes de recherche collectifs nationaux ont permis de concevoir un logiciel d'Analyse et d'Intégration des Données EDI pour une meilleure prévision technique et commerciale (projet AIDE) et de mettre en place une plateforme d'outils logiciels de modélisation et simulation du procédé de tissage pour matériaux composites (projet NUMTISS). 5 programmes de recherche internationaux ont permis de concevoir des structures tissées 3D interlocks chaines à base de fils thermoplastiques et à base de fils de carbone (projet MAPICC 3D), de proposer différentes solutions de protection souple pour les forces armées contre les menaces NRBC et balistiques (projet EPIDARM) et d'élaborer des matériaux textiles à base de fils de nano-tubes de carbone pour des matériaux composites à destination de l'industrie ferroviaire et aéronautique (projet IMS&CPS). Les projets INTERREG RESIST et TRITEX ont respectivement permis de créer un REseau de Soutien à l'Innovation Scientifique et Technologique pour le Textile pour le premier et proposer des modules de formation en e-learning appliqués au textile intelligent pour le second. Les 17 programmes de recherche privatifs ont permis de développer des tissus à base de fils à mémoire de forme, de définir des propriétés de mise en forme de tissus à base de fils comélés thermoplastiques (verre/polypropylène), d'étudier la protection à l'explosif et aux munitions 7.62x51mm AP WC (typeAP8) des véhicules blindés ainsi qu'analyser et comprendre le comportement dynamique de nouvelles solutions de protection soumises à un effet de souffle.

Le flair des chiens
policiers est fiable

par SOPHIE MARCHAL et BARBARA FERRY

L'odorologie est une technique d'identification mise en œuvre dans les enquêtes criminelles et délictuelles par la Direction Centrale de la Police Judiciaire (Sous-direction de la police technique et scientifique, [SDPTS]) à Ecully depuis 2003. Elle permet, grâce aux capacités olfactives de chiens spécialement entraînés, de démontrer la présence de l'odeur d'un individu sur une scène d'infraction. Si cette science a initialement pu susciter quelques interrogations parmi certains enquêteurs ou magistrats, l'analyse par le CNRS des résultats obtenus depuis 2003 permet aujourd'hui de démontrer qu'à l'issue des deux premières années de formation, les chiens atteignent un taux de spécificité olfactive de 100 % : ils ne commettent aucune erreur dans la reconnaissance des odeurs individuelles. Cette étude a été publiée le 10 février 2016 dans la revue scientifique PLOS ONE.

BARBARA FERRY

Chargée de recherche
CNRS
Centre de Recherches en Neurosciences Lyon

SOPHIE MARCHAL

Ingénieur chargé de la veille scientifique
SCIJ/Groupe Odorologie
Sous-Direction de la Police Technique et Scientifique
Direction Centrale de la Police Judiciaire

Contexte scientifique et historique

Le groupe odorologie a été créé en 2000 au sein de la Direction Centrale de la Police Judiciaire (Sous-Direction de la Police Technique et Scientifique, SDPTS à Ecully) ; c'est le seul laboratoire en France qui applique depuis 2003 la technique de l'odorologie importée de Hongrie.

L'odorologie est une technique de criminalistique permettant de comparer et d'identifier des odeurs humaines à l'aide de chiens spécialement formés. L'objectif est d'identifier des auteurs ou victimes d'infractions criminelles ou délictuelles aggravées, qui ont pu laisser sur la scène de crime ou sur un objet leur trace odorante, au même titre que leur ADN ou leur trace digitale. Ainsi, l'odeur prélevée sur l'objet ou sur la scène de crime est comparée à l'odeur d'un suspect.

L'odorologie permet également d'établir un lien entre deux scènes d'infractions (même odeur prélevée sur les deux scènes) ou d'identifier l'odeur d'une victime (dans le coffre d'une voiture par exemple, pour caractériser la séquestration). Elle est aussi utilisée pour déterminer le rôle des différents protagonistes d'une affaire : l'odeur de l'un peut être prélevée sur le siège conducteur d'une voiture par exemple, l'autre sur le siège d'où les témoins ont vu que les tirs étaient émis.

Telle qu'elle est pratiquée au sein de la SDPTS, cette technique repose sur une identification indirecte, c'est-à-dire que les odeurs humaines sont prélevées sur des supports (tissus) permettant d'éviter toute subjectivité des chiens vis-à-vis d'un objet ou d'un individu, et de conserver les odeurs humaines pendant de longues périodes (au moins 10 ans) ce qui permet de réaliser des comparaisons ultérieures.

Récemment, la communauté scientifique a validé la qualité des procédures de formation par la publication des données obtenues depuis 2003 au sein de la SDPTS (Marchal et al., 2016).

Méthodes

L'odorologie repose d'une part, sur le fait que chaque individu possède une odeur qui lui est propre et unique (Curran et al., 2007) et d'autre part, sur le principe de Locard, selon lequel « *nul ne peut agir avec l'intensité que suppose une action criminelle sans laisser des marques multiples de son passage* » (Locard, 1940). Si le principe d'échange de Locard a été appliqué depuis de nombreuses années pour prélever des fibres de vêtements, des traces papillaires et biologiques, il permet aussi de prélever des odeurs sur des objets présents sur la scène d'infraction selon une technique très précise.

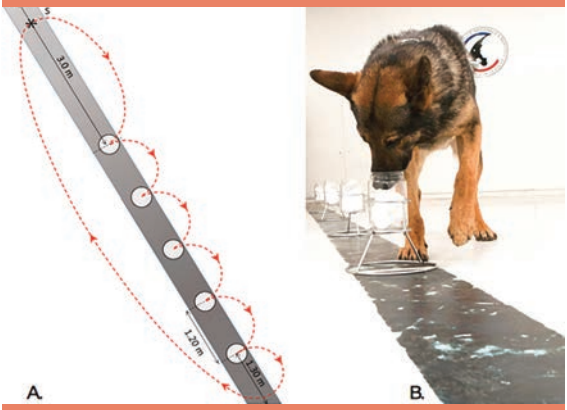
Les odeurs humaines sont prélevées à l'aide de tissus spécifiques, présentant des caractéristiques particulières permettant de capter, conserver et restituer les odeurs humaines. Il existe deux types de prélèvements :

- les Traces odorantes (TO), qui sont collectées sur les scènes d'infraction ou sur les objets potentiellement manipulés par l'auteur par apposition des tissus spécifiques sur les supports à prélever,

- les Odeurs corporelles (OC), qui sont collectées suite à la manipulation des

tissus par un individu. Tous les prélèvements sont effectués par des techniciens spécifiquement habilités par la SDPTS-DCPJ répartis sur l'ensemble du territoire national. Ces prélèvements sont ensuite adressés à la SDPTS à Ecully, où ils sont conservés dans des conditions particulières.

Les chiens sont des Bergers Allemands et des Bergers Belges Malinois, sélectionnés pour leurs capacités olfactives, leur endurance au travail et leur motivation. Ils sont formés au sein du groupe odorologie de la SDPTS par des maîtres de chiens qualifiés par le Centre national de formation des unités cynotechniques de la Police nationale.



Représentation de la salle de travail.
A : schéma de la ligne sur laquelle les chiens se déplacent pour flairer chaque bocal. Le point S symbolise le point de départ où le bocal contenant l'échantillon est présenté à l'animal. Lorsqu'il a flairé l'échantillon, il est libre de parcourir la ligne (selon la ligne fléchée pointillée rouge) sur laquelle sont placés les cinq bocaux contant les odeurs de comparaison.

La tâche d'identification d'odeurs humaines se base sur des principes de conditionnement opérant, dont l'acquisition se déroule en cinq phases de dressage du chien :

Phases de 1 à 3
le chien acquiert les comportements de flairage (bocal échantillon présenté en début de ligne (point S) et 5 bocaux successifs disposés sur la ligne - voir Figure) et d'expression d'une réponse conditionnée : il se couche devant le bocal contenant la récompense. Lorsque le chien montre 100% de réponses correctes il peut entrer en phase 4. La moyenne du nombre total d'essais pour effectuer les trois phases est 363 ± 25, soit 10 à 11 semaines de formation.

Phase 4
Le chien apprend à reconnaître la présence d'une odeur humaine et à se coucher devant le bocal qui contient l'odeur correspondant à l'échantillon. Une réponse correcte, récompensée, est notée « Vrai Positif » ou Hit. Lorsque le chien ne s'arrête pas au niveau de l'odeur cible, la réponse est notée « Faux Négatif » ou Miss. Le nombre de Hit et de Miss, pour chaque session et pour chaque chien, est comptabilisé pour

calculer le score de reconnaissance selon la formule : nombre de Hits / nombre total d'essais. Les chiens atteignant le critère de 95 % de reconnaissance sur 20 essais consécutifs peuvent passer en phase 5. La moyenne du nombre total d'essais pour atteindre ce critère est de 226 ± 30, soit 6 semaines de formation.

Phase 5

Le chien apprend à mémoriser, comparer et identifier une odeur humaine parmi cinq témoins. Cette phase correspond à l'acquisition de la tâche d'identification.

Trois types de combinaisons sont utilisés pour la comparaison des odeurs humaines :

- OC/OC correspond à une OC en échantillon et une OC dans la ligne,
- OC/TO correspond à une OC en échantillon et une TO dans la ligne,
- TO/OC correspond à une TO en échantillon et une OC dans la ligne.

Des lignes à vide, ne contenant pas l'odeur cible sont testées de manière aléatoire au cours des essais. Lorsque le chien ne s'arrête pas au cours de ces essais, la réponse, récompensée, est notée « Vrai Négatif » ou *Correct Rejection* (CR). S'il se couche devant le bocal contenant une odeur différente de celle présentée en échantillon, sa réponse est notée « Faux Positif » ou Fausse Alarme (FA). Le nombre d'essais avec une réponse CR et FA pour chaque session et pour chaque chien est utilisé pour calculer le score de spécificité d'identification olfactive selon la formule : CRs / (CRs + FAs). Les chiens qui atteignent le critère de 100 % de spécificité sur 100 essais consécutifs (12 sessions, soit 2 à 3 semaines de formation) peuvent passer en phase d'entraînement continu. L'obtention d'un score de 100% sur cette durée suggère que le chien a parfaitement acquis les règles de la tâche d'identification et ne fait plus d'erreur. La moyenne du nombre d'essais nécessaires pour atteindre ce critère et de 377 ± 57, soit 9 à 10 semaines de formation.

Lorsque le chien a validé les 5 étapes de sa formation initiale, il suit une formation continue tout au long de son activité afin de maintenir et améliorer ses compétences de mémorisation et d'acuité olfactives.

Entraînement continu : la procédure est similaire à celle décrite en phase 5 mais une combinaison de comparaison d'odeur supplémentaire est utilisée : TO/TO qui correspond à une TO en échantillon et dans la ligne. Seuls les chiens qui ne montrent pas de FA sur les 200 derniers essais de l'entraînement continu peuvent entrer dans le programme judiciaire d'identification.

Test d'identification judiciaire (affaires) : avant chaque test d'identification judiciaire, les performances des chiens sont évaluées lors d'un test d'aptitude au

cours duquel le chien doit effectuer trois essais selon une procédure similaire à l'entraînement continu. Les aptitudes de tous les chiens sont testées avec cette procédure avant chaque affaire et seuls les animaux qui montrent un score de 100 % de réponses correctes selon le calcul : (CRs + Hits) / total, peuvent effectuer le test d'identification judiciaire.

La procédure pour ce test est similaire à celle utilisée lors de l'entraînement continu mais seules 3 types de combinaisons d'odeurs sont présentés à l'animal (compte tenu du fait que les traces olfactives prélevées sur la scène d'infraction doivent être comparées à l'odeur de l'individu suspecté) :

– TO/OC (79% des affaires)
– OC/TO (20% des affaires)
– TO/TO (1% des affaires)

Dans le cas où le chien identifie l'échantillon comme étant identique à l'odeur cible placée dans la ligne, le test est effectué au moins une seconde fois, après avoir modifié l'ordre de placement des bocaux de la ligne. De plus, le chien devra effectuer au moins une ligne à vide. Un deuxième chien devra venir confirmer cette identification selon le même protocole (une ligne à vide, deux lignes contenant l'odeur cible) pour que l'identification soit considérée comme formelle par le maître-chien qui rédigera en ce sens un rapport d'identification transmis à l'enquêteur ou à l'autorité judiciaire.

Dans le cas où il n'y a pas d'identification, l'essai est noté comme Miss et le test est considéré comme étant négatif. Une absence d'identification peut signifier que les odeurs ne correspondent pas ou que la qualité ou la quantité de l'odeur prélevée n'est pas suffisante pour donner lieu à une reconnaissance. Dans tous les cas, le chien ne s'arrête jamais devant une odeur différente de l'échantillon. Les données traitées sur 10 années de formation initiale et continue, et de test d'aptitude (plus de 28200 données) ont été exploitées.

Des résultats probants

Spécificité de reconnaissance olfactive lors de l'entraînement continu

Périodes	Scores de spécificité (±S.E.M.) [CRs / (CRs + FAs)] ↑ 100	Nombre de FP sur l'ensemble des essais
1re	100	0
2nde	98.43 ± 1.22	4 (/2403)
3me	99.12 ± 0.88	2 (/2346)
4me	100	0
5me	99.00 ± 1.00	1 (/1996)
6me	99.23 ± 0.77	1 (/1850)
7me	100	0
8me	100	0
9me	100	0
10me	100	0

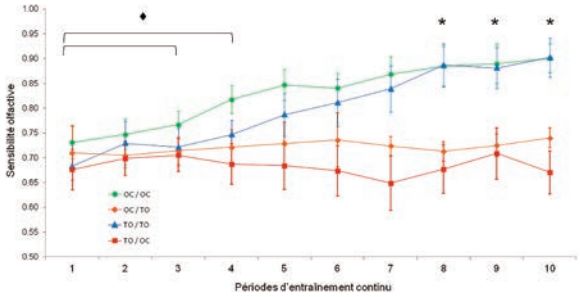
Moyenne des scores de spécificité olfactive calculés pour chacune des périodes de l'entraînement continu selon la formule : CRs / (CRs + FAs).
Chaque période correspond à une moyenne de 193.5 ± 2.7 essais effectués par chien.

L'analyse des données du tableau montre qu'à l'issue des 6 premières périodes, les chiens ne commettent plus de faux positif. Aussi, il est intéressant de constater que la totalité des faux positifs en entraînement a été commis par des bergers malinois et en particulier par un chien. Mis à part ce chien, qui n'a été admis à effectuer les identifications dans les affaires opérationnelles que très tard, l'ensemble des bergers allemands ont atteint le critère de 100 % de spécificité de reconnaissance olfactive (= le chien ne fait plus d'erreur) dès la première période de l'entraînement continu.

Sensibilité de reconnaissance olfactive lors de l'entraînement continu

Les résultats des analyses statistiques montrent que la sensibilité olfactive (= taux d'identification) des chiens augmente avec le nombre d'entraînements et que les scores de sensibilité pour les combinaisons OC/OC et TO/TO (0.9 ± 0.03 et 0.9 ± 0.04 respectivement) sont significativement meilleurs que ceux obtenus pour les combinaisons TO/OC et OC/TO (0.67 ± 0.04 et 0.74 ± 0.02 respectivement) au cours des trois dernières périodes. Ces résultats suggèrent que 1) la sensibilité olfactive des chiens augmente avec les entraînements, 2) que le type de combinaison influe sur la qualité des scores ; les identifications étant meilleures lorsque la nature des odeurs présentées en échantillon et dans la ligne est la même.

De manière très intéressante, les combinaisons utilisées lors des tests d'identification officiels sont de type TO/OC (79 % des cas), OC/TO (20 % des cas) ou TO/TO (1 % des cas). Or, nos données montrent que la sensibilité olfactive est significativement supérieure dans le cas où la nature des odeurs



Les différents scores de sensibilité olfactive obtenues pour chacune des périodes de l'entraînement continu selon la formule [Hits / [Hits + Miss]) en fonction des différentes combinaisons d'odeurs ont fait l'objet d'une analyse de variance à deux facteurs (Type de combinaison × Période) avec mesures répétées (programme SYSTAT 12.0®). Les comparaisons intergroupes ont été ensuite réalisées avec une analyse à un facteur suivie par une analyse Fisher post-hoc. Le seuil de significativité a été fixé à 0.05.
* Indique $P < 0.05$ entre les courbes OC/OC et TO/TO et les deux autres pour les périodes 8 à 10. Comparaison intragroupe : ◆ indique une progression significative des performances entre les périodes 3 (OC/OC) et 4 (TO/TO) et les autres.

présentées en échantillon et dans la ligne est similaire. Dès lors, il apparaît que l'utilisation de la combinaison TO/TO devrait être préférentiellement utilisée dans le futur. Une évolution du protocole est en conséquence actuellement à l'étude à la SDPTS (préconisation d'un prélèvement de TO du mis en cause, et non pas de son OC), qui devrait conduire à une augmentation du nombre d'identifications judiciaires.

Malgré les performances démontrées scientifiquement de détection et de reconnaissance olfactive des chiens du groupe odorologie de la SDPTS-DCPJ, et la stricte application de protocoles et procédures validées et éprouvées, il subsiste encore parfois une méconnaissance de cette technique d'identification. En montrant que les chiens entraînés selon le protocole de la SDPTS-DCPJ ne commettent aucune erreur de reconnaissance, l'étude menée par le CNRS et le groupe odorologie prouve que ces procédures de formation et d'entraînement continu conduisent à des performances d'identification fiables et reproductibles qui pourront être considérées par tous les magistrats comme des éléments de preuve scientifiques ayant fait l'objet d'une validation formelle par la communauté scientifique, au même titre que les identifications des empreintes papillaires ou d'ADN.

Entre 2003 et 2016, l'odorologie a été utilisée dans 522 procédures à la SDPTS-DCPJ, et a permis de résoudre 162 affaires judiciaires.

LES AUTEURES

Barbara FERRY est chargée de recherche en neuroscience fondamentale spécialisée dans l'étude des processus à la base des troubles cognitifs observés dans certaines atteintes neurodégénératives de type Alzheimer. Les travaux qu'elle a menés au sein du CRNL sur l'implication des structures cérébrales dans la mémoire des odeurs lui ont permis de publier 72 articles et résumés dans des revues à comité de lecture international, de publier 3 ouvrages, et de présenter ses résultats lors de 90 congrès nationaux et internationaux depuis 1997.

Sophie MARCHAL, ingénieur de police scientifique, est chargée de la veille technologique et de la mise en place de la charte qualité au sein du groupe odorologie de la Sous-Direction de la Police Technique et Scientifique (SDPTS) de la Direction Centrale de la Police Judiciaire (DCPJ). Les travaux qu'elle a menés ont abouti à un premier article et à plusieurs communications.

La LAPI : le « filet numérique »
des flux et des territoires

par JEAN-FRANÇOIS FERAY

Présente au sein des services et unités de la police et de la gendarmerie nationales, et des services de la douane depuis 2009, la LAPI (Lecture automatisée des plaques d'immatriculation) est une technologie qui a fait ses preuves en matière de lutte contre la délinquance. Capable de lire des plaques d'immatriculation d'un flux de circulation en temps réel et de confronter ces lectures avec des bases de comparaison (Fichier des objets et véhicules signalés – FOVES et Système d'Information Schengen – SIS), ces systèmes permettent une réaction opérationnelle immédiate une fois les opérations de levée de doute réalisées par l'opérateur. Ils sont le plus souvent embarqués dans des véhicules de patrouille sérigraphiés ou banalisés, qu'ils soient fixes ou nomades.

JEAN-FRANÇOIS FERAY

Lieutenant-colonel de gendarmerie
Chef de la division de l'administration des applications judiciaires
Service Central de Renseignement Criminel

La lutte contre la délinquance utilisant les voies de communication est la mission séculière de la gendarmerie nationale. Ces outils, puissants et efficaces, constituent également pour leurs détracteurs un moyen de contrôle généralisé de la population, ce qui ne saurait être toléré dans un État de droit respectueux des libertés individuelles. L'acquisition, la conservation et l'analyse des données à des fins judiciaires ou administratives doivent ainsi répondre à un cadre juridique contraignant protecteur des libertés individuelles.

La LAPI : un outil bivalent

Il est difficile d'attribuer un qualifiant unique à la LAPI, en ce sens qu'elle permet d'obtenir deux effets visant le même objectif - la lutte contre la

délinquance - mais selon deux modes d'action distincts.

Le premier est l'interpellation immédiate des occupants d'un véhicule signalé dans les bases de comparaison FOVES et SIS. Dans ce cas, après une phase indispensable de levée de doute visuelle pour éviter les erreurs de lectures inhérentes à la technologie OCR[1] et aux déformations liées aux conditions ambiantes, l'interpellation peut se dérouler en respectant les règles de l'art en matière de sécurité et d'intervention professionnelle. Les lectures ayant donné lieu à un rapprochement positif sont conservées dans une base dédiée pour une durée d'un mois[2].

(1) Optical Character Recognition : reconnaissance optique de caractères.

(2) Article L.233-1 et L.233-2 du code de la sécurité intérieure

Le second apport est le recueil d'informations *a posteriori* dans la base de données qui permet de conserver pendant 15 jours toutes les lectures n'ayant pas donné lieu à une confrontation positive avec les bases de comparaison. Ce délai est celui de la flagrance, fixé par le législateur[3]. En apparence très court, ce délai s'avère supérieur à ceux que connaissent certains de nos homologues comme les Néerlandais qui, bien qu'équipés d'un réseau de capteurs fixes et mobiles des plus dense en Europe, n'ont pas cette faculté juridique. Ainsi, toutes les lectures, qu'il s'agisse de véhicules recherchés ou non, sont conservées et accessibles aux enquêteurs, directement ou par l'intermédiaire d'une réquisition judiciaire en fonction de la finalité retenue[4]. Il est donc aisé de suivre un véhicule sur l'ensemble du maillage de capteurs fixes ou mobiles : c'est tout l'intérêt de la LAPI.

(3) Id. 2

(4) Les finalités de la LAPI sont la lutte contre le terrorisme, les trafics de stupéfiants, la criminalité organisée, les vols et recels de véhicules, la contrebande et l'ordre public (finalité administrative).

Un outil qui nécessite une intervention humaine pour valider les rapprochements de bases de données.

La collecte de données, et après ?

Outre l'interpellation en temps réel, la LAPI offre la possibilité d'opérer des analyses à finalité judiciaire pour rechercher des véhicules de suspects, de témoins, voire de victimes d'infractions. À travers la recherche d'une plaque, mais également d'une marque, d'un modèle, d'une couleur, d'une catégorie de véhicule, l'enquêteur a la possibilité de croiser des données issues de plusieurs traitements de données pour réduire une masse considérable en une masse pertinente, et humainement exploitable. Ces procédés d'analyse de

données issues de la LAPI rappellent quelque peu les difficultés rencontrées en matière de données de téléphonie fixe ou mobile, ou d'analyse de flux financiers. Après une phase de mise en forme des données vient le rapprochement entre plusieurs bases de données (SIV[5], EUCARIS[6], ADOC[7], autres bases). Ceci nécessite l'utilisation de logiciels de rapprochement criminel, dont l'utilisation n'est possible qu'après accord d'un magistrat[8]. Il y a de fait une contrainte majeure entre le temps nécessaire à l'exploitation des données et l'urgence des situations, notamment dans le cadre d'enlèvements et séquestrations ou d'actes de terrorisme. La célérité avec laquelle ces données doivent être traitées est un impératif de succès de l'enquête voire de l'intégrité physique des personnes. Un des enjeux du traitement des données issues de la LAPI sera donc la définition de modes opératoires consolidés, permettant aux analystes criminels d'apporter une réponse la plus précise et rapide possible. Ce qui a été rendu possible pour la téléphonie et les comptes bancaires devra l'être pour ce type de données.

(5) Système d'Immatriculation des Véhicules

(6) EUropean CAR Identification System

(7) EUropean CAR Identification System

(8) Article R.40-40 du CPP

Le dimensionnement du maillage et la manœuvre LAPI

Soldat infatigable, le capteur LAPI est une « sonnette » qui ne dort jamais et qui donne l'alerte de manière continue : il faut donc intégrer ce « bavard » dans une manœuvre permanente ou conjoncturelle, autour de deux modes d'action, le rideau de surveillance et d'interception ou le poste de surveillance depuis un point ou sur un axe. Outil de renseignement opérationnel et criminel issu des capteurs, la manœuvre LAPI ressort de ce que le monde du renseignement appelle communément le SIGINT ou ROEM[9]. Cette intégration du LAPI dans la manœuvre de renseignement ou d'interception est relativement récente. Certains groupements de gendarmerie sont bien en avance sur le sujet comme le GGD 59 qui a mis en œuvre une cellule d'investigation LAPI (CI-LAPI) qui apporte au commandement de groupement une gestion centralisée de ses capteurs mobiles, en plus de capteurs fixes implantés soit sur les axes majeurs (autoroutes) ou autour de points sensibles (centrales nucléaires, installations de défense). Dans certaines situations opérationnelles, la collecte de renseignement sur les axes routiers est déterminante dans la résolution des affaires judiciaires (vols à main armée, enlèvements, séquestrations, cambriolages) et elle doit être orientée et intégrée dans une manœuvre plus globale, intégrant des patrouilles mobiles, des points de barrage, la participation citoyenne et sa mobilisation *via* les réseaux sociaux.

(9) SIGINT : Signals Intelligence. ROEM : renseignement d'origine électro-magnétique.

La multiplication des capteurs fixes et mobiles constitue donc une couche supplémentaire dans la cartographie opérationnelle des échelons territoriaux de commandement et des unités de

La technologie LAPI s'insère dans un dispositif territorial coordonné

recherches. À l'échelle du ministère de l'intérieur, une réflexion est menée sur la stratégie d'implantation des capteurs fixes, en complément de ceux déjà mis en œuvre par la direction générale des douanes et des droits indirects qui dispose quant à elle de son propre maillage.

Les échanges internationaux de données : un enjeu stratégique pour la sécurité de l'espace Schengen

Le moins que l'on puisse dire, c'est que l'Europe avance en ordre dispersé sur le contrôle des flux *via* la LAPI. Si la Grande-Bretagne fait figure de leader dans le domaine, tant sur les équipements que sur l'analyse des données, les autres nations ne suivent pas la dynamique de manière univoque. Les axes routiers permettent de circuler de la mer Noire à l'océan Atlantique, mais les contrôles restent encore nationaux et les échanges rares. Deux leviers peuvent améliorer la situation existante :

– une infrastructure répondant à un schéma de contrôle des flux à l'échelle européenne,

– des normes communes pour le traitement des données de lecture.

En effet, la directive 95/46/CE étant commune à l'ensemble des États membres, l'échange de données entre ces pays ne pose aucun problème juridique[10]. En revanche, l'absence de standardisation du format de données captées puis exportées peut ralentir la capacité de traitement par les enquêteurs ou les services de renseignements.

(10) L'article L.235-1 du code de la sécurité intérieure prévoit ces échanges de données.

À l'heure où les questions de terrorisme, de criminalité organisée et de migrations de masse font débat dans la société civile européenne, l'Europe doit être en mesure d'apporter une réponse coordonnée face à des flux menaçant la stabilité de l'espace communautaire. Le Système d'Information Schengen offre actuellement un partage efficace des informations relatives aux biens et aux personnes signalées. Ce support technico-juridique est à n'en pas douter le système le plus efficace pour partager des données entre États membres, au sein de l'espace Schengen.

Les risques autour de la LAPI.

La technologie LAPI présente plusieurs risques bien identifiés pour lesquels des parades sont nécessaires. La confidentialité des données : Les capteurs LAPI amassent une quantité de données considérable, sans discriminer *a priori* s'il s'agit d'un véhicule recherché ou non, la comparaison étant différée. Le risque majeur est une utilisation détournée des données en dehors des finalités du

traitement, pour des raisons personnelles étrangères au service. Seules des procédures internes de contrôle sur la traçabilité, impliquant notamment l'inspection générale de la gendarmerie nationale et les chefs hiérarchiques peuvent permettre de limiter le risque, sans pour autant le réduire à zéro.

La qualité des données : C'est un aveu un peu cinglant, mais la vraie intelligence du LAPI ne réside pas dans son capteur ni dans sa base de données, mais dans la qualité de la base de comparaison et dans la qualité du lecteur optique OCR. Pour pouvoir fonctionner de façon optimale, LAPI a besoin d'une base de données de comparaison d'une très grande fiabilité, dont les données sont exactes, complètes et mises à jour, pour paraphraser l'article 6 de la loi informatique et libertés[11]. On serait pour le moins gêné d'interpeller le propriétaire légitime d'un véhicule automobile car le FOVES ou le SIS comporte des données non mises à jour. L'exactitude de la base de données est donc un enjeu majeur. De la même manière, un capteur dont les performances seraient en deçà d'un niveau acceptable d'erreur engendrerait un nombre de faux positifs tel qu'il perdrait toute sa crédibilité.

(11) Loi n° 78-17 du 6 janvier 1978 modifiée.

Le suréquipement : En matière de LAPI, le plus est bien souvent le pire ennemi du bien. Les Pays-Bas se sont dotés d'un maillage très serré de capteurs, sur un tout petit territoire et relié à un nombre très important de bases de comparaison. Au final, il ressort que le système produit tellement d'alertes qu'elles ne peuvent pas être prises en compte en raison du « bruit » qu'elles produisent, rendant le système malheureusement peu efficace.

La LAPI est un moyen formidable de captation de renseignement d'intérêt criminel. À l'heure du big data, elle offre des potentialités importantes dans le cadre des investigations judiciaires. Son utilisation entraîne cependant certaines limites juridiques ou techniques qui nécessitent une intervention humaine indispensable pour fiabiliser les résultats. Elle offre également une capacité de manœuvre nouvelle aux chefs opérationnels, qu'ils doivent l'intégrer dans leurs modes d'action. Sans aller vers un *big brother* européen, la normalisation et le partage des données issues des capteurs LAPI sont un réel enjeu à l'échelle européenne dans l'espace Schengen. Le filet numérique des flux et des territoires se met progressivement en place dans l'espace de liberté, de sécurité et de justice.

L'AUTEUR

Le lieutenant-colonel Jean-François FERAY est un ancien élève de l'école des officiers de la gendarmerie nationale, promotion SLT Foulon (1998-2001). Licencié en droit, diplômé en criminalistique et en gestion de crise, il a exercé des responsabilités opérationnelles en gendarmerie départementale à Beaune (21) et à Abbeville (80). Après un passage à l'IRCGN de 2008 à 2011, il intègre la 19e promotion de l'école de guerre. Il est chef de la division de l'administration des applications judiciaires au Service central de renseignement criminel de Pontoise depuis le 1er août 2012.

TECHNIQUES DE RECONNAISSANCE

Fotolia - Annett Seidler

LA RECONNAISSANCE FACIALE EST UNE TECHNOLOGIE ENCADREE

En matière de sécurité, les nouvelles techniques appliquées à la reconnaissance faciale touchent essentiellement à la détection d'intrusion, la surveillance de foule ou le suivi de personnes dans les transports collectifs. Leur mise en œuvre nécessite un encadrement complexe. On ne peut envisager une absence d'information du public du fait du caractère substantiel de la capture des caractéristiques d'un individu et de ses pérégrinations. Les solutions juridiques retenues doivent satisfaire un impératif de sécurité et la protection des libertés individuelles. Sur un plan purement technique, les normes doivent être de haut niveau pour garantir une exploitation des données fiables et susciter une réponse opérationnelle en temps réel. Ces technologies posent essentiellement les problématiques de la fiabilité des algorithmes qui traitent l'image, de la protection des zones de stockage et de l'habilitation légale et réglementaire des opérateurs.

Reconnaissance faciale
et sécurité

par JEAN-MARC JAFFRÉ

L'utilisation de l'image d'un visage pour la reconnaissance et l'identification d'individus est d'actualité dans le domaine de la sécurité particulièrement sous tension depuis quelques mois. La conjonction des besoins de contrôles et des capacités croissantes du numérique dans le domaine de l'imagerie ouvre de nouvelles perspectives en la matière.

La reconnaissance faciale est le traitement automatique d'images numériques qui contiennent le visage de personnes. C'est une technologie biométrique dont le principe est simple : un capteur « saisit » un visage, le transforme en données numériques pour le comparer à une base de données, ces deux dernières opérations étant réalisées par un algorithme. L'image d'une personne, plus particulièrement celle du visage, touche à l'intime bien plus peut-être qu'un code-barres identifiant un ADN. Sa reproduction, sa détention par un tiers et sa comparaison ne peuvent se faire sans une acceptation de la société. Dès 2012, l'Union européenne formulait des recommandations sur l'emploi de cette technologie[1], notamment en matière de protection des données à caractère personnel. Le constat est pourtant sans appel, c'est une technologie qui se développe mais qui révèle certaines limites.

JEAN-MARC JAFFRÉ
Lieutenant-colonel de gendarmerie
Chargé de projets au Centre de recherche de l'EOGN
Référent national sciences et recherche pour le collège européen de police

(1) Avis 2012-02 du 22 mars 2012 de l'Union européenne sur la reconnaissance faciale dans le cadre des services mobiles et en ligne , Groupe de travail « article 29 » sur la protection des données.

Le « visage numérisé », une technologie mise à l'épreuve dans le domaine de la sécurité

Les technologies dédiées au « visage numérisé » sont fortement opportunes

Fotolia : Kentoh

L'encadrement juridique de l'emploi des images numérisées utiles à l'identification d'individus est un enjeu majeur de libertés individuelles.

dans le cadre de la recherche et l'identification de personnes. Le contexte de la sécurité s'inscrit dans le mouvement d'accélération qu'impose le numérique. Les usages relèvent soit d'une phase d'anticipation ou de préparation d'événements soit d'une phase d'investigation. Dans cette dernière, il s'agit de comparer l'image captée avec une base de données pour repérer une personne qui fait l'objet d'un intérêt particulier. Dans une phase préventive et en temps réel, le but est de révéler un indicateur, prenant la forme de comportements anormaux, afin d'empêcher la survenue d'un trouble ou désordre qui nécessiterait une réaction des forces de sécurité.

La reconnaissance faciale est déjà utilisée par certaines forces de sécurité. La police de Calgary, au Canada, était la première force de police à faire usage de cette technologie. Aux États-Unis, le *Federal bureau of investigation* dispose de l'outil Next Generation Identification Program qui utilise les fichiers nationaux et les médias sociaux pour construire une base de données de plus de 52 millions de personnes. Les polices de Chicago, New York, Seattle, San Diego, Dayton Beach ou d'Hawaï ont investi dans ces moyens techniques proposés par *Neoface Reveal* de Nec ou Morpho. Intégrée dans des programmes qui visent principalement à lutter contre le phénomène des gangs, la reconnaissance faciale devient un outil d'une stratégie de sécurité. Fin 2015 et pour un budget de 18,5 millions de dollars, le gouvernement australien lançait le programme Capability pour lutter contre le terrorisme et la délinquance transfrontalière.

En Inde, la ville de Surat a combiné l'application *NeoFace Reveal* de Nec avec son système de vidéosurveillance pour procéder en temps réel à la

reconnaissance faciale. Avec le même objectif, la ville de Buenos Aires a modernisé son système de vidéosurveillance en améliorant l'éclairage de ses rues afin d'obtenir une qualité d'image supérieure et faciliter ainsi le travail de reconnaissance faciale. Dans certains aéroports européens (Belgique et Allemagne), des systèmes de reconnaissance faciale ont été mis en place. Dans le sas du dispositif appelé e-gate, un capteur prend une photo du voyageur qui est comparée aux documents d'identité. Dès 2016, Aéroports de Paris va expérimenter ce système dans le cadre du traitement Parafe[2] (Passage rapide aux frontières extérieures).

(2) https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022960056 et https://www.service-public.fr/particuliers/actualites/A10544

Le monde de la recherche s'est aussi très investi dans la reconnaissance faciale. Ainsi, le projet européen *Secur-ed* (*SECured URban transportation-European Demonstration*)[3] aborde la reconnaissance faciale au même titre que la détection d'intrusion, la surveillance de foule ou le suivi de personnes dans les transports collectifs. Des projets comme Methodeo (Méthodologie d'évaluation des algorithmes d'exploitation des enregistrements de la vidéoprotection) de Thales ou Physionomie (Rapprochement physionomique à des fins d'investigation) de Morpho se concentrent dans la phase judiciaire sur l'exploitation des images de visages et sur la qualité des algorithmes d'exploitation des données. En Allemagne, le projet GES-3D (Multi-Biometrische Gesichtserkennung)[4] souligne l'intérêt de cette technologie en abordant la notion de 3e dimension pour la reconnaissance faciale. On peut également citer une application comme LISA (*Logiciel d'Identification de Suspects par Analogie*) de l'entreprise Spikenet Technology qui identifie des caractéristiques propres à des individus (parties du visage ou du corps). Avec l'appui de l'entreprise Morpho, Interpol s'implique dans la reconnaissance faciale[5] et l'intègre désormais dans ses domaines d'expertise forensique. En 2015, cette agence créait un groupe de travail (*Facial Expert Working Group*) avec pour objectif de déterminer des normes de qualité, de format et de transmission des images pour alimenter une base de données dès 2016 et d'être en capacité de l'exploiter en temps réel sur le terrain lors d'opérations.

(3) http://www.secur-ed.eu/

(4) https://www.igd.fraunhofer.de/Institut/Abteilungen/IDB/Projekte/Multi-Biometrische-Gesichtserkennung-GES-3D

(5) http://www.interpol.int/fr/INTERPOL-expertise/Forensics/Facial-recognition

Le visage numérisé : quelles limites ?

Les différentes expériences et outils développés ne doivent cependant pas cacher certaines contraintes. La première d'entre elles est la qualité des images. Les conditions de prise de vues, les

performances des capteurs et l'absence de normes rendent compliquée l'exploitation des images. Par ailleurs, cette technologie n'est pas nécessairement acceptée par la société. Ainsi, la police de Boston a mis un terme à l'utilisation de ce procédé à l'instar de celle d'Oakland du fait de vives réactions citoyennes. La mise en place de la reconnaissance faciale a pu se faire sans information du public. Au Royaume-Uni, ce sont des unités de police qui, sans cadre juridique stabilisé, ont alimenté une base de données (Police National Database) avec les photos de milliers d'individus prises lors des gardes à vue. L'autorité administrative indépendante britannique en charge des questions de biométrie relevait que les outils et applications n'avaient fait l'objet d'aucun test de fiabilité et d'efficacité. Cela met en valeur la nécessité d'un cadre juridique structuré.

Par ailleurs, les enquêteurs, à la recherche d'individus, n'ont de cesse de solliciter leur mémoire, celles de leurs pairs ou de citoyens, afin d'identifier ou de reconnaître des visages. Certains agents sont dédiés à ce travail notamment à l'occasion de rencontres sportives pour repérer les hooligans. Ce procédé est mis en valeur dans certaines unités de police britanniques. Ainsi en est-il des « super recognizers »[6], policiers qui ont le don de mémoriser les visages au point de les repérer dans une foule avec une efficacité supérieure à une application de reconnaissance faciale. L'humain est encore très efficace.

(6) http://www.bbc.com/news/uk-england-34544199

Il existe aussi d'autres limites à la reconnaissance faciale. Ainsi, la société AVG a expérimenté des lunettes, qui par l'utilisation de led à infrarouge ou de matériau rétroréfléchissant, atténuent considérablement la qualité de l'image captée et rendent donc inopérante la technologie. De plus, dans la construction des algorithmes de comparaison, certains biais structurels ont été mis en évidence notamment quant à l'identification de la couleur de peau ou la forme des yeux qui relève d'un outil potentiellement discriminatoire en absence de corrections. La crainte de cette technologie repose aussi sur la fiabilité des lieux de stockage des documents numérisés ainsi que leurs conditions d'accès. On peut remplacer un code PIN ou un numéro de carte volé mais, à l'instar d'une usurpation d'identité, on imagine aisément la force du préjudice d'un détournement du visage numérisé. La protection des systèmes de reconnaissance faciale est donc un enjeu majeur du déploiement de cette technologie.

Le cadre juridique est aussi et heureusement une limite. À l'échelle européenne la directive 95/46/CE sur la

protection des données s'applique aux systèmes de reconnaissance faciale. Elle s'impose à la France où les risques d'atteinte à la vie privée, à la protection des données à caractère personnel sont de véritables enjeux de société. La Commission nationale informatique et libertés est particulièrement attentive sur les évolutions des technologies de reconnaissance et la gestion qui est faite des données au regard de la finalité poursuivie par les opérateurs ou les enquêteurs. Pour autant, la technologie évolue et doit ouvrir sur des solutions juridiques satisfaisant l'ensemble des parties prenantes (État, société, forces de sécurité). Les forces de sécurité intérieure françaises ont déjà la possibilité juridique de recourir à un processus de reconnaissance faciale (article 40-26 du code de procédure pénale pour les mis en cause, les victimes décédées ou les personnes disparues) à partir de l'application de Traitement des antécédents judiciaires.

La reconnaissance faciale est donc une technologie qui a atteint une certaine maturité au point d'en faire une solution parmi d'autres pour améliorer la sécurité et répondre à divers besoins. Toutefois, le citoyen reste attaché à sa vie privée et au droit à l'anonymat quand bien même la menace est forte. Le premier enjeu du développement de la reconnaissance faciale est celui d'une éthique et de convaincre la société de l'utilité de cette technologie. Il s'agit ainsi de montrer les qualités techniques et de sécurité qu'elle offre dans un cadre juridique bien précis. Elle doit garantir le juste équilibre entre liberté et sécurité que doit illustrer tout projet de mise en place d'un tel outil. La loi doit également anticiper l'évolution de la technologie vers le « big data », l'internet des objets voire l'intelligence artificielle. Kelly Gates, de l'université de Californie, mettait en garde dès 2011 sur les risques de cette technologie[7]. Mais au final, en matière de sécurité, la reconnaissance faciale, que ce soit dans une phase préventive ou d'investigations, reste un des éléments du faisceau d'indices utiles à la décision. À « l'image » des super-recognizer, la reconnaissance faciale ne peut se passer de l'action humaine qui porte le poids de la responsabilité du choix d'intervenir ou non.

(7) Kelly Gates, 2011, Our Biometric Future, facial recognition technology and the culture of surveillance, Paperback editions

niruttt - Fotolia.com

L'ANALYSE VIDEO DEVIENT UNE DISCIPLINE MAJEURE

La force de l'analyse d'une vidéo repose sur une capacité de détecter un fait anormal, de l'isoler techniquement et de permettre une validation par des opérateurs habilités à mettre en œuvre des mesures correctives.

Un arc vertueux combine la mise en œuvre de technologies d'acquisition des événements, devant avoir une force probatoire, avec une intelligence artificielle qui puisse assurer une gestion d'un contexte en communiquant à distance et en temps réel avec un opérateur. Cette liaison devra être paramétrable pour garantir une évolutivité du système et garantir sa propre intégrité.

Cette sphère, mise en œuvre par les entreprises civiles de sécurité qui recourent à des technologies nouvelles, suscite un partage du métier de la sécurité qui, outre la distinction entre les tâches régaliennes et privées, sépare les activités des hommes de celles de machines intelligentes. Cela pose la question juridique de l'habilitation à la préhension de scènes de vie, de la destination de la donnée après sa captation et du respect des libertés individuelles dans un contexte de sécurité.

L'analyse vidéo ou l'extraction d'informations pertinentes en temps réel

par **JEAN-BAPTISTE DUCATEZ**

Pour protéger un site ou un bâtiment, de nombreuses possibilités sont aujourd'hui offertes, dont certaines sont encore parfois méconnues. Câbles enterrés, clôtures détectrices, barrières infrarouge, analyse vidéo… comment reconnaître la solution la plus adaptée et surtout, les bénéfices qu'elle procure ? Afin de comprendre les avantages de l'analyse vidéo, il est essentiel de commencer par le début et de bien comprendre son fonctionnement.

JEAN-BAPTISTE DUCATEZ

Dirigeant de Foxstream, spécialisée dans l'analyse et le traitement automatique en temps réel du contenu d'images vidéo

L'analyse vidéo, quesaco ?

L'analyse vidéo est dite intelligente car elle permet de classer les objets en mouvement (personnes, animaux, véhicules, mouvements de la végétation, *etc.*) en fonction des besoins du site client. Ainsi, on peut choisir de ne détecter que les personnes, ou les personnes et les véhicules, et de filtrer tout le reste. Afin de filtrer efficacement les objets dans la vidéo, des algorithmes puissants sont mis en place pour détecter toute intrusion avec une très grande fiabilité, tout en limitant au maximum les fausses alarmes[1]. Elles sont souvent dues au changement de luminosité ou de météo qui altèrent la finesse de l'analyse. C'est pourquoi on recommande fortement l'utilisation des caméras thermiques : bien que l'engagement financier soit un peu plus élevé au départ, le retour sur investissement se fait lors de l'utilisation puisque les problèmes de luminosité (soleil couchant, réflexion lumineuse, *etc.*) et de météo (pluie, brouillard, *etc.*) sont atténués. Cela permet d'arriver à une seule fausse alarme par semaine, soit un

(1) Une fausse alarme est une alarme remontée comme pertinente alors qu'elle ne l'est pas et aurait dû être filtrée, par exemple un chat qui passe.

Comparaison d'une même scène filmée avec une caméra couleur et une caméra thermique.

taux quasi insignifiant. L'un des principaux intérêts de l'analyse vidéo est que l'objet source de l'alarme est mis en évidence par un OSD[2], c'est-à-dire un détourage rouge de la personne ou du véhicule, ce qui évite d'avoir à chercher la source de l'alarme dans l'image et permet de l'identifier en un clin d'œil. En effet, le temps est un élément déterminant pour déclencher une intervention et appréhender les auteurs d'intrusions, c'est pourquoi l'un des objectifs majeurs est de transmettre les informations en temps réel[3] pour faciliter le travail des opérateurs de sûreté ou des télésurveilleurs, et par là-même le travail des forces de l'ordre.

(2) de l'anglais « On Screen Display » : interface utilisateur qui apparaît à l'écran d'un téléviseur ou d'un ordinateur et qui permet d'effectuer des réglages de cet écran ou bien d'un autre appareil qui lui est relié (source: https://fr.wikipedia.org/wiki/Menu_à_l'écran)

(3) La transmission d'informations en temps réel et une levée de doute immédiate fait partie de choix stratégiques de Foxstream.

La transmission rapide de l'information pertinente

Lors d'une intrusion, une alarme est déclenchée. Cette information d'alarme est envoyée automatiquement et en temps réel au télésurveilleur, accompagné du clip vidéo de la séquence pertinente où l'intrusion a eu lieu et avec le détourage rouge de l'objet source de l'alarme. Contrairement à des solutions tierces (détecteurs, barrières infrarouges, *etc.*), l'analyse vidéo permet au télésurveilleur une levée de doute immédiate puisqu'il voit, quelques secondes seulement après l'intrusion, la personne à la source de l'alarme et peut confirmer qu'il ne s'agit pas d'une fausse alarme. Aucun besoin d'aller se connecter à une caméra, de charger les enregistrements vidéo des dernières heures et d'essayer de repérer à l'œil nu ce qui a pu bouger (et à quel moment exactement) pour déclencher l'alarme. Ce fonctionnement permet l'économie d'un temps précieux pour le télésurveilleur qui est ainsi plus efficace et peut réagir de manière adéquate pour appréhender l'intrus.

En plus d'aider le télésurveilleur, le clip vidéo qui lui est automatiquement envoyé facilite le travail des forces de l'ordre puisque selon l'article L613-6 du Code de Sécurité intérieure, il constitue une preuve tangible, une levée de doute, qui autorise l'appel au 17. Les gendarmes ou policiers

qui se rendent sur place savent qu'il ne s'agit pas d'une intrusion probable mais bien réelle, preuve à l'appui. Le temps gagné dans le processus d'alerte accélère le déplacement des policiers ou gendarmes et augmente fortement la probabilité d'arrêter l'auteur du délit. Par ailleurs, les sociétés de télésurveillance utilisant ce système forment un cercle vertueux avec les Forces de l'Ordre qui, n'étant pas appelées pour rien ou trop tard, accordent leur confiance à ces prestataires et interviennent donc plus utilement sur site.

Quelles solutions pour quels sites ?

Maintenant que les bénéfices de l'analyse vidéo ont pu clairement être démontrés, il s'agit de s'y retrouver parmi toutes les différentes offres de solutions en analyse vidéo. La manière la plus simple est certainement de classer les sites selon leurs besoins. Certains sites très sensibles ou complexes nécessitent une solution permettant une analyse sur-mesure. Foxstream a par exemple équipé certains sites du ministère de l'Intérieur et de la Défense avec son logiciel d'analyse vidéo FoxVigi, permettant de relier un nombre illimité de caméras pour une analyse puissante sur serveur. Plus d'une centaine de caméras, thermiques ou couleurs sont ainsi dispersées sur plusieurs sites de ces Ministères et regroupées pour l'analyse à des fins de protection périmétrique, mais aussi de détection d'objets abandonnés. L'analyse est dite sur-mesure car elle permet une configuration très précise en termes de perspective, sensibilité, classification d'objets et offre de nombreuses possibilités annexes grâce au gestionnaire d'événements : FoxVigi permet par exemple de programmer plusieurs tâches par évènement, ou de relire un clip de détection d'intrusion en modifiant les paramètres pour voir les conséquences sur l'analyse et ainsi optimiser la détection sur un site précis.

D'autres sites recherchent une solution plus simple et rapide à mettre en œuvre, tout en restant fiable. Une solution packagée, la FoxBox, a été conçue et commercialisée dans ce but. Cette solution permet d'enregistrer, de stocker et de transmettre les alarmes et clips vidéos aux télésurveilleurs en reliant simplement ses caméras (jusqu'à 4 caméras) à la FoxBox. En moins de 5 minutes de paramétrage, la solution est prête pour l'emploi. Une solution Plug&Play dont l'objectif est de rendre accessible à tous, les performances innovantes de l'analyse vidéo. Cette solution équipe déjà des centaines de sites de logistique, d'entrepôts, de concessionnaires automobiles, etc.

Enfin, grâce aux progrès de la technologie de ces dernières années, il est désormais possible d'embarquer directement l'analyse vidéo dans les caméras. Plus besoin de serveur sur site, l'envoi du clip vidéo de l'alarme se fait simplement via un serveur ftp.

Le projet YELLOW, système embarqué de détection et d'alerte, préserve la sécurité des "hommes en jaune" et des usagers.

Recherche et projets collaboratifs

La société Foxstream travaille en étroite collaboration avec l'UMR (Unité Mixte de Recherche) LIRIS[4] du CNRS[5]. Ce partenariat est formalisé et pérennisé par une convention. Cette convention, signée par le laboratoire, l'université de Lyon, et le CNRS au niveau national, permet des échanges fructueux avec la communauté des chercheurs. Ces échanges ont permis à la société d'intervenir depuis 10 ans dans une dizaine de conférences internationales de Singapour à Las Vegas pour y présenter ses travaux, restant ainsi en contact étroit avec la recherche académique. Foxstream participe également à divers projets collaboratifs : l'un d'entre eux, confidentiel, a pour but d'aider la Police Technique et Scientifique dans des situations extrêmes et de sauver des vies. Les analyses utilisées pour ce projet sont la Détection d'intrusion, le Comptage de personnes, la Mesure de densité et la Lecture de plaques minéralogiques.

(4) Le LIRIS (Laboratoire d'InfoRmatique en Image et Systèmes d'information) est une unité mixte de recherche dont les tutelles sont le CNRS, l'INSA de Lyon, l'Université Claude Bernard Lyon 1, l'Université Lumière Lyon 2 et l'Ecole Centrale de Lyon.

(5) Le Centre National de la Recherche Scientifique (CNRS) est un organisme public de recherche (Établissement public à caractère scientifique et technologique, placé sous la tutelle du Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche).

(6) LUTB Transport & Mobility Systems est le seul pôle en Europe à centrer son action sur les enjeux des transports collectifs de personnes et de marchandises en milieu urbain, liés la croissance de la population urbaine mondiale et aux contraintes environnementales.

(7) Lles ministres en charge de la politique des pôles de compétitivité, en lien avec les présidents des Conseils régionaux et l'association des Régions de France, ont décidé le financement de 62 nouveaux projets de R&D collaboratifs pour un montant d'aide de l'Etat de 47,6 M€. 137 dossiers ont été présentés lors de cet appel à projets du FUI.

Un autre projet collaboratif est le projet « Yellow ». Labellisé par LUTB Transport & Mobility Systems[6], il a été sélectionné lors du récent 19e appel à projets du Fonds unique interministériel (FUI)[7]. En 2013 en France, près d'une centaine d'accidents se sont produits sur des chantiers d'autoroute, parfois très graves. Pour réduire fortement ce nombre, aussi bien en France qu'à l'étranger, et pour préserver la sécurité des "hommes en jaune" et des usagers, le projet YELLOW vise à créer un système embarqué de détection et d'alerte de risques de collision sur les chantiers. Les systèmes innovants prévus se décomposent ainsi :

1. Détection des véhicules entrant dans la zone de chantier ayant un fort risque de percussion. Elle sera assurée par une caméra thermique embarquée sur les équipements de balisage (flèche lumineuse

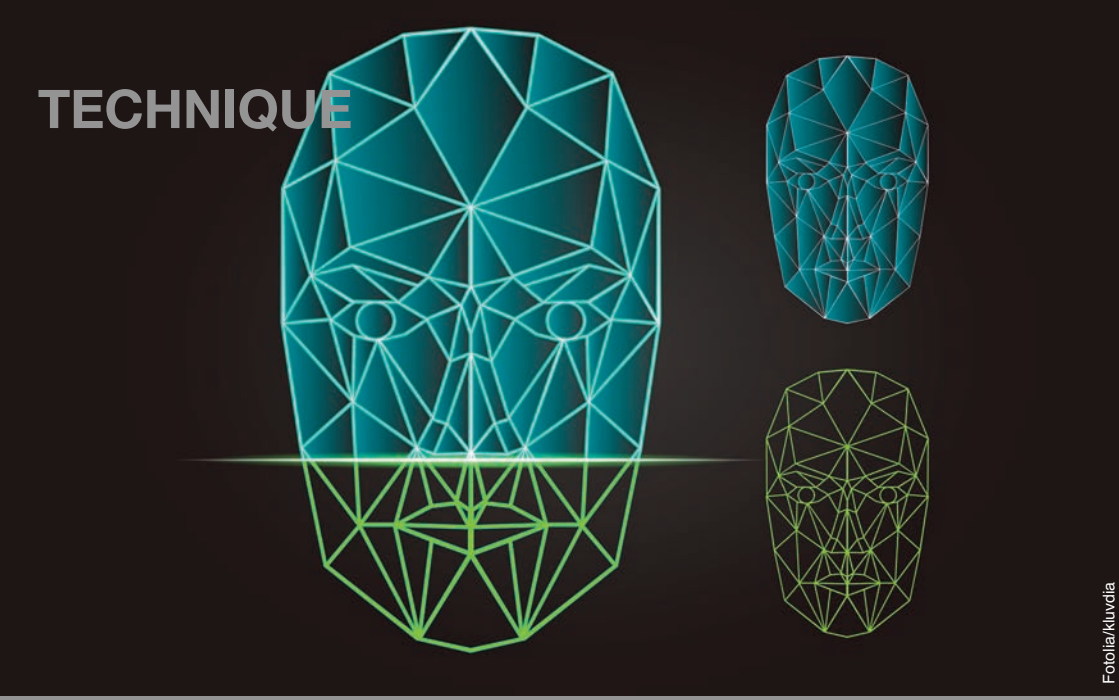
de rabattement par exemple) ainsi que par un logiciel d'analyse d'images conçu par la société Foxstream.

2. Alerte vers l'usager en approche et vers les agents de chantier.

Une campagne d'évaluation sur piste, sur simulateur de conduite et en conditions réelles sera mise en place pour tester la fiabilité et l'ergonomie des dispositifs conçus[7].

L'AUTEUR

Jean-Baptiste Ducatez a fondé la société Foxstream en 2004. Ingénieur de formation, il a ensuite étendu ses connaissances aux Etats-Unis avant de revenir en France pour encadrer une équipe d'ingénieurs internationaux. Ancien directeur technique d'une société d'édition de logiciels, il a choisi de fonder sa propre société d'édition logicielle dans l'analyse vidéo en partenariat avec le LIRIS, laboratoire de recherche associé CNRS à Lyon, pour se spécialiser dans la détection d'intrusion et la gestion des flux de personnes.



Fotolia/kluvdia

L'IDENTIFICATION ET L'AUTHENTIFICATION : DEUX PROCESSUS D'UNE CONNEXITE COMPLEXE

Une politique prenant en compte l'interaction croissante des systèmes numériques doit assurer la sécurité des transactions par une connexité maîtrisée entre les processus d'identification et d'authentification. Elle doit réduire l'incertitude liée à la qualité du croisement des données issues de capteurs biométriques et de bases de données référencées. Elle doit concourir à la sécurité des structures d'intérêt vital d'une nation et contribuer à la protection des libertés individuelles par une authentification diversifiée.

On notera que cette dernière peut être encore leurrée techniquement et que cela suscite des pratiques alternatives mais on relèvera qu'un chiffrement numérisé homomorphe empêcherait une exploitation par l'auteur d'une captation frauduleuse de données biométriques.

Biométrie
et authentification

par PHILIPPE WOLF

La biométrie est l'ensemble des technologies qui exploitent des caractéristiques humaines, physiques ou comportementales pour différencier des personnes. Elles comprennent l'analyse morphologique (l'empreinte digitale et palmaire, l'iris, la rétine, le visage, le réseau veineux, etc.), l'étude des traces biologiques (l'ADN, le sang, la salive, l'odeur, etc.) et l'analyse comportementale (la signature, la reconnaissance vocale, la démarche, un geste de la main, etc.). Nous nous concentrons ici sur son usage pour l'authentification dans les systèmes d'information qui a pour but, d'après le glossaire de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), « *de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.* »

PHILIPPE WOLF
Institut de recherche technologique SystemX (Palaiseau)

Avant d'aborder l'authentification biométrique, il peut être utile de souligner quelques progrès spectaculaires de l'anthropométrie, à savoir la mesure des corps humains à des fins criminologiques et policières, qui a débuté avec le bertillonnage, mis au point par le Français Alphonse Bertillon en 1879. Le FAED (Fichier Automatisé des Empreintes Digitales) qui comprenait 3 767 810 enregistrements en 2010 a permis, cette même année, de résoudre 13 391 affaires. Pour le FNAEG (Fichier

National Automatisé des Empreintes Génétiques) les chiffres sont de 1 724 173 enregistrements et de 111 002 affaires, toujours en 2010. Les avancées technologiques facilitent le recueil des traces. Ainsi, pour ne citer que l'exemple de la société française Morpho (Safran), sa solution d'identification biométrique MorphoBIS permet, grâce à la recherche automatisée de toutes les crêtes papillaires de la main, d'analyser les plus petites empreintes trouvées sur une scène de crime.

En octobre 2003, nous avions rédigé un article sur l'authentification biométrique dans la revue sécurité informatique du CNRS. Il nous a paru utile de mesurer, treize ans après, les avancées technologiques pouvant éventuellement remettre en cause sa conclusion principale :

« *L'utilisation de la biométrie comme moyen d'authentification dans le cadre d'une politique de sécurisation d'un système d'information est à déconseiller. Les deux raisons fondamentales sont les suivantes :*

– l'usurpation d'une donnée biométrique est réalisable par des techniques diffusées et accessibles ;

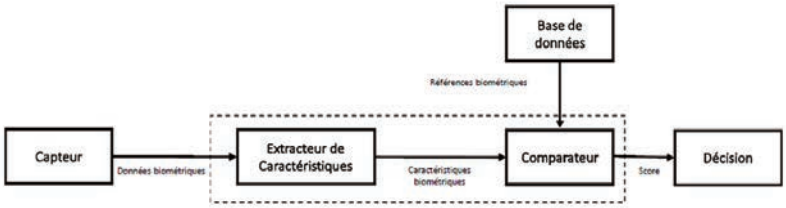
– une donnée biométrique ne se révoque pas quand elle est compromise ; or la donnée biométrique sera de plus en plus une donnée publique (au sens de la Sécurité des Systèmes d'Information).

En revanche, les capteurs biométriques sont utilisables pour faciliter l'opération d'identification préalable à une authentification, par exemple en remplaçant un login (identifiant de connexion) par une reconnaissance d'empreinte. Ce qui importe, c'est d'éviter de confondre ces deux opérations ; dans le cas précédent, le mot de passe nécessaire à l'authentification devra de toute façon être saisi après l'identification biométrique. »

Commençons par le second point sur la donnée biométrique

La CNIL distingue la biométrie « à traces » (empreintes digitales et palmaires) qui constituent des dispositifs sensibles soumis à autorisation. Les dispositifs « sans traces » (contour de la main, réseau veineux des doigts de la main) ou « intermédiaires » (voix, iris de l'œil, forme du visage) pourraient d'ailleurs être requalifiés tant les dispositifs électroniques invasifs se sont développés partout (caméras, micros, ordiphones, *etc.*). Ces faits confirment que la donnée biométrique reste irrévocable, en attendant peut-être les endosquelettes, et qu'elle est de plus en plus publique posant des problèmes sérieux de protection des données personnelles que nous abordons à la fin de l'article.

En comparaison avec une opération d'authentification classique, le code porteur (4, 6 ou 8 chiffres) débloquant une carte à puce ou le mot de passe sont eux des éléments secrets (mémorisés dans le seul cerveau de l'usager) qui doivent être révoqués après compromission. Mais, dans la pratique, ce n'est pas toujours le



Wolf - SystemX

Figure 1 : un système biométrique générique.

cas (partage des codes dans un cercle de confiance, difficultés de mémorisation) car les bonnes pratiques — « une clé, un usage » ; « je ne partage jamais mes secrets » — tiennent peu compte de la multiplication des systèmes et de la multiplicité des objets connectés qui vont envahir notre quotidien. Les architectures globales à bases de mots de passe à usage unique ou les solutions d'authentification unique (en anglais Single Sign-On) ont également montré leurs limites. Dans ce dernier cas, l'accès à des services variés avec une seule authentification crée un point de vulnérabilité unique et sera peu compatible avec l'hétérogénéité des systèmes hyperconnectés du futur.

Le premier point sur l'usurpation d'identité est inhérent à la nécessité d'utiliser un capteur biométrique à la fois pour l'enrôlement initial dans les opérations d'acquisition ou de capture et pour les opérations de reconnaissance (voir figure 1). Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances. En mode vérification pour l'authentification, le système doit répondre à une question de type : « *Est-il bien la personne qu'il prétend être ?* ». L'utilisateur propose une identité au système et le système compare le signal avec un seul des modèles présents dans la base de données souvent locale (problème de type 1 contre 1). Les algorithmes utilisés ici sont de type « filtrage par motif » (en anglais pattern matching). Ils progressent régulièrement par combinaison de diverses approches : corrélations, partitionnement, regroupement, analyses spectrales et cepstrales, processus stochastiques, réseaux de neurones, *etc.* La reconnaissance automatique de la parole complétée par une traduction automatique multilingue sur YouTube en fournit un exemple spectaculaire.

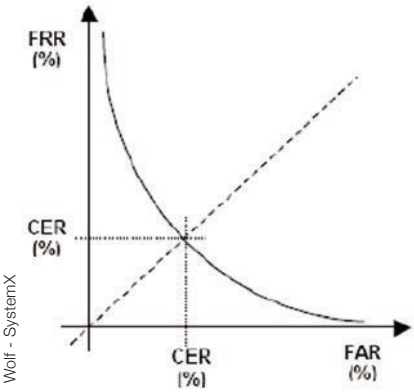
Contrairement à la validation par une machine d'un code pin ou code porteur ou

d'un mot de passe (permanent ou évanescent), le résultat n'est donc pas binaire (oui ou non) ce qui complique la décision. Deux principaux critères d'évaluation des systèmes biométriques sont souvent mis en avant, même si les données publiques objectives manquent :

le taux de faux rejet FRR (en anglais False Rejection Rate) : il indique dans quelle mesure un système biométrique donné ne réussit pas à faire correspondre des échantillons provenant du même utilisateur (rejet d'un utilisateur légitime). Ce critère est favorable à la sécurité du système à protéger mais provoque un inconfort d'utilisation. Il peut être rédhibitoire quand il s'agit d'intervenir opérationnellement sur un système critique.

Le taux de fausses acceptations FAR (en anglais False Acception Rate) : il indique dans quelle mesure un système biométrique donné fait correspondre des échantillons ne provenant pas du même utilisateur (confusion d'un imposteur avec un utilisateur légitime). Ce critère peut mettre en péril le système sous contrôle d'accès.

Un troisième paramètre (voir figure 2), le taux d'exactitude croisée CER (en anglais Crossover Error Rate), est alors défini qui est le point d'intersection entre la courbe du taux de fausses acceptations et la courbe du taux de faux rejets. En général, la valeur de l'exactitude croisée augmente



Wolf - SystemX

Figure 2 : critères d'évaluation.

parallèlement à l'exactitude inhérente d'une technologie biométrique (taux d'erreur plus faible au point d'intersection).

Tout capteur est potentiellement leurrable par un artefact reproduisant la caractéristique biométrique à mesurer. Le domaine le plus exploré depuis quinze ans concerne la reconnaissance d'empreinte digitale. Les technologies mises en œuvre (capteurs capacitifs à matrices entières ou à défilement, capteurs optiques à prismes ou à vue directe, capteurs thermiques) sont aussi variées que les techniques de fabrication de faux doigts (doigts morts, silicone, latex, pâte à modeler, circuit imprimé flexible, buée, poudre de graphite, etc.). Mais celle qui marche le mieux est à base de gélatine alimentaire (expérience personnelle de l'auteur). Elle fait l'objet de

démonstrations publiques régulières comme celle du Chaos Computer Club allemand qui, dès 2013, trompait la technologie TouchID de l'iPhone (voir figure 3) en allant jusqu'à reproduire les empreintes de la ministre de la Défense captées, à son insu, par un simple appareil photo. Ces démonstrations répétées confirment les risques d'usurpation d'identité. Suite à un reportage télévisé français sur le contrôle automatisé aux frontières des aéroports, il a fallu durcir le capteur en service. Les contre-mesures proposées aujourd'hui (détection du vivant, oxymétrie, analyses multi facteurs) sont soit inefficientes soit trop onéreuses pour être déployées à grande échelle. Les autres techniques biométriques sont et seront aussi susceptibles de tentatives de tromperie : iris et rétine <-> lentille ; visage <-> caméra ; le réseau veineux <-> circuit imprimé ; ADN, sang, salive <-> fausses traces ; odeur <-> parfum ; signature <-> faussaire ; reconnaissance vocale <-> synthèse vocale ou imitateur ; démarche ou geste de main <-> film ou physiologiste.

Le dernier point de la conclusion de 2003 proposait l'ajout (et non la substitution) de la biométrie à des systèmes d'authentification plus classiques pour en faciliter l'usage.

L'évolution du processus d'achat sur Internet est instructive. Pour durcir la saisie, sous navigateur avec protocole

Wolf - SystemX

Figure 3 : leurrage d'un capteur d'ordiphone.

chiffrant https, du numéro de la carte de paiement complété d'un code à 3 chiffres au verso (qui complique l'usurpation photographique de celle-ci) des techniques de vérification dites 3-D Secure ont été rajoutées depuis quelques années. Une des solutions consiste à envoyer un code par sms sur le téléphone de l'acheteur pour qu'il puisse affirmer son identité. Cette transmission par un canal plus sûr permet aussi de combattre certains programmes malveillants. Mais le constat commercial, c'est que cela freine les achats, parfois compulsifs, surtout des jeunes utilisateurs habitués à l'ergonomie tactile de leur ordiphone.

Une solution a été proposée récemment par La Banque Postale pour faciliter le paiement à distance. Elle fait appel à la reconnaissance vocale et fait reposer l'authentification forte sur le système rodé

de la téléphonie mobile à base de cartes à puces. Les étapes pour le client sont alors les suivantes : lors de l'achat en ligne, une extension s'ouvre automatiquement sur son navigateur ; le client déclenche alors, depuis cette extension, le mécanisme d'authentification vocale ; un appel est émis sur son téléphone mobile sur lequel il prononce la phrase d'authentification ; quand le locuteur est identifié comme étant le porteur de la carte, l'extension génère le cryptogramme à usage unique de la carte et remplit automatiquement le formulaire de paiement ; pour finir le client valide son paiement en ligne.

Une autre initiative intitulée FIDO (Fast IDentity Online), qui fédère des acteurs industriels du domaine, est également à suivre. Le World Wide Web Consortium (W3C) cherche une alternative au mot de passe sur Internet. Ses travaux s'orientent vers les spécifications de l'écosystème FIDO 2.0, justement proposées par l'alliance FIDO pour standardisation. L'objectif global de ces interfaces est de permettre à différentes méthodes d'authentification d'être traitées de la même manière. Les premiers dispositifs, de type jeton matériel d'authentification, sont déjà commercialisés. Des versions biométriques (scan de l'iris et reconnaissance d'empreinte digitale) ont également été fonctionnellement spécifiées.

Reste l'épineux problème de la protection de la vie privée même si quelques voix en annoncent sa fin dans un monde de plus en plus robotisé. Le législateur, dans les pays européens, limite la constitution de bases de données centralisées de données biométriques. En France, un décret, publié le 4 décembre 2015, précise les finalités pour lesquelles le traitement automatisé de traces et empreintes digitales et palmaires est autorisé. Il limite aux seuls crimes et délits le champ infractionnel dans le cadre duquel il est possible de recourir au traitement. Des vols massifs de données biométriques confortent cette position : aux États-Unis en 2015, un fichier contenant 5,6 millions d'empreintes digitales de fonctionnaires a été dérobé par des pirates au sein de l'OPM (Office of Personal Management), l'organisme en charge des fonctionnaires, dont des employés du Pentagone, du FBI ou de la NSA.

Des avancées technologiques, pourront éventuellement infléchir cette situation. Une application du chiffrement homomorphe qui a été présentée à l'IRT SystemX, le 10 mars 2016, permet de faire des calculs sur des données chiffrées. La preuve mathématique de sa faisabilité est très récente et date de 2009 ; depuis, des réalisations pratiques essaient de faire progresser les temps d'exécution et de mieux gérer les expansions de données inhérentes à

cette technologie. Cette démonstration développée avec le CEA LIST, dans le domaine de la biométrie faciale, permet la reconnaissance d'un individu en confrontant sa photographie avec une version chiffrée de ses caractéristiques faciales. L'avantage essentiel est qu'un vol de cette donnée protégée ou même qu'une observation des traitements ne donne aucune information exploitable au pirate informatique. Le graal de la protection des données personnelles serait à portée de calcul !

Au-delà de cette avancée dont les applications seront limitées par les puissances de stockage et de calcul disponibles, la conception d'une politique d'authentification pour les futurs systèmes hyper-connectés (réseaux d'énergie intelligents, transport connecté, usine du futur, Internet des objets) nécessite des travaux novateurs. Ceux-ci devront réconcilier robustesse aux attaques, facilités d'emploi, hétérogénéité des solutions, respect de la vie privée, passage à l'échelle. La biométrie n'en constitue qu'une des briques technologiques disponibles.

L'AUTEUR

Né en 1958, ancien élève de l'École Polytechnique (1978), docteur en Informatique (1985) de l'Université Pierre et Marie Curie, Paris 6ème et ingénieur général de l'Armement, M. Philippe WOLF fut responsable du département « sécurité électronique et informatique » du Centre d'Électronique de l'Armement (CELAr) à Bruz (1985-1995). Il fut Directeur des études de l'École Polytechnique à Palaiseau (1995-2000). En octobre 2000, il a été nommé Directeur du Centre de formation à la sécurité des systèmes d'information (CFSSI) puis Sous-directeur « Télécommunications et Réseaux Sécurisés » au Secrétariat général de la défense nationale (2005-2008). De janvier 2008 à avril 2015, il fut le Conseiller du Directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Depuis avril 2015, il est chef du projet « Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité » (EIC : voir http://www.irt-systemx.fr/project/eic/) à l'IRT-SystemX.
M. Philippe WOLF enseigne l'« Intelligence économique, Société de l'information et Société de la désinformation » à l'École Polytechnique, les « conflits et coopérations dans le cyberespace » au sein du "Master in International Security" de Sciences-Po Paris, la « Connaissance des réseaux et sécurité », dans le Master « Droit de l'internet public (administration – entreprises) », Université Paris 1 Panthéon-Sorbonne. Il donne des cours et conférences à l'École des Mines-ParisTech, à l'École Nationale d'Administration et à l'Institut des hautes études de défense nationale. Il publie régulièrement des articles sur la sécurité dans le cyberespace.
Chevalier de la Légion d'honneur et officier de l'ordre national du mérite, il est ancien auditeur de la 44e session du centre des hautes études de l'armement.

Pour tous renseignements bibliographiques et autres, merci de vous adresser à l'auteur : philippe.wolf@irt-systemx.fr

Fotolia : Strazkul

UNE TRACABILITE ENCADREE JURIDIQUEMENT

La protection des droits fondamentaux oblige le législateur à encadrer les systèmes de traçabilité. La loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation répond à cet impératif en normant la mise en œuvre de ce moyen de traçabilité des individus et des objets. Les décisions de justice successives, conformément à l'article 8 de la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, consacrent le contrôle par le juge de cette ingérence dans la vie privée. La lutte contre le terrorisme et la grande criminalité a posé également la question de l'équilibre entre les impératifs d'ordre public et le respect des droits fondamentaux. Le croisement de bases de données permettant de suivre les flux de personnes entre dans cette problématique. Au niveau européen, le traitement de données ne pourra se faire que dans le respect des prescriptions de la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Elle doit permettre de garantir un niveau élevé de protection des droits fondamentaux et un niveau élevé de sécurité publique. Cette décision-cadre s'inscrit dans la droite ligne du programme de La Haye de 2004.

Traçage des personnes
et droits fondamentaux

par MYRIAM QUÉMÉNER

L'ère numérique a entraîné une mutation profonde de la société, des habitudes de vie, des modes de pensée. Les données numériques sont autant de traces laissées par les individus qui permettent de le suivre voire de le surveiller géographiquement, médicalement, socialement et même psychologiquement. Cependant, au nom de la protection des droits fondamentaux, le législateur encadre systématiquement les outils de traçabilité et la jurisprudence tant européenne que française se charge d'assurer le respect des conditions fixées.

MYRIAM QUÉMÉNER

Magistrat,
Expert pour le conseil de l'Europe
Conseiller auprès du préf et chargé de la lutte contre les cybermenaces

Depuis les déclarations d'Edward Snowden et les attaques terroristes perpétrées en France ces derniers mois, le débat sur l'équilibre entre libertés et sécurité a été relancé. Il constitue un enjeu important et des plus sensibles. Il s'agit de garantir les droits fondamentaux tout en préservant l'ordre public qui peut être particulièrement ébranlé. En conséquence, les outils de traçage permettant la surveillance de masse ont été largement repensés[1].

(1) Bauman Zygmunt, BigoDidier, Esteves Paulo, Guild Elspeth, Jabri Vivienne, LyonDavid, Walker R. B. J. (Rob)

Si les nouveaux systèmes numériques de traçabilité des individus peuvent être performants pour la sécurité et l'identification d'auteurs d'infractions, inévitablement les questions liées aux droits de l'homme ressortent lorsqu'il s'agit de surveillance de masse. A cet égard, deux dispositifs illustrent à notre sens parfaitement ces enjeux, à savoir d'une part la géolocalisation et le fichier du passager, couramment appelé PNR.

Fotolia/Sangoiri

Le recueil des données liées à la circulation des personnes doit être juridiquement encadré pour garantir les libertés individuelles

Traçabilité et géolocalisation

La géolocalisation à la fois outil de sécurité mais également de surveillance[2] a suscité des polémiques assez vives et la jurisprudence de la cour européenne des droits de l'homme a exigé que cette ingérence dans la vie privée des individus soit prévue par une loi suffisamment précise et qu'elle offre des « *garanties adéquates et suffisantes contre les abus* »[3] .

(2) J. Perriault « Traces numériques personnelles, incertitude et lien social », Hermès, La Revue 1/2009 (n° 53), p. 13-20.

(3) CEDH 2 sept. 2010, Uzun c/ Allemagne, n°35623/05.

(4) Cass. crim., 22 oct. 2013, no 13-81.945 et no 13-81.949, RLDI 2013/98, no 3289, obs. Costes L. ; sur cet arrêt voir Quéméner M., La géolocalisation à l'épreuve de la procédure pénale, RLDI, no 3299

La chambre criminelle[4] par deux arrêts en 2013 a estimé qu'il se déduit de l'article 8 de la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales que le procédé de géolocalisation constitue « *une ingérence dans la vie privée dont la gravité nécessite d'être ordonnée sous le contrôle d'un juge garant du respect des libertés individuelles* ». Il est désormais encadré par la loi n° 2014-372 du 28 mars 2014[5] qui a fixé des conditions strictes pour la mise en œuvre de ce moyen de traçabilité des individus et des objets.

(5) Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation (JO, 29 mars).

Le recours à cette technique est possible en cas d'investigations concernant les délits contre les personnes punis d'une peine d'emprisonnement supérieure ou égale à 3 ans et les autres crimes et délits punis d'au moins 5 ans. Une telle possibilité est offerte s'agissant d'une enquête en recherche des causes de la mort, des causes de la disparition et en recherche d'une personne en fuite.

L'opération est autorisée dans le cadre de l'enquête de police en flagrance ou en préliminaire par le procureur de la République, pour une durée maximale de quinze jours consécutifs. À l'issue de ce délai, cette opération est autorisée par le juge des libertés et de la détention (JLD) pour une durée maximale d'un mois renouvelable. Au cours de l'instruction, elle est autorisée par le juge d'instruction, pour une durée de 4 mois renouvelable.

Le texte encadre encore les hypothèses d'introduction dans un lieu privé professionnel et d'habitation afin d'installer un dispositif de géolocalisation. Ainsi, seul le JLD ou le juge d'instruction peut l'autoriser sous réserve que l'infraction soit passible d'une peine d'au moins 5 ans d'emprisonnement.

(6) Crim. 9 févr. 2016, FS-P+B+I, n° 15-85.070

La chambre criminelle[6] a aussi récemment précisé que les données issues d'une géolocalisation mise en œuvre sur le territoire national et s'étant poursuivie sur le territoire d'un autre État ne peuvent, lorsque cette mesure n'a pas fait l'objet d'une acceptation préalable ou concomitante de celui-ci au titre de l'entraide pénale, être exploitées en procédure qu'avec son autorisation.

Traçabilité et PNR

La lutte contre le terrorisme et la grande criminalité est devenue depuis quelques années une priorité pour de nombreux États et l'Union européenne. Elle a eu pour conséquence la création de multiples mécanismes de stockage et d'échange de données personnelles entre autorités publiques, qui peuvent porter atteinte aux droits fondamentaux.

(7) En français, dossier du passager.

(8) S. Peyrou , Revue du droit public - 01/01/2016 - n° 1 - page 55

Le *Passenger Name Record*[7] (PNR) est ainsi une illustration intéressante de ce débat entre la nécessité d'assurer l'ordre public et le respect des droits fondamentaux. Après les derniers attentats en France et en Belgique, les discussions sur son adoption ont été à nouveau lancées car il est apparu comme l'une des solutions pour stopper les terroristes et le gouvernement français a insisté sur l'urgence qu'il y a à adopter ce texte[8].

En effet, tous les services de renseignements y sont favorables car il permet notamment de savoir si une personne considérée comme dangereuse a pris l'avion et pour quelle destination.

DIRECTEUR DE LA PUBLICATION
Général de brigade **Philippe Guimbert**

Rédaction
Directeur de la rédaction :
général d'armée (2S) **Marc WATIN-AUGOUARD,**
directeur du centre de recherche de l'EOGN

Rédacteur en chef : colonel (ER) **Philippe DURAND**

Maquettiste PAO :
Major **Carl GILLOT**

Message aux abonnés

La veille juridique de la gendarmerie nationale et la revue du centre de recherche de l'EOGN sont maintenant consultables sur le site internet du CREOGN
www.gendarmerie.interieur.gouv.fr/crgn/publications

Sûreté aérienne et maritime

L'accroissement des flux maritimes et aériens, qui se traduit par une complexité des aires aéroportuaires et des hinterland, amène à reconsidérer ces points névralgiques en terme de couverture de sûreté. Cette dernière recouvre la surveillances des personnes, des lieux de transfert et la gestion de la qualité des opérateurs qui se partagent ce marché du travail. A ces problématiques, il faut rajouter la question des normes internationales de filtrage des passagers et une prise en compte d'un nouveau mode de sécurisation des voies maritimes. L'architecture des technologies déployées dans la sécurisation de cette écosphère économique fait l'objet d'une vive concurrence entre fournisseurs car elle est la base d'un leadership mondial en termes de supervision des échanges planétaires. La gendarmerie nationale, par son expertise multimodale, concourt à cette mission de sécurité en épousant les évolutions des mœurs, des moyens et des technologies nouvelles mises en œuvre dans ces espaces spécialisés.

MINISTÈRE DE L'INTÉRIEUR

www.gendarmerie.interieur.gouv.fr