INTERNATIONAL

© Fotolia_123392025

LA COOPÉRATION INTERNATIONALE POUR ANTICIPER L'ÉVOLUTION DE LA CYBERCRIMINALITÉ

L'évolution des menaces numériques et le chiffrement généralisé des données impose aux forces de polices européennes de densifier leurs échanges techniques et de mutualiser des moyens matériels. La création de plateformes multidisciplinaires européennes contre les menaces criminelles facilite des coopérations techniques en matière de cybermenaces. Dans ce fil, la création de groupes de travail d'action contre la cybercriminalité, la mise en œuvre ponctuelle de bureaux mobiles d'Europol ou la mobilisation de laboratoires détenant des expertises spécifiques participent à cette démarche collaborative. La Gendarmerie nationale a pris le parti de s'orienter vers une forte coopération avec le monde universitaire et de construire un dispositif incitatif aux travaux de recherches via des mesures d'accompagnement prenant en compte des innovations de rupture. Elle participe, aux côtés d'industriels et d'universitaires, à des programmes internationaux de financement de recherches orientées vers les besoins des forces de l'ordre.

Coopération Technologique

Internationale (CTI): la nouvelle arme de la gendarmerie scientifique et des cyber-gendarmes

Par Thibaut Heckman

Les criminels suivent de très près l'évolution des technologies numériques et sont plus particulièrement attentifs aux technologies de chiffrement leur promettant une impunité totale (confidentialité, authentification et intégrité). Les supports de stockages sécurisés par mot de passe, les messageries chiffrées (WhatsApp, Telegram, Signal) et les téléphones portables sur-sécurisés sont systématiquement utilisés pour les communications entre membres de puissants réseaux criminels ou terroristes dans le cadre de leurs diverses activités. Devant la difficulté technique d'absorber les technologies de chiffrement de plus en plus complexes et pour faire face aux crimes organisés et à la cybermenace, les forces de sécurité intérieure n'ont pas d'autre choix que de multiplier les Coopérations Technologiques Internationales (CTI) en s'ouvrant à de nouveaux partenariats et en développant des échanges techniques avec les forces de sécurité étrangères, les industriels et les universitaires.

THIBAUT HECKMANN

Capitaine de Gendarmerie. Docteur en Mathématiques de l'ENS-Paris. Chargé de Projets au CREOGN

Ainsi, pour la gendarmerie scientifique et les cyber-gendarmes, la coopération technologique internationale se concrétise principalement sous trois formes : les échanges techniques et la mutualisation des moyens matériels avec les forces de police étrangères, la coopération technique avec le monde universitaire/industriel international et la participation à des programmes de recherche internationaux impliquant des acteurs similaires. Si la première forme de collaboration est active depuis de nombreuses années, les deux dernières formes sont bien plus

récentes et immédiatement dépendantes des difficultés techniques générées par l'évolution des nouvelles technologies.

Les grandes organisations internationales, un pilier solide mais non suffisant de la chaîne de coopération technique...

L'organisation internationale de police criminelle (*Interpol*), dont le siège se trouve à Lyon, a été créée en 1923 afin d'initier et de faciliter la coopération policière internationale (*elle s'appelait alors Commission internationale de police criminelle*[1]). L'idée de la création d'Interpol est née lors du premier Congrès de police judiciaire internationale, qui s'est tenu du 14 au 20 avril 1914 à Monaco, et dont les conférences portaient notamment sur la nécessité de réaliser des échanges techniques en identification humaine (*section sur l'anthropométrie préventive internationale des conscrits dirigée par le célèbre policier français Alphonse Bertillon*).

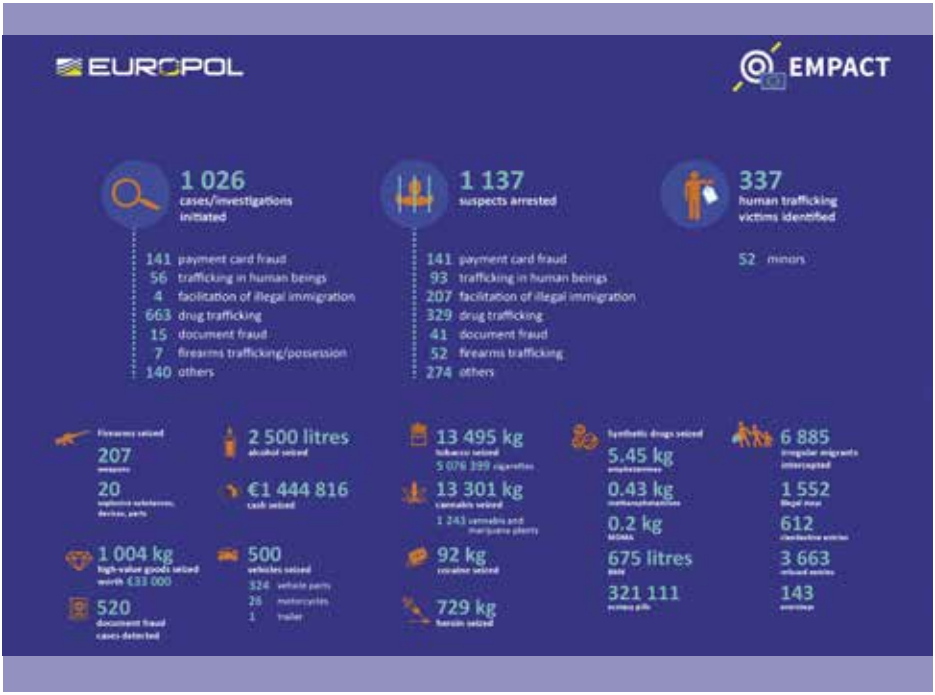
(1) Statut adopté par l'Assemblée générale de l'Organisation en sa 25e session (Vienne–1956).

© Interpol

Affiche du Congrès de police judiciaire international de 1914.

Interpol est forte aujourd'hui de 194 États membres. Chaque pays membre dispose d'un bureau central national, véritable point d'entrée des demandes de coopération policière, judiciaire et technique. La coopération scientifique entre forces de police étrangères fait d'Interpol le véritable précurseur de la CTI des forces de l'ordre. Mais devant la montée croissante des nouvelles menaces numériques et les difficultés techniques posées par la généralisation du chiffrement des données dans les affaires criminelles, les forces de police européennes avaient besoin d'une force de frappe spécialisée afin de densifier les échanges techniques et les mutualisations de moyens matériels. C'est ainsi qu'en 2013 a été créé le Centre européen de lutte contre la cybercriminalité (European Cyber Crime Centre – EC3[2]) dirigé par EUROPOL sous l'égide de l'Union Européenne, dans le but de lutter plus efficacement contre la cybercriminalité.

(2) Commission Européenne IP/12/37 et MEMO/12/221, Brussels, 28 Mars 2012.



L'EC3 soutient techniquement les services de police dans la lutte contre la criminalité organisée. Dans ce sens, plusieurs leviers ont été mis en place par Europol pour contrer le crime numérique : une plateforme multidisciplinaire européenne contre les menaces criminelles via les programmes quadriennaux EMPACT (European Multidisciplinary Platform Against Criminal Threats) véritables facilitateurs des coopérations techniques en matière de cybermenaces ; la création d'un groupe de travail conjoint d'action contre la cybercriminalité (*Joint Cybercrime Action Taskforce*) pour aider les enquêteurs nationaux; la création des bureaux mobiles d'Europol dans le cadre d'opérations majeures et enfin la création des journées d'actions communes (*Joint Action Days*).

Du point du vue de la criminalistique, la coopération européenne a été facilitée par la création en 1995 de l'ENFSI (European Network of Forensic Science Institutes[3]) qui regroupe les laboratoires de police technique et scientifique de l'UE. Dix-sept groupes de travail ont été instaurés permettant aux experts internationaux d'échanger leurs résultats mais également de mutualiser

(3) Founding Meeting on October 20, 1995 in Rijswijk (The Hague).

leurs moyens techniques et humains (stages, formations, conférences). Ainsi, les experts français de l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), acteur majeur de l'ENFSI, intègrent l'ensemble de ces groupes. Ils ont ainsi vu les échanges techniques et humains se multiplier ces dernières années. Des ateliers techniques et des conférences internationales majeures sont organisés pour inciter à l'innovation comme par exemple la conférence de l'EAFS (*European Academy of Forensic Science*) qui est un événement public triennal organisé par l'ENFSI et permettant à l'ensemble de la communauté criminalistique internationale de se réunir.

Enfin, d'autres organismes européens comme le collège européen de police (CEPOL), ou le collège européen de sécurité et de défense (CESD), permettent des échanges européens et le perfectionnement des militaires de la gendarmerie. La coopération scientifique internationale entre forces de l'ordre est également grandement favorisée par l'échange d'officiers de liaison.

La tuerie de San Bernardino, un tournant décisif dans la coopération entre les forces de sécurité intérieure et le monde universitaire dans l'échange de techniques de déchiffrement

De l'enquête sur la tuerie de San Bernardino (USA) en 2015, l'histoire retiendra surtout la procédure judiciaire intentée par le FBI contre Apple pour contraindre l'entreprise à développer un logiciel permettant d'extraire et de déchiffrer les données du téléphone portable du tueur. La procédure n'était pas allée à son terme puisque le FBI avait finalement reçu une solution provenant de partenaires universitaires (*comme l'université de Cam bridge qui proposa une technique publiée*[4]) ou d'autres entités privées étrangères alors restées anonymes. Le directeur du FBI indiqua en conférence de presse avoir payé la solution plus d'un million d'euros. Le FBI qui était, avant la tuerie de San Bernardino, opposé à échanger techniquement (*culture du secret et développement interne de ses propres solutions*) s'est alors ouvert à la coopération technologique extérieure. Les mêmes questions se sont posées au niveau des forces de sécurité intérieure françaises. La Gendarmerie nationale a alors pris le parti de se réorganiser et de s'orienter vers une forte coopération avec le monde universitaire en participant à de nombreux projets de recherche nationaux et européens. Elle a construit un dispositif incitatif afin d'encourager les gendarmes à réaliser des travaux de recherches via des mesures d'accompagnement innovantes (*temps réservé à la rédaction, publications, conférences, dépôts des brevets industriels, thèses*)

(4) Skorobogatov, Sergei. «The bumpy road towards iPhone 5c NAND mirroring.» arXiv preprint arXiv:1609.04327 (2016).

et en décidant de scolarités alternatives à l'École de guerre pour ses futurs chefs (*formations universitaires de hauts niveaux, doctorat, Master of Business Administration, préparation d'Habilitations à Diriger des Recherches*). En 2018, elle a créé le programme « DISRUPT » pour soutenir l'innovation de rupture via des thèses et des études scientifiques autour du numérique, du big data, de l'intelligence artificielle, de la robotique, de l'humain augmenté et de l'identification humaine. Pour pérenniser et renforcer ce rapprochement avec le monde universitaire, elle a signé en 2019 un accord-cadre avec le CNRS ainsi qu'une convention avec la Conférence des Présidents d'Universités.

La gendarmerie accueille également de nombreux étudiants du cursus Licence, Master, Doctorat ou des grandes écoles d'ingénieurs (*X, ENS, mines*) leur permettant de travailler sur des sujets d'intérêt pour l'Institution avec la perspective également de constituer un vivier de recrutement. La Gendarmerie nationale compte actuellement dans ses rangs près de 350 docteurs et doctorants, toutes disciplines confondues, et ce chiffre ne cesse de croître chaque année. Le CREOGN (*Centre de recherche de l'école des officiers de la gendarmerie nationale*) a notamment pour mission de recenser, d'encourager et de valoriser les militaires de la gendarmerie qui mènent des activités de recherche. Ainsi, un dialogue régulier et des invitations aux évènements scientifiques permettent aux personnels de la gendarmerie et aux chercheurs du monde entier de se rencontrer et d'échanger autour de la recherche et de l'innovation.

Le financement de la recherche, le nerf de la guerre…

Comme dans toute structure, qu'elle soit publique ou privée, la recherche et le développement ont un coût important qui constitue bien souvent une grosse partie du budget de fonctionnement. Afin d'augmenter considérablement ce budget, la Gendarmerie nationale participe, aux côtés d'industriels et d'universitaires, à des programmes internationaux de financement de recherches orientés vers les besoins des forces de l'ordre tels qu'Horizon 2020, OLAF, le Fonds de Sécurité Intérieure de l'Union Européenne. La gendarmerie est déjà présente dans bons nombres d'entre eux (*CERBERUS, EXFILES, Shuttle, OP-MoPS, ILEAnet, ...*) et continuera à l'être dans les prochains programmes (Horizon Europe). À compter de 2021, la Commission Européenne proposera un budget de 94 milliards d'euros pour Horizon Europe en remplacement du programme Horizon 2020 (*doté de 77 milliards d'euros*).

Les résultats prometteurs de la gendarmerie dans la Coopération Technologique Internationale

En France, la criminalité organisée est réprimée plus sévèrement. Cette

répression se retrouve à deux niveaux sur le plan pénal : la circonstance aggravante de bande organisée (*132-71 du code pénal*) et l'infraction d'association de malfaiteurs (*l'article 450-1 du Code pénal*). Du fait de cette répression, les réseaux criminels se sont protégés et se sont rapprochés des nouvelles technologies afin de laisser un minimum de traces, rendant difficile le travail de la justice. Le stockage des données et les communications entre les membres des réseaux criminels se sont donc portés naturellement vers les nouvelles techniques de chiffrement. L'une d'elles a fait la une des médias en juillet 2020. La société Encrochat commercialisait des téléphones portables sécurisés à destination de milliers de criminels (*basés sur Android mais utilisant des surcouches logicielles de chiffrement*). La caméra, le micro et le GPS étaient physiquement retirés pour écarter tout risque d'interception et traçage par les forces de l'ordre. Le réseaux Encrochat a été démantelé en 2020 par la gendarmerie française dans le cadre d'une coopération technologique internationale exemplaire.

Début 2019, le projet de recherche européen CERBERUS, piloté par la Gendarmerie nationale et financé par les Fonds de Sécurité Intérieure de l'Union Européenne, permettait d'accélérer les recherches de l'IRCGN et du centre de lutte contre les criminalités numériques (C3N) sur ces téléphones. Devant l'ampleur des résultats obtenus, en avril 2020, il a été décidé, de créer une Équipe Commune d'Enquête (ECE) entre la France et les Pays-Bas, sous l'égide d'EUROJUST avec le soutien d'EUROPOL. Au terme de cette opération, des centaines de criminels ont été interpellés dans toute l'Europe, 10 tonnes de cocaïne et 1 200 kg de crystal méthamphétamine ont été saisis, dix-neuf laboratoires clandestins de drogues synthétiques démantelés et des projets d'assassinats stoppés.

L'action de la gendarmerie scientifique et des cyber-gendarmes en coopération technique étroite avec les forces étrangères a permis de démanteler ce réseau de grande envergure, avec des arrestations et des saisies records à la clé. Cette action illustre parfaitement les résultats directs de la Coopération Technologique Internationale et elles seront très certainement encore plus nombreuses dans les années à venir.

Le projet CEBERUS, co-financé par le Fond de Sécurité Intérieure de la Commission Européenne, a pour principal objectif la mise au clair de la donnée dans un contexte de lutte contre la criminalité organisée. L'IRCGN (France) est porteur du projet, avec pour partenaires le NFI (Pays-Bas) et l'Irlande (UCD Dublin).

L'AUTEUR

Le capitaine Thibaut Heckmann est docteur en mathématiques de l'École normale supérieure de Paris et chercheur associé à l'ENS depuis 2018. Ancien chercheur associé à l'université de Londres et à l'université de Cambridge, en 2017 et 2018, il a rejoint le CREOGN en août 2020. Il a été de 2015 à 2020 expert à l'IRCGN et a notamment dirigé l'unité d'expertise extraction des données. Il a obtenu en 2018 le prix Européen Emerging Forencic Scientist Award 2018-2021 de l'académie européenne de police technique et scientifique (ENFSI) et le Trophée de cybersécurité du Cercle K2 en 2020. Il est membre du comité d'organisation de nombreuses conférences internationales et projets européens.