Crime et expertises

A la cour d'appel de Reims

Site Internet : https://cnemj.fr/

Livret pédagogique introductif
© CNEMJ – 2023

COLLOQUE du vendredi 13 octobre 2023 (10H – 17H30)

Sous la Présidence d'honneur des chefs de cour :

Monsieur Christophe REGNARD, premier président

Monsieur Hugues BERBAIN, procureur général

Cour d'appel de Reims 201 Rue des Capucins, 51100 Reims

Soirée dans le caveau MUMM

« Crime et expertises »

Sous la Présidence d'honneur des chefs de cour de Reims :
Monsieur Christophe REGNARD, premier président
Monsieur Hugues BERBAIN, procureur général
Cour d'appel de Reims
Vendredi 13 octobre 2023 : 10H – 17H30

Programme

Chaque intervention est prévue avec une large discussion

Propos introductifs et matinée : « Le crime classique »

10H – 10H30 : Propos introductifs

10H30 – 11H00 : Pierre LAURENT, expert en balistique près la CA de Paris, agréé CC

« La balistique et ses pièges sur les lieux du crime »

11H00 – 11H30 : Marc SCHWEITZER, expert psychiatre près la CA de Paris et à la Commission Pluridisciplinaire des Mesures de Sûreté de la Cour d'Appel de Paris

« Dangerosité(s) : Quelles évaluations pour le psychiatre expert ? »

11H30 – 12H00 : Muriel JOSIÉ, présidente de chambre à la cour d'appel de Paris, en charge des assises

« L'expert aux assises – point de vue du magistrat »

12H00 – 12H30 : Henry COUDANE, professeur émérite de médecine légale, expert honoraire près la CA Nancy, agréé CC

« Le médecin légiste et le crime : de la levée de corps aux assises »

Cocktail déjeunatoire sur site 12h30-14h00

Court extrait en projection « privée » du film historique de 1976 Le juge et l'assassin

Après-midi et synthèse : « Le crime du futur » Animateur Maître Gérard CHEMLA

14H00 – 14H30 : Sylvie MENOTTI, conseiller honoraire, membre de la formation de jugement de la Cour de justice de la République

« L'évolution relative au jugement des crimes »

14H30 – 15H00 : David ELKOUBI, expert en traces et empreintes près la cour d'appel de Chambéry

« Quelle confiance accorder aux serrures en criminalistique ? »

15H00 – 15H45 : Sabine KHERIS, 1ère vice-présidente chargée de l'instruction, coordonnatrice du pôle national des crimes non élucidés, sériels et complexes, TJ de Nanterre

Valérie DUBY, greffier principal, TJ de Nanterre

« Les cold cases »

15H45 - 16H30 : général Christophe HUSSON, commandant du COMCYBER :

« La cybercriminalité aujourd'hui et demain »

16H30 - 17H00 : Roch MENES, expert honoraire près la cour d'appel de Riom, ancien président de la CNEMJ, membre du conseil d'administration de l'EEEI

« Le crime hors de nos frontières »

17H00– 17H30 : discussion générale et synthèse

****

DOCUMENTATION

Livres :

Victor HUGO :

Histoire d'un crime

Jacques DALLEST :

Cold cases : un magistrat enquête

Jean ALBERT, Jean-Baptiste MERLIN :

L'avenir de la justice pénale internationale

Revue EXPERTS :

- Faire parler les serrures : l'expertise en intrusion furtive ou la serrurerie forensique
- Innover fait partie de l'ADN des experts scientifiques de la Gendarmerie
- Les cyberattaques : un phénomène inquiétant qui exige des réponses
- Démêler le vrai du faux

DIU NATIONAL D'EXPERTISES EN ACCIDENTS MEDICAUX

Rejoignez-nous à la CNEMJ !

****

SOMMAIRE

Crime et expertises : Propos introductif

Mary-Hélène BERNARD

Présidente CNEMJ

Expert honoraire (neurochirurgie et médecine légale)

Reims

Ce thème « crime et expertises » choisi par la Compagnie Nationale des Experts Médecins de Justice pour son second colloque annuel 2023 peut concerner nombre de citoyens et toutes sortes de catégories d'experts : il s'agit d'un thème transversal et évolutif.

La séparation en « crime classique » et « crime du futur » veut souligner que le crime évolue avec la société au sein de laquelle il est commis, avec ses progrès scientifiques et ses mentalités.

La matinée sera consacrée à la balistique, à l'évaluation particulièrement difficile de la dangerosité du criminel, et aux sessions d'assises vues par un magistrat et par un légiste.

Lors de la pause « déjeuner », vous aurez la possibilité de regarder un court extrait de l'excellent film historique de 1976 « le juge et l'assassin » de Bertrand TAVERNIER.

L'après-midi animée par Maître Gérard CHEMLA sera ouverte par une mise au point sur l'évolution du jugement des crimes, puis le pôle des « cold cases » récemment créé qui jouit d'un grand succès, et la cybercriminalité qui explose littéralement. Enfin, la mondialisation du crime qui suit l'évolution des sociétés là encore…

Surtout, n'hésitez pas à poser les questions qui vous interpellent car nous avons la chance d'avoir les éminents spécialistes du sujet à disposition et un temps de discussion est systématiquement réservé.

Excellent colloque en terre rémoise !

******

SOMMAIRE

La science balistique

Pierre LAURENT

Expert en balistique près la CA de Paris, agréé par la Cour de cassation

Président de la Compagnie Nationale des Experts en Armes et Munitions près les Cours d'Appel

L'objectif de la présentation sera de montrer au travers d'exemples que, comme dans d'autres disciplines, le diable est souvent dans les détails.

L'expertise en balistique est supposée être d'abord un piège pour les auteurs de crimes qu'ils espèrent parfaits. Certains dossiers ne tiennent que par la qualité de l'expertise balistique.

Dans un dossier, Mme D meurt brûlée dans sa voiture tandis que son mari est agressé par arme à feu. Un examen du projectile 48h après les faits permettra de connaitre le calibre, deux particularités de la cartouche utilisée et la marque probable de la carabine. Sachant quoi chercher, les enquêteurs allaient trouver les éléments exploitables par le balisticien qui s'avéreront déterminant.

Dans d'autres cas, l'auteur est connu et a tout expliqué. Le dossier est simple. L'expert n'est là que pour confirmer. Mais attention aux conclusions trop évidentes, fausses ou simplistes !

Dans le dossier H, les atteintes sur la victime étaient atypiques. En dépit des interrogations du médecin légiste, les conclusions d'un premier sachant furent trop hâtives, conduisant les proches à inventer des scénarios pour charger encore plus l'auteur. Mais cela a pu être corrigé en reconstitution et confirmé par des essais. Le mis en cause n'avait pas menti !

Enfin, l'expertise en balistique peut être déterminante pour apporter des éléments à décharge. Encore faut-il creuser pour ne pas les manquer.

Dans le dossier K, une rixe entre bandes pour un point de deal se concluait par des tirs de kalachnikov par les jeunes du quartier et un mort dans la bande adverse. Tous s'accordent sur l'identité du tireur qui lui même s'incrimine. La balistique conduit pourtant à une relaxe.

Dans le dossier C, dans un échange de coups de feu où il y aura 3 morts, les tirs s'arrêtent lorsque l'auteur survivant termine de vider son chargeur en finissant au sol l'autre tireur. A la suite des conclusions balistiques, l'auteur survivant obtiendra la relaxe pour l'homicide...mais tout de même pas pour le port d'arme illégal.

Dans le dossier B, l'ADN d'un suspect "très défavorablement connu" est retrouvé sur un talon de chargeur Walther / Manuhin retrouvé sur la scène de crime. La victime a été tuée de 3 balles 9 mm de 8 grammes en plomb par un seul tireur. Les projectiles ne sont pas marqués par des rayures. 3 étuis 9 mm Parabellum sont au sol et ont été tirés dans une seule arme. Il en est conclu que le suspect a tiré dans un pistolet Walther / Manurhin (ou un clone à blanc) trafiqué pour tiré à balle. Sauf qu'il y a un "drag mark" sur les percussions, donc que l'arme du meurtre est Incompatible avec le chargeur !

Certes l'ADN appartenait une personne défavorablement connue...mais de là à lui attribuer le meurtre de son ami...

****

SOMMAIRE

Dangerosité(s) :
Quelles évaluations pour le psychiatre expert ?

Dr Marc Schweitzer, MD, PHD.
Expert psychiatre près la Cour d'Appel de Paris

La *dangerosité potentielle d'un individu* reste une question omniprésente dans le contexte sociétal actuel. Toutefois, elle est éludée ou abordée indirectement avec l'utilisation de diverses paraphrases et reprise en termes de risque de récidive ou d'implication dans des activités marginales, criminelles ou mafieuses.
La terminologie la plus fréquemment utilisée a été celle *d'individu dangereux,* ce qui implique une certaine confusion entre la possibilité de devenir, d'être et un état induisant une action dangereuse pour autrui. Cette action est susceptible d'être activée par un ensemble de facteurs personnels, environnementaux, sociaux ou politiques.

Débattue au fil des temps, mais aussi par les aliénistes, la notion de dangerosité reste attachée aux représentations collectives et à leurs évolutions en raison des conceptions de la maladie mentale et des troubles psychiques, le crime ayant été longtemps associé à la folie et aux troubles psychiatriques.
La figure du « *fou dangereux* » s'est effacée progressivement, sans pour autant disparaître des représentations contemporaines, telle la réapparition de formules telles la « *folie meurtrière »* nous le rappelle.

Dès le début du XIXème siècle, le Code pénal (1810) avec l'article 64 attribuait aux médecins et aliénistes chargés des expertises mentales un rôle dans l'évaluation de la responsabilité des auteurs de crimes. Plus tardivement, des missions spécifiques apparaitront : examen psychiatrique par les neuropsychiatriques et psychiatres, puis -à partir de 1958– examen médico-psychologique en dualité médecin-psychologue.

La notion de Dangerosité est développée par les des théories positivistes du 19ème siècle, dans un contexte de *Défense sociale* et le souci de protection contre le crime. La « *dangerosité criminelle* » a dominé le dernier tiers du XIXème siècle, s'est prolongée prolongera au 20ème siècle avec les travaux des criminologues qui avaient développé l'idée d'une la personnalité criminelle (De Greff, Pinatel).

Au 20ème siècle, les apports des sciences sociales et les évolutions des chimiothérapies ont permis de s'éloigner de la pensée « déterministe » et d'envisager une possible amélioration symptomatique avec des soins spécialisés et institutionnels.

Sur le plan législatif, le Code Pénal de 1810 a fonctionné avec l'article 64 et la notion de démence au moment des faits jusqu'à la loi du 22 juillet 1992.
Avec cette loi, le rôle dévolu à l'expert psychiatre porte sur l'évaluation de troubles psychiques au moment des faits (art 122 du CP) et leur incidence sur le discernement (altération/abolition) dont, pour le magistrat, peut ou non découler la responsabilité pénale de l'auteur.

Dans un contexte de recrudescences d'homicides particulièrement violents, de nombreux Rapports parlementaires (Rapport Burgelin, Lamanda, Fennech, Garraud…) seront consacrés à la Dangerosité entre 2004 et 2006 ; il en est résulté un mouvement législatif avec la finalité régulièrement réaffirmée de « *renforcer les modalités de lutte contre la récidive* ».
Ces dispositifs ont renforcé le rôle de l'expert psychiatre en l'impliquant à plusieurs niveaux de procédure. Ainsi la loi du 12 décembre 2005 (lutte contre la récidive) a introduit *« l'expertise de dangerosité »* et la mise en place des premières Mesure de Sureté (placement sous Surveillance Judiciaire) . La loi du 25 février 2008 développera les mesures de sureté (*Surveillance de sureté* et de *Rétention de sureté*), procédures impliquant l'avis d'un psychiatre expert au regard de la dangerosité potentielle de la personne concernée, même à distance des faits.

Au cours de cette intervention, nous examinerons dans un premier temps la pluralité des interventions de l'expert psychiatre dans l'évaluation de la dangerosité et ce, à différents temps de la procédure judiciaire (instruction, post-sentenciel, aménagements de peines).

L'insécurité sociale ressentie à présent par une partie de la population est largement relayée par les médias, ce qui contribue à une approche globale de problèmes qui renvoie à diverses questions de société et qui restent très éloignées de la spécificité des missions pour lesquelles un expert psychiatre est désigné. Ceci nous avait conduit il y a quelques années à insister sur la distinction entre *dangerosité psychiatrique* et *dangerosité criminologique.* Cependant, ces distinctions, difficilement à admises à une époque,

apparaissent maintenant dans les missions d'examen psychiatrique et parfois d'examen psychologique, comme en témoigne la question : « *dire si l'intéressé présente un état dangereux au sens psychiatrique ou criminologique, en énumérant les éléments de pronostic défavorables ou favorables »*

Nous examinerons dans un second temps le rôle de l'expert psychiatre dans une démarche individuelle (celle de l'expertise psychiatrique) en le distinguant du rôle de l'expert dans une dimension collective au sein d'une approche pluridisciplinaire (CNE et CPMS), inscrite dans un cadre institutionnel et procédural.

Nous évoquerons aussi les questions nouvelles apparues à la suite des attentats terroristes, notamment les questions concernant l'évaluation de la dangerosité des personnes condamnées pour une infraction à caractère terroriste, lorsque ces personnes parviennent en fin de peine (loi du 30 juillet 2021

Nous nous nous interrogerons sur les mesures prises et -puisqu'il a été prévu que nous évoquerions aujourd'hui le ***futur du domaine du crime*** et de ses acteurs- ce qui en résulte dans le cadre des formations universitaires et professionnelles.

Dans un avenir proche, on pourrait assister à un élargissement des professionnels s'autorisant à intervenir dans l'appréciation d'une dangerosité potentielle chez tout individu mis en examen.
Nous reviendrions alors à une approche globalisante d'une situation et non d'un individu et nous éloignerions de la question posée dans la mission psychiatrique.

Quelques Lectures ?

CONTE Philippe et TZITZIS Stamatios, Dir*., Essais de philosophie pénale et de criminologie,* Editions Dalloz.

HANAFY Isis, MARC Bernard, *Dictionnaire médico-psycho-légal,* Des normes sociétales et de la violence humaine, Paris, Editions in Press, 2017, 332 p.

SOMMAIRE

L’expert aux assises : point de vue du magistrat

Muriel JOSIÉ

Présidente de chambre à la cour d'appel de Paris

En charge des assises

La déposition de l’expert devant la cour d’assises répond à la nécessité d’éclairer la Justice sur des domaines techniques qui ne sont pas de sa compétence.

Cette déposition est régie par les grands principes qui prévalent devant cette juridiction : oralité des débats, principe du contradictoire.

La déposition peut se faire en présentiel à la barre ou en visioconférence.

L’exercice de la déposition aux assises suppose de maîtriser certains aspects pratiques tout en gardant à l’esprit que cette déposition se déroule sous l’autorité attentive et bienveillante du président de la cour d’assises.

****

SOMMAIRE

Expertise et levée de corps - L'expert et la déposition en cours d'Assises

Henry COUDANE
Professeur émérite, Université de Nancy, Doyen honoraire
Expert agréé par la Cour de cassation

Le médecin légiste de garde est prévenu par la gendarmerie de la découverte d'un corps dans un hôtel de la Meuse. Les renseignements fournis par la gendarmerie permettent de savoir que cet homme d'une quarantaine d'année est arrivé la veille, a payé une nuit en espèces et ressorti pour faire des courses pour rejoindre sa chambre vers 19h.Il a demandé qu'on lui monte pour 21h un plateau repas. Ne répondant pas aux sollicitations du personnel (à la porte de sa chambre et par téléphone) la direction de l'hôtel pénètre dans la chambre vers 21h35 et retrouve l'homme étendu sur lit « un couteau planté dans la région cardiaque ». Les services de gendarmerie sont sur place à 22H12 La recherche de l'identité est restée vaine car les premiers constats n'ont pas permis de retrouver les papiers d'identité. Le médecin légiste est sur la scène à 23H12 et retrouve un homme de type caucasien mesurant environ un mètre 80, avec un couteau à manche de bois situé dans la région xiphoïdienne ; du sang coagulé stagne dans la région ombilicale. Il n'y a pas de rigidité cadavérique, pas d'hématome ou d'ecchymoses ; il n'y a pas de signes de strangulation pas de tache verte ou de gonflement abdominal. La température rectale est à 36,2. Le médecin légiste retrouve des cicatrices fines mesurant environ 16 cm dans les régions postéro externes des fesses droite et gauche.

Sur la table nuit était déposée une bouteille de whisky à demi vide.et une boite de diazépam avec un emballage- blister entamé dans lequel manquaient 10 comprimés.

Le médecin légiste demande le transfert du corps pour autopsie à l'Institut médico-légal.

Les radiographies réalisées retrouvent un corps étranger métallique se projetant au niveau de la région cardiaque en forme de lame de coureau mesurant 21 cm de long ; la radiographie du bassin retrouve la présence de deux prothèses de hanche non cimentées. Ces prothèses seront extraites lors de l'autopsie : les cols prothétiques sont porteurs d'une référence qui sera communiquée aux enquêteurs. Elle permettra de retrouver le fabriquant des implants et l'établissement hospitalier ou elles furent livrées aux Pays Bas. L'indentification de la victime fut alors possible.

Par ailleurs l'autopsie permis d'établir les causes de la mort : plaie du cœur par lame de couteau, avec hémothorax ; 10 comprimés de diazépam furent retrouvés dans le contenu gastrique. L'analyse toxicologique retrouvait une alcoolémie à 3,8 g/l. Le reste de l'analyse toxicologique était négative.

En résumé : la levée de corps a permis de dater l' heure de la mort et l' examen clique de retrouver les cicatrices d'interventions chirurgicales et d'orienter l' autopsie qui a nécessité l' ablation de deux prothèses de hanches permettant l' identification de la victime .L' enquête devait montrer que la victime de nationalité hollandaise avait décidé de mettre fin à ses jour en France (pour un rejoindre une compagne qui l' avait délaissé) en utilisant un mode de suicide particulier (suicide de type rituel japonais par couteau)après avoir ingéré un demi litre de whisky.

<u>La déposition de l'Expert aux assises est un exercice parfois périlleux qui nécessite une préparation …</u>

L'affaire de Me W. avait eu en 1991 un impact médiatique important .Sur le plan médico-légal il s'agissait de « l' autopsie » d'un tronc retrouvé dans la Marne dont il fallait confirmer l' identité ; à l' époque la technique des empreintes génétiques n'existait pas Deux experts avaient été nommés (un professeur de radiologie et un de chirurgie orthopédique et de médecine légale) .Les dossiers médicaux avaient pu être récupérés dans différents services de médecine et de chirurgie : l'un de ces dossiers comportait une radiographie du bassin et d'une partie de la colonne lombaire effectuée dans le cadre du bilan du patient qui devait être opéré d'une lésion méniscale du genou droit (c'était bien avant l' époque des arthroscopies du genou)4 ans avant sa disparition. A partir de la radiographie du bassin du tronc les experts ont tiré à l' échelle des calques et effectué une comparaison qui a permis de retrouver une concordance de tous les éléments squelettiques et en particulier l' existence sur la radio préopératoire d'une anomalie de la jonction L5/S1 (lyse isthmique bilatérale) associée à une coxarthrose débutante identique sur les 2 clichés .Par ailleurs les prélèvements effectués sur le tronc avaient permis de retrouver le groupe sanguin du tronc qui correspondait à celui du patient .Un second dossier médical faisait état d'une hospitalisation en urgence avec à l' examen toxicologique une intoxication au Diazépam ; dans le dossier médical le Chef de clinique de l' époque avait noté « j'ai rencontré la compagne du patient qui m' a précisé que ce dernier ne prenait aucun médicament mais que son compagnon chauffeur routier avait tendance à s'endormir au volant ; elle n' a pas voulu répondre à d'autres questions et elle m' a paru très bizarre »

Les conclusions des Experts faisaient état d'une « concordance entre le tronc étudié et le patient disparu sans pour autant pouvoir conclure en une similitude absolue. Lors de la session des assises de la Meurthe et Moselle l'un des experts devait déposer : il confirmait que l'anomalie retrouvée au niveau vertébral étaient certes rare et que son existence associée aux autres pathologies décrites

était en faveur d'une concordance sans que l'on puisse parler de certitude absolue. L'avocat de la mise en cause devait alors poser de multiples questions sur la fréquence dans la population générale des lyses isthmiques bilatérales, des groupes sanguins de la coxarthrose : l'expert y répondit simplement et insista sur les similitudes sans pouvoir affirmer la notion d'identité absolue.

En résumé : la patiente fut condamnée à 20 ans de réclusion criminelle en particulier pour l'assassinat de son compagnon qu'elle avait démembré avec une meuleuse à béton, mis dans une valise lestée par des parpaings et jetée dans la Marne à plus de 300 km des faits .Il faut noter aussi que dans la procédure le juge d'instruction avait demandé des analyses techniques sur les parpaings sur l'origine de la valise qui avaient permis de retrouver des achats proches du lieu où résidait la mise en cause …

En résumé :

La déposition par l' expert aux assises est parfois un exercice périlleux ; elle nécessite une préparation qui peut être résumée de la façon suivante : reprendre connaissance des rapports réalisés , en cas d'autopsie vérifier les différentes étapes et reprendre connaissance des examens complémentaires (anatomo-pathologie , toxicologie) ; ne pas se présenter avec tout le dossier médico-légal dans les mains à la barre , toujours regarder la présidente ou le président de la cour d' Assises ; ne jamais se retourner pour répondre directement aux questions des avocats…qui ne manqueront pas de déstabiliser l' expert qui doit rester simple, factuel et didactique dans ses propos ; ne jamais rentrer dans le domaine de l' interprétation , des querelles d' écoles .Et au besoin ne pas hésiter à dire « je ne peux pas répondre à cette question en fonction des données confirmées de la science médico-légale »

Dans le cas rapporté, la patiente après avoir exécuté sa peine, a envoyé un courrier à l'adresse personnelle de l'expert en lui précisant qu'elle n'avait jamais commis d'assassinat et que si elle l'avait fait elle aurait dû être condamnée à une peine bien supérieure à 20 ans de réclusion …

****

SOMMAIRE

L'ÉVOLUTION RELATIVE AU JUGEMENT DES CRIMES

Sylvie Ménotti, conseiller honoraire,
membre de la formation de jugement de la Cour de justice de la République
13 OCTOBRE 2023

La cour d'assises juge classiquement les crimes.

LA NAISSANCE DE LA COUR D'ASSISES

La cour d'assises est née d'un **élan révolutionnaire**, souhaitant une justice rendue, au nom du peuple français, par des représentants du peuple.

Mais elle présentait de nombreux inconvénients :
1) la **composition du jury** en faisait initialement une justice de classe ;
2) la **distribution des rôles entre les jurés, statuant sur la culpabilité, et les juges, statuant sur la peine**, a produit des effets pervers et des acquittements scandaleux.

Il a donc fallu trouver des remèdes :
1) tirage au sort des jurés sur la liste électorale pour en faire un jury véritable « populaire » ;
2) compétence des juges et des jurés pour statuer, ensemble, tant sur la culpabilité que sur la peine ;
3) audition des experts à l'audience pour contrecarrer « l'incompétence » des jurés.

LES RÉFORMES INTERVENUES DANS LE FONCTIONNEMENT DE LA COUR D'ASSISES POUR SATISFAIRE, NOTAMMENT, AUX CANONS EUROPÉENS

La loi du 15/06/2000 :
- a crée le **droit d'appel** contre les décisions des cours d'assises :
- a donné aux avocats et aux jurés le **droit de poser des questions directement à l'audience** après avoir demandé la parole au président.

La loi du 10 août 2011 a imposé l'**obligation de motivation des décisions** des cours d'assises.

La loi du 27 mai 2014 a consacré le **droit au silence de l'accusé**.

UNE REMISE EN QUESTION DE LA PRÉSENCE DES JURÉS POUR CERTAINES AFFAIRES

Une remise en question de la présence de jurés en raison de la défaillance de ceux-ci pour certains types d'affaires

La loi du 9 septembre 1986 a instauré une **cour d'assises spéciale pour juger les crimes terroristes**, composée uniquement de magistrats professionnels (article 698-6 CPP).

La loi du 16 décembre 1992 a fait de même **pour les faits les plus graves en matière de trafic de stupéfiants** (article 706-27 CPP).

Une remise en question de la présence des jurés en raison d'une bonne administration de la justice

Deux considérations :
1) **un procès d'assises est très chronophage** car les jurés n'ont pas accès au dossier et qu'il faut donc faire comparaître, à l'audience, tous les témoins ou tous les experts dont l'audition peut être utile à la manifestation de la vérité ;
2) **les stocks des affaires criminelles** à juger se sont accrus ces dernières années.

La pratique de la correctionnalisation

Cela consiste à **« oublier » volontairement une circonstance qui rend criminel un agissement**, et ce, afin de le faire juger comme un délit. Il faut, bien évidemment, que toutes les parties au procès en soient d'accord.

La création des cours criminelles départementales

Les CCD ont été créées par la loi du 23 mars 2019 à titre expérimental.
Elles ont été **généralisées par une loi** du 21 décembre 2021 **entrée en vigueur le 1er janvier 2023**.

Elles sont compétentes pour juger :
- les crimes commis par les majeurs ;
- faisant encourir 15 ou 20 ans de réclusion criminelle ;
- lorsque l'accusé n'est pas en état de récidive.

Elles statuent en 1er ressort et est uniquement composé de **5 magistrats professionnels**, sans juré.

Elles ont vocation à « réduire le format » de la cour d'assises classique, afin de gagner du temps.

Elles ont été vivement critiquées sur plusieurs points :
1) elles seraient contraires au principe du jury populaire ;
2) elles porteraient atteinte au principe d'égalité des citoyens devant la justice :
    * problème de l'oralité des débats ;
    * problème des règles de majorité.

La cour de cassation, saisie d'une question prioritaire de constitutionnalité concernant les CCD, les a renvoyées au Conseil constitutionnel, par des arrêts du 20 septembre 2023.

Le Conseil constitutionnel doit se prononcer dans les 3 mois, soit avant la fin du mois de décembre 2023, sur la constitutionnalité des CCD, question qui reste donc en suspens.

Il ne faut pas non plus méconnaître la **dimension « restauratrice », pour les victimes, des procès d'assises**, tels qu'en témoignent les procès d'assises en matière terroriste. La CCD peut-elle répondre à une telle attente ?

SOMMAIRE

Quelle confiance accorder aux serrures en criminalistique ?

David ELKOUBI
Expert en traces et empreintes près la cour d'appel de Chambéry

Il est commun de penser que, si elles n'ont pas la prétention d'être parfaitement « inviolables » les serrures verrouillées, et leurs l'ouvertures d'une manière illégitime, constituent tout de même un bon indicateur de la commission d'une intrusion illicite.

Mais envisageons-nous avec suffisamment de conscience et de manière suffisamment méthodique, l'ouverture « fantomatique » d'une serrure par un intrus ?

Est-il possible d'ouvrir et de refermer une serrure, sans la clé d'origine, et sans laisser de traces ?

Et comment appréhender cette possibilité de manière objective et sans projeter de manière utopique ce qui est réellement possible ?

Y a-t-il des cas probants ?

Qu'en est-il des modes opératoires retrouvés actuellement sur des affaires récentes ?

Nous allons vous présenter l'expertise en intrusion furtive.

******

SOMMAIRE

Sabine KHERIS

1ère Vice-Présidente chargée de l'instruction

Coordonnatrice du pôle national des crimes non élucidés, sériels et complexe

Plan de l'intervention

1) les raisons de la création du pôle des crimes sériels ou non élucidés (pôle cold case)

2) la création du pôle

3) le but du pôle : traiter des dossiers anciens avec des techniques innovantes :

-techniques innovantes en sciences humaines

-techniques innovantes en génétique et physique

-techniques innovantes en matière anthropologique

-techniques innovantes en fouille opérationnelle

-l'apport de l'intelligence artificielle dans le traitement du cold case

****

SOMMAIRE

Le Commandement de la Gendarmerie dans le cyberespace (ComCyberGend)

La « menace cyber », pour définir des actions menées par une entité ou un individu ayant recours au monde virtuel de l'Internet, est devenue un fléau à la mesure du développement des technologies et de la rapidité des échanges, mêlée à la puissance de l'environnement informatique (structure réseau, stockage plus important et réduit, etc.).
Pour assurer la fonction « sécurité » tout en assurant une certaine autonomie de décision stratégique, les États n'ont d'autre choix que d'investir dans leur moyen « cyber ». Positionnée à la croisée de plusieurs thématiques régaliennes, la Gendarmerie nationale a depuis longtemps investi le champ du développement de son offre cyber, et se transforme pour pouvoir participer en coordination et en collaboration avec d'autres opérateurs, privés et publics, aux prochains défis de notre siècle.

La création du commandement de la gendarmerie dans le cyberespace (ComCyberGend) s'inscrit dès lors dans la nouvelle stratégie nationale de cybersécurité du ministère de l'Intérieur et des Outre-mer, et dans la volonté de la Gendarmerie nationale d'accompagner et protéger les Français dans leur vie numérique.
Directement rattaché au Directeur Général de la Gendarmerie Nationale (DGGN), le ComCyberGend assure la coordination stratégique et opérationnelle des 9000 cybergendarmes, présents :

✓ dans les territoires (brigades territoriales),
✓ à l'échelle départementale (100 sections opérationnelles de lutte contre les cybermenaces),
✓ au niveau régional (12 antennes du centre de lutte contre les criminalités numériques – C3N)
✓ et au niveau national pour les opérations du très haut du spectre (C3N).

Articulé autour de quatre divisions, le ComCyberGend s'appuie sur cinq fonctions principales :

✓ Prévention : travail en collaboration avec les collectivités locales, les TPE/PME, l'ANSSI, Cybermalveillance.gouv.fr, etc.
✓ Proximité numérique : magendarmerie.fr (brigade numérique) et le réseau territorial CyberGEND ;
✓ Interventions et investigations : opérations dans le cyberespace dans une vision globale du bas au très haut du spectre ;
✓ Appui numérique aux opérations : recherche et innovation ;
✓ Partenariats territoriaux et nationaux.

Porteur de la stratégie et de l'action de la Gendarmerie nationale dans le cyberespace, il bénéficie en outre, au sein du Campus Cyber, d'une proximité avec d'autres acteurs de l'État, du monde industriel, de la recherche ou encore universitaire. S'insérer dans cet écosystème d'innovation et d'échange offre à la gendarmerie un espace propice à la cohérence stratégique et à l'entretien de partenariats pérennes. Parallèlement à son implantation au sein de cette structure unique, le Campus Cyber, le ComCybergend s'appuie et s'articule autour de plusieurs acteurs :

- les brigades territoriales
- le réseau CyberGEND, composé de militaires titulaires d'une ou plusieurs formations qualifiantes, telles enquêteur sous pseudonyme (ESP), nouvelles technologies (N-TECH) ou enquêteur numérique spécialisé en crypto-actifs (FINTECH),
- au niveau central, le Centre de lutte contre les criminalités numériques (C3N) est l'unité de police judiciaire à compétence nationale de la gendarmerie en matière de lutte contre la cybercriminalité.

Le C3N représente la gendarmerie dans les instances de coopération opérationnelle d'Europol, et en particulier auprès du Centre européen de lutte contre la cybercriminalité (EC3).
- les 12 antennes C3N, réparties sur l'ensemble du territoire national, au sein des sections de recherches implantées sur le chef-lieu d'une juridiction interrégionale spécialisée (JIRS), notamment pour la direction des investigations relatives aux infractions spécifiques cyber relevant de leur zone de compétence respective, ainsi qu'aux infractions non spécifiques relevant de la compétence de la JIRS.
- rattaché au C3N, le Centre national d'analyse des images de pédopornographie (CNAIP) a quant à lui pour mission d'identifier les victimes et auteurs des contenus à caractère pédopornographique. Cette structure centralise pour la police et la gendarmerie les fichiers saisis lors des enquêtes judiciaires et fournit des images illicites aux enquêteurs habilités aux investigations sous pseudonyme.

L'ensemble de ces acteurs, ouvrant en totale coordination, s'appuient en outre sur deux volets structurants, qui caractérisent le ComCybergend : prévention/partenariat et assistance cyber.

Face à une diversification de la menace cyber, accentuée par l'Intelligence Artificielle (IA), tel ChatGPT, le déploiement de la 5G ou encore l'essor des objets connectés, la sensibilisation et l'accompagnement de la population, ainsi que des acteurs publics et privés dans leur vie numérique, revêtent en effet un caractère primordial.
En partenariat avec l'ensemble des acteurs participant à diffuser une culture de la cybersécurité, le ComCyberGend élabore ainsi des contenus visant à diffuser une prise de conscience du risque lié à l'utilisation des technologies numériques, et ce dans le but de mieux s'en prémunir et d'évoluer en sécurité sur les réseaux.
Par le biais de communications ciblées ou plus larges, d'événements organisés sur des espaces privilégiés par les usagers concernés, il entretient dès lors la vigilance de chacun et la confiance numérique. S'appuyant sur des infographies accessibles à tous les usagers, parents comme enfants, et sur des diagnostics simples au profit des entreprises de toutes tailles et des collectivités territoriales, les actions de prévention conduites en partenariat notamment avec le dispositif national de prévention et d'assistance Cybermalveillance.gouv.fr visent ainsi à infuser une culture de la cybersécurité dans les foyers, et à améliorer le niveau de sécurité numérique des établissements publics comme privés.

Parmi ces communications figurent « Les risques Internet pour les enfants : que peuvent faire les parents ? », « Mots de passe : les bons réflexes », ou encore le « Petit logiciel illustré ». Par ailleurs, près de 150 000 élèves de primaire ont été sensibilisés à l'occasion de l'opération « Permis Internet » en 2022, en métropole et en Outre-mer.
Aussi, au profit des entreprises et des hôpitaux, de nombreux webinaires de sensibilisation à la cybersécurité ont été animés, et de nombreuses communications ont été diffusées par la Gendarmerie nationale pendant la crise sanitaire, pour faire face aux nouvelles cybermenaces. En 2022, ce sont ainsi 7 500 entreprises qui ont fait l'objet d'une action de prévention visant à lutter contre les cybermenaces dont elles pourraient faire l'objet.
Enfin, en 2022, plus de 8000 actions de sensibilisation aux cybermenaces destinées aux élus, collectivités territoriales et établissements publics, ont été menées, alors qu'environ un tiers des collectivités territoriales affirmant avoir été touché par un rançongiciel a bénéficié d'un pré-diagonostic cyber « Di@gonal », outil d'aide permettant d'appréhender et de mieux circonscrire les vulnérabilités souvent ignorées.

Complémentaires de ces actions de sensibilisation et de prévention, les opérations d'investigations numériques, soutenues par le Centre national d'assistance cyber du COMCyberGEND, apportent 24 heures sur 24 et 7 jours sur 7 un appui opérationnel aux enquêteurs des unités de la gendarmerie

dans leurs relations avec les opérateurs de téléphonie, les fournisseurs d'accès à Internet et de services numériques. Cette structure propose également une interface d'assistance technique au niveau national, destinée aux enquêteurs de la gendarmerie et aux services d'enquête partenaires dans leurs investigations liées à la téléphonie et à Internet.
En outre, ce Centre entretient un lien permanent avec les partenaires de la gendarmerie, et concourt aux réunions de contacts avec les « géants du web » et les opérateurs de communications pour améliorer le processus de réquisition, accélérer les demandes urgentes, valider des recherches spécifiques et suivre les évolutions technologiques. Il est par ailleurs proactif dans l'enrichissement de son réseau de contact auprès des entreprises développant une activité de service dans le numérique, en particulier sur la thématique des objets connectés et des nouveaux moyens de communication.
Enfin, le Centre national d'assistance cyber contribue à la formation des enquêteurs de la gendarmerie et entreprend des études sur diverses problématiques numériques, au premier rang desquels se situent les technologies numériques et leur évolution continue, les réseaux sociaux et leurs usages, les relations avec les services Internet français ou étrangers, la dématérialisation des services, mais aussi les processus de diffusion de l'information.

Le ComCyberGend assume donc, dans le cyberespace, l'un des impératifs majeurs de la gendarmerie au quotidien : entretenir et consolider le lien avec la population qu'elle protège. Il incarne la composante numérique que toute mission de la gendarmerie comporte désormais, et exerce ses missions sur l'ensemble du territoire national, en appui ou au profit de l'ensemble des unités de l'Arme.
Le ComCyberGend développe en somme des compétences criminalistiques de haut niveau sur tout le territoire national, en métropole et en Outre-mer. Pour cela, il s'appuie sur ses enquêteurs N-TECH, au sein des plateaux techniques départementaux, et sur des experts en capacité de procéder à l'analyse des supports numériques, d'être projetés sur le terrain si nécessaire lors de perquisitions ou d'auditions en milieu complexe, et de concevoir et développer des outils cyber orientés sur l'investigation numérique et destinés à l'usage des enquêteurs sur le terrain.

Les compétences du ComCyberGend s'illustrent enfin dans le domaine des fraudes aux moyens de paiement en ligne, par le biais de la plateforme PERCEV@L. Cette dernière vise à lutter contre la fraude à la carte bancaire sur Internet. Elle permet à tout internaute de signaler aux forces de l'ordre un ou plusieurs usages frauduleux, et est développée et administrée par la Division Proximité Numérique (DPNUM) du ComCyberGend.
L'usager de la plateforme peut ainsi signaler toute transaction par carte bancaire dont il n'est pas à l'origine, alors qu'il est toujours en sa possession. PERCEV@L, à vocation exclusivement judiciaire, permet ainsi de rapprocher des faits dont le préjudice est individuellement faible, de matérialiser d'emblée des atteintes lourdes et sérielles, d'identifier des suspects, puis de saisir les services d'enquête de la gendarmerie et de la police nationales.

A l'approche de grandes échéances, telle la Coupe du Monde de Rugby 2023 et les Jeux Olympiques et Paralympiques Paris 2024, mais aussi au regard du caractère hybride de la menace, le ComCyberGend, fort de son maillage « cyber » étendu sur tout le territoire national, de ses structures et de ses partenaires européens et internationaux, poursuit inlassablement sa volonté de remplir le triptyque missionnel : anticiper, accompagner, enquêter.
Véritable espace à part entière où œuvrent les cyberdélinquants, le cyberespace nécessite en somme une vigilance et une adaptation constantes, pour lesquelles le ComCyberGend reste, aux côtés de ses nombreux partenaires, plus que jamais mobilisé.

****

SOMMAIRE

Le crime hors de nos frontières et hors du temps

Roch MENES
Président d'honneur de la CNEMJ
Expert honoraire près la cour d'appel de Riom
Membre du conseil d'administration de l'EEEI

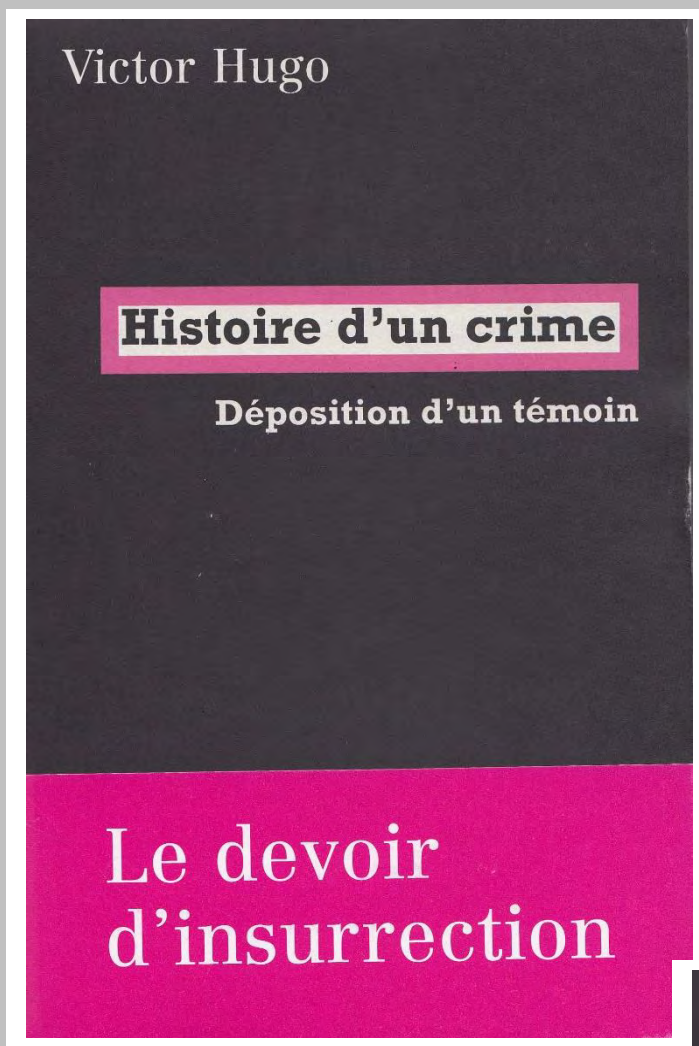
Dès le Moyen-Age le Droit Romain s'était imposé des rivages sud de la Méditerranée aux embouchures des fleuves s'ouvrant dans la mer du Nord. Rien ne semblait pouvoir remettre en cause cette institution. Mais le droit romain était administré en LATIN – une langue déjà morte, partagé seulement par les clercs et les savants. Dès lors notre Droit Romano-Civiliste était condamné à terme faute d'avoir su se remettre en question et s'adapter à l'évolution du monde.

A l'opposé le régime dit de *Common Law* (Commune Ley – le Droit étant administré en français jusqu'en 1650 par les Cours Royales siégeant à Westminster) pour harmoniser les différentes juridictions à travers le Royaume, s'est développé au sein, d'une communauté de langage, s'infiltrant dans le doit des affaires, le commerce l'industrie, l'informatique.

Comme la langue anglaise, la Common Law s'infiltre partout. Grace à la télévision il n'est pas rare d'entendre les jeunes, victimes ou mis en cause, répondre au Président du Tribunal en le qualifiant de « Votre Honneur »

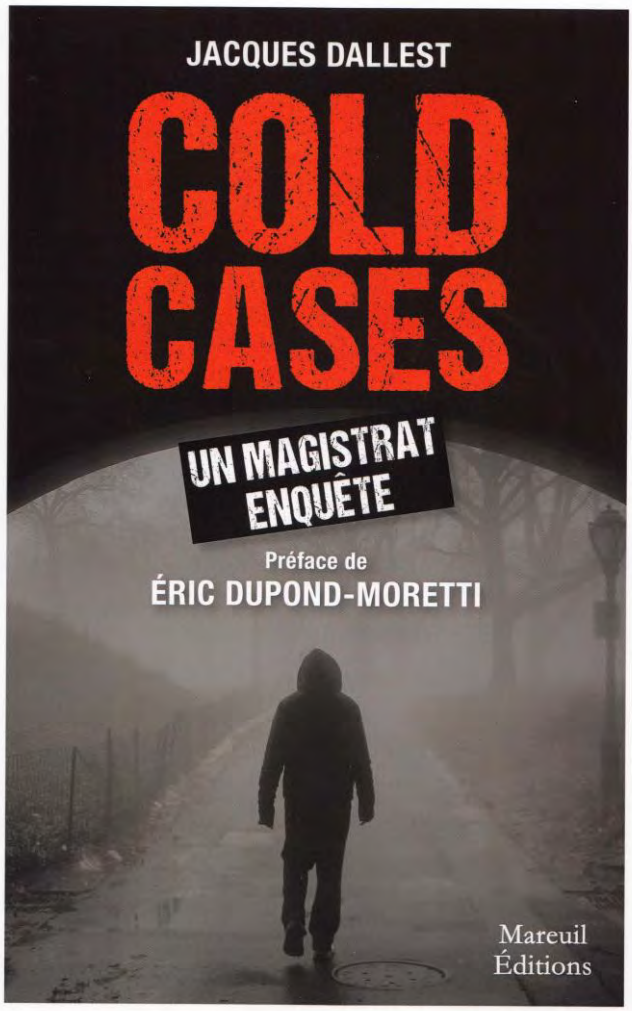
Dès lors, tout en défendant notre patrimoine juridique hérité du Droit Romain, il apparait nécessaire d'appréhender les bases d'un système judiciaire pratiqué par des millions d'individus à travers le monde, que ces pays aient ou non conservé leurs liens avec la Couronne.

****



SOMMAIRE

« Malheur à qui resterait impartial devant les plaies sanglantes de la liberté ! » *Histoire d'un crime* est tout sauf un livre impartial. C'est le récit, à la première personne du singulier, d'un homme qui était à la veille du 2 décembre 1851 un écrivain illustre, académicien, pair de France sous Louis-Philippe, député à l'Assemblée législative, et qui soudain devient un proscrit. Errant d'appartements d'amis en arrière-salles de marchands de vin, Hugo tente d'organiser la résistance au coup d'État, de soulever le faubourg Saint-Antoine, avec Schœlcher, avec de Flotte, avec Baudin qui s'y fera tuer (« J'aperçus, à cent pas devant nous, au point de jonction de la rue de Cotte et de la rue Sainte-Marguerite, une barricade très basse que les soldats défaisaient. On emportait un cadavre. C'était Baudin. ») Il croise les futurs notables du Second Empire (« Tiens ! me dit M. Mérimée, je vous cherchais. Je lui répondis : j'espère que vous ne me trouverez pas. Il me tendit la main, je lui tournai le dos. ») Il visite les barricades dressées au centre du vieux Paris, « Une à la pointe Saint-Eustache. Une à la Halle aux huîtres. Une rue Mauconseil. Une rue Tiquetonne… Une plus avant dans la rue Greneta barrant la rue Bourg-l'Abbé (au centre une voiture de farine renversée ; bonne barricade)… »
Dans la soirée, « je rentrai dans mon asile. J'étais las, j'avais faim, j'eus recours au chocolat de Charamaule et à un peu de pain qui me restait ; je me laissai tomber dans un fauteuil, je mangeai et je dormis. »
Un récit heure par heure d'événements oubliés, un document exceptionnel contre la réhabilitation rampante de Louis Bonaparte.



SOMMAIRE

JACQUES DALLEST

COLD CASES

L'histoire criminelle est jalonnée d'assassinats sordides, de meurtres sauvages, de disparitions énigmatiques et de suicides étranges. « Énigmatiques » et « étranges », car ces affaires n'ont jamais été résolues, leurs auteurs jamais identifiés, les coupables jamais condamnés. Ces dossiers, sont appelés en bon français des « *cold cases* ». Ils se chiffrent par dizaines, et sont souvent inconnus du grand public. Seules quelques grandes affaires restées inexpliquées sont inscrites dans les tablettes de l'histoire judiciaire et suscitent toujours débats et interrogations ; l'affaire de Bruay-en-Artois, l'affaire Fontanet, l'affaire Grégory, l'affaire Boulin, ou, plus récemment, la tuerie de Chevaline.

Mais qu'appelle-t-on un *cold case* ? Quelle signification ce terme anglo-saxon revêt-il dans notre paysage judiciaire français ? Doit-on rouvrir ces dossiers ? Comment peut-on leur trouver une issue après toutes ces années ?

Dans cet essai érudit et très documenté, Jacques Dallest, ancien juge d'instruction, procureur et avocat général, fait le point sur la question comme aucun livre ne l'avait fait auparavant.

Magistrat honoraire, ***Jacques Dallest*** *a été juge d'instruction, procureur de la République et procureur général. Il a enseigné pendant de nombreuses années au sein des facultés de droit de Lyon, Bordeaux et Chambéry, ainsi que dans les Instituts d'études politiques de Lyon et Aix-en-Provence. Il a exercé également en qualité de professeur associé à Sciences Po Grenoble. Il a dirigé plusieurs sessions de formation continue à l'École nationale de la magistrature (ENM), où il est un intervenant régulier. Il intervient par ailleurs à l'École nationale supérieure de la police.*

ISBN 978-2-372-54277-7
PRIX 22 EUROS TTC
Design : Le-petitatelier.com
Photo © Marianne Catafesta/Shutterstock

SOMMAIRE

L'avenir de la justice pénale internationale

Sous la direction de Jean Albert, Jean-Baptiste Merlin

Présentation de l'éditeur

Discipline relativement récente, le droit pénal international tient une place toujours plus grande dans le règlement des conflits depuis la fin de la Seconde Guerre mondiale. Pour autant, le chemin est encore long jusqu'à la fin de l'impunité.

En effet, bien que le droit pénal international ait connu de nets progrès depuis les années 1990, de nombreux obstacles demeurent à sa pleine effectivité, qui tiennent pour certains à la structure même de la communauté internationale.

Le présent ouvrage a pour ambition de mettre en perspective les obstacles actuels et défis à venir de la justice pénale internationale en matière de lutte contre l'impunité et la défense des droits fondamentaux. Entre éclairages juridiques doctrinaux et examen d'options pour l'action, cette étude fait vœu de réalisme et se veut une contribution à la fois aux plans théorique et pratique à un outil de résolution des conflits en pleine expansion.

L'ouvrage rassemble les contributions de : Alea Ben Rais, Cécilia Dumesnil, Donald M. Ferencz, Élise Le Gall, Agnès-Catherine Ndongo Obama, Henri Panjo et Ludivine Tomasso.

Sommaire

Macro Droit, 398 pages. 45€

SOMMAIRE

Faire parler les serrures : l'expertise en intrusion furtive ou la serrurerie forensique

David Elkoubi
Expert près la cour d'appel de Chambéry en Sciences Criminelles – traces et empreintes
Expert en intrusion et en technologies du renseignement
Formateur en intrusion tactique pour des unités spécialisées des ministères des Armées et de l'Intérieur
Intervient auprès de services de Police scientifique, de la Gendarmerie et de la Police

L'intrusion furtive réside dans l'ouverture puis la fermeture d'un local verrouillé, en l'absence de clé. L'effraction est réalisée à l'aide d'un ou de plusieurs instrument(s) spécifique(s), et ne dégradera pas forcément la serrure. Seule une expertise spécialisée peut déterminer si l'ouverture a réellement été commise et de quelle manière. L'expert devra connaître parfaitement le fonctionnement des différentes familles de serrures, maîtriser l'ensemble des méthodes d'effraction possibles, destructives ou non, et les principes physiques et mécaniques qui entrent en jeu.

Domaine assez méconnu, l'intrusion furtive qui réside dans l'ouverture puis la fermeture en l'absence de clé d'un local verrouillé, est néanmoins définie par le législateur.

Le Code pénal rappelle, en effet, en son article 311-5 alinéa 3 relatif au vol aggravé, que l'une de ces circonstances est établie : *« 3° Lorsqu'il est commis dans un local […] en pénétrant dans les lieux par ruse,* ***effraction*** *ou escalade. »*

« L'effraction » est quant à elle définie à l'article 132-73 du Code pénal[1] : *« L'effraction consiste dans le forcement, la dégradation ou la destruction de tout dispositif de fermeture ou de toute espèce de clôture. Est assimilé à l'effraction l'usage* ***de fausses clefs****, de clefs indûment obtenues ou de tout* ***instrument pouvant être frauduleusement employé*** *pour actionner un dispositif de fermeture* ***sans le forcer ni le dégrader****. »* Ainsi, le législateur :

1. Prend en compte la possibilité qu'un dispositif de fermeture verrouillé, puisse être ouvert sans sa clé légitime, et sans dégradation.
2. Considère ce mode opératoire comme une circonstance aggravante.
3. Assimile ce mode opératoire à l'effraction « classique » (avec casse).

Que ce soit dans le cadre de l'application de la loi pénale ou au regard des assurances (pour lesquelles le vol « sans effraction » est souvent une clause classique d'exonération de garantie), il est important de pouvoir se prononcer sur la réalité de cette effraction.

MAIS COMMENT LA DÉTERMINER ?

L'effraction réalisée à l'aide d'un (ou plusieurs) instrument(s) spécifique(s) ne dégradera pas forcément la serrure. Cette ouverture, par essence non destructive, reste néanmoins frauduleuse et donc punissable au regard de la législation. Mais comment savoir si l'ouverture a réellement été commise et de quelle manière ? Seule une expertise spécialisée peut apporter les réponses à ces questions.

PAR AILLEURS, QU'EN EST-IL DE LA RÉALITÉ DE CES PRATIQUES ?

Marotte des films d'action, l'ouverture sans force ni dégradation est-elle pour autant une réalité ?

Outre la simple carte de crédit glissée entre le chambranle et la porte (le type de déverrouillage « classique » que toute personne ayant claqué un jour sa porte en oubliant ses clés à l'intérieur a en tête) ce type d'ouverture est-il réellement possible ? Peut-on procéder au déverrouillage d'une porte à cinq points de verrouillage, voire blindée, sans laisser de traces évidentes ?

Nous allons, dans cet article, nous attacher à présenter l'étendue « invisible » de ces effractions dites « douces » et du travail d'expertise qu'il est possible de réaliser pour « faire parler » les serrures.

L'EFFRACTION « DOUCE » SANS TRACE APPARENTE, EST-CE POSSIBLE ? ET SI OUI, COMMENT FONCTIONNE-T-ELLE ?

Il est communément admis que, pour l'ouverture d'une « vraie » serrure (excepté donc les serrures très basiques) sans utilisation de la clé légitime, il faut soit casser celle-ci, soit casser l'élément sur lequel la serrure est fixée ou l'un des éléments de solidarisation de l'ensemble (porte, chambranle et pêne).

Pourtant, il est possible de s'attaquer au mécanisme de la serrure et ainsi agir sur lui « comme si une clé légitime était présente », sans pour autant l'avoir introduite.

Lors d'un « crochetage » par exemple (une des techniques « douces » parmi plus d'une quinzaine

Photo 1 : serrure tournée sans clé

d'autres), la serrure « tourne » sans que la clé ne soit à l'intérieur. Il devient alors possible de déverrouiller la porte. On peut même la refermer facilement, sans avoir à crocheter la serrure à nouveau.

Après l'ouverture et la fermeture de la serrure, aucune trace n'est visible de l'extérieur et la serrure continue de fonctionner comme avant.

QUELLES SONT LES SERRURES ET, PLUS GÉNÉRALEMENT, LES SYSTÈMES DE SÉCURITÉ CONCERNÉS PAR CES « RISQUES » ?

Plus un système sera bien pensé, plus il sera difficile de trouver le moyen de le contourner. Mais tout système comporte des failles. En ayant les connaissances et en y passant le temps nécessaire, il sera toujours possible de l'outrepasser. En termes de sécurisation (pour les lecteurs qui commenceraient à s'inquiéter pour la protection effective de leur porte d'entrée) c'est la multiplication des systèmes et leur installation judicieuse qui apporteront le niveau de sécurité satisfaisant. Néanmoins, chaque système, pris individuellement, reste contournable. Tous les types de serrures sont donc concernés par ce risque et peuvent faire l'objet d'une expertise en cas de doute.

CES TECHNIQUES SONT-ELLES RÉELLEMENT UTILISÉES, PAR QUI ET DANS QUELS CAS ?

Dans la majorité des cas : cambriolages d'opportunité, crimes générant de nombreuses traces, etc... le ou les auteur(s) n'auront pas obligatoirement les compétences pour agir de manière furtive sur la partie « intrusive » de leur méfait. L'usage d'un pied-de-biche permet une plus grande rapidité d'exécution et, si les traces laissées sur place ne présentent pas à leurs yeux une grande contrariété, ils ne font pas l'effort de dissimuler leur passage.

Pour autant, les méthodes d'intrusion furtives peuvent être employées dans les cas spécifiques où les auteurs essaient de dissimuler au maximum leur présence (homicides, vols d'informations sensibles, vols maquillés, etc…).

L'attrait pour ces techniques est bien réel. De nombreuses vidéos en ligne présentent, sous la forme de tutoriels, les différentes techniques de contournement de serrures. De même, de multiples boutiques spécialisées proposent les outils nécessaires à la mise en œuvre de ces techniques. Sur ce point, il est regrettable de constater que certains fabricants de matériels ne réservent pas toujours leurs produits aux seules forces de l'ordre ou serruriers. D'autant plus que les serruriers n'emploient pratiquement pas ces techniques, trop coûteuses en temps d'entraînement, en matériel, et sans grand intérêt d'un point de vue commercial. Ils préfèrent, bien souvent, recourir à une simple perceuse.

Si ces vidéos sont, dans la très grande majorité des cas, « réalisées par » et « destinées à » des crocheteurs « sportifs », il n'empêche qu'elles présentent néanmoins des techniques qui deviennent de plus en plus accessibles, voire à la portée de tous et donc également à la portée de personnes à la moralité douteuse.

C'est une réalité de terrain : de plus en plus de malfaiteurs se spécialisent dans l'une ou l'autre des techniques d'ouverture douce, et ce en fonction de leur affinité pour tel ou tel délit.

Dans le cadre d'une opération de police judiciaire telle qu'une perquisition, les enquêteurs peuvent être amenés à découvrir des objets susceptibles de correspondre à du matériel d'intrusion. Dans ces circonstances, nous sommes régulièrement sollicités afin de savoir s'il s'agit bien de matériel d'intrusion et s'il peut réellement fonctionner. L'identification précise de ces outils peut ainsi orienter les enquêteurs vers une manière d'opérer particulière ou vers une marque de véhicule ciblée (lorsqu'il s'agit d'outils dédiés à l'ouverture des véhicules) et ainsi concourir à la manifestation de la vérité.

À QUOI RESSEMBLENT LES OUTILS UTILISÉS ?

Tout dépend du type de serrure visé. Certains outils sont « généralistes » et couvrent un large spectre de serrures. D'autres sont, au contraire, extrêmement spécialisés. Dédiés uniquement à un type et modèle particulier de serrure, ils sont d'une efficacité redoutable pour qui sait s'en servir.

Lorsqu'on réalise une expertise sur les traces d'outils laissées et afin d'apporter une réelle plus-value à

Photo 2 : trousse à outils généralistes pour serrures à goupilles, pour la pratique du crochetage et de quelques autres techniques assimilées.

Photo 3 : outil spécialisé, dédié aux serrures TIBBE présentes sur certains véhicules Ford et Jaguar.

Photo 4 : Plusieurs outils en vrac.

Photo 5 : outils destinés à ouvrir principalement des serrures de type radiales (clés horizontales à micros points), par la méthode d'auto-impressionning, ou « clé molle ».

l'enquête, il est aussi important de faire le distinguo entre les outils manufacturés, qu'on peut trouver plus ou moins facilement dans le commerce spécialisé, et les outils « faits maison » que certains confectionnent eux-mêmes (attestant d'un certain savoir-faire, tout en désignant parfois leur auteur).

Il faut également citer l'existence de « faux outils » susceptibles d'avoir laissé des traces ou d'être découverts sur les lieux, sans pour autant être en mesure d'ouvrir la serrure en question. En effet, il arrive que certaines personnes veuillent faire croire, pour diverses raisons, en la réalité d'une intrusion (qui n'a pas réellement eu lieu ou alors pas comme on voudrait le laisser penser). Ces individus utilisent pour cela toutes sortes d'outils (incrustant possiblement peu de traces pour accréditer le scénario d'un « crochetage » de la serrure). Là encore, l'expertise tentera de déterminer si les traces sont consécutives à l'usage d'un outil ayant réellement la possibilité de déverrouiller la serrure ou non.

QUELLES TRACES PEUVENT ÊTRE VISIBLES ?

Les techniques d'ouverture « non destructives » laissent des micro-traces. Ces traces, n'ont rien à voir avec celles que laisse de manière « normale » et « habituelle » une clé légitime dans sa serrure, et ce pour une multitude de raisons. Parmi elles, citons :

- La forme et l'épaisseur des outils, qui diffèrent complètement de celles de la clé et de ce fait marquent différemment la surface des éléments rencontrés.
- Lors de l'insertion d'une clé, le mouvement rotatif de celle-ci intervient après son insertion rectiligne, sans tension, de sorte que ce passage n'appuie pas outre mesure sur les différentes « sûretés » de la serrure ; ce qui n'est pas le cas lors d'un crochetage, où des appuis prononcés, ou « microforçages », doivent être réalisés pour mettre en place les « sûretés » de la serrure (les éléments qui la verrouillent).
- Certains emplacements d'une serrure ne sont jamais au contact de la clé et ne devraient jamais présenter la moindre trace, hormis celles de l'usinage d'origine. Lors d'un crochetage, les outils « raclent » ces emplacements, supposés vierges de

Photo 6 : goupille d'une serrure ayant subi une ouverture par crochetage.

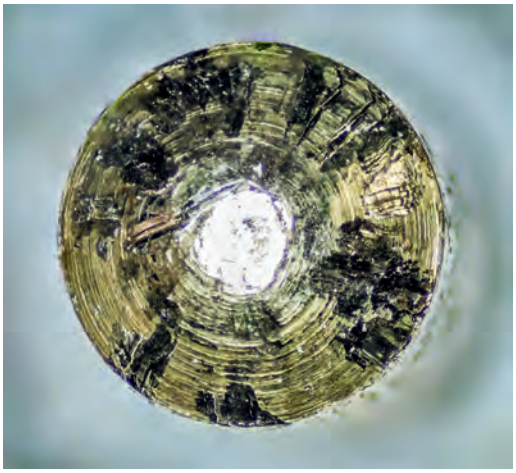


Photo 7 : goupille d'une serrure où des clés à percussion ont été utilisées.

tout contact, et laissent ainsi des traces significatives.

De ce fait, si l'on sait où chercher et quoi chercher, il est non seulement possible de voir que des outils ont été utilisés, mais également de déterminer avec précision le type d'attaques (même « non destructives ») qu'a pu subir une serrure.

Par exemple, pour l'utilisation d'une technique appelée « bumping », l'outil « percute », parfois à plusieurs reprises, les goupilles de la serrure avec pour résultat les traces présentes sur la photo n° 7 ci-dessus. Ces traces ainsi générées sont caractéristiques de ce type d'attaques.

Cette mise en évidence peut être d'une aide précieuse pour l'enquête et permet en outre d'identifier le profil « intrusif » de l'auteur des faits.

SUR QUELLES CONNAISSANCES S'APPUIE L'EXPERT POUR IDENTIFIER L'EFFRACTION NON DESTRUCTIVE ?

Pour expertiser des serrures et mettre en évidence la présence ou l'absence de traces d'ouverture, il est impératif que l'expert connaisse parfaitement le fonctionnement des différentes familles de serrures, qu'il maîtrise l'ensemble des méthodes d'effraction possibles (destructives et non destructives) ainsi que les principes physiques et mécaniques qui entrent en jeu.

Il doit avoir une connaissance approfondie de l'ensemble des outils d'intrusion existants et de ceux pouvant être improvisés, avoir étudié en profondeur les traces et microtraces que laissent ces ouvertures, et savoir démonter proprement une serrure en évitant absolument la « contamination » de celle-ci par des traces supplémentaires. Enfin, il doit connaître les méthodes de minimisation des traces pouvant être employées par les auteurs, afin de les identifier et déterminer si elles ont été utilisées.

Chercher des traces sans savoir quoi chercher ne rime évidemment pas à grand-chose. Dans certains cas, la serrure peut présenter des traces suspectes ne relevant pourtant pas d'une intrusion. Ces « faux positifs »[2] peuvent être nombreux pour celui qui ne connaît pas réellement la discipline. Pour ces raisons, il est impératif, avant de chercher les traces, de savoir quelle technique a pu être employée et de mettre en cohérence la faisabilité d'une attaque avec la réalité environnementale de la serrure ou de tout élément de sécurisation.

Pour finir, l'expert doit pouvoir se mettre en situation, c'est-à-dire être lui-même compétent pour pratiquer ces méthodes d'ouverture, voire d'en inventer de nouvelles lorsque cela est possible et que ce type de *modus operandi* « innovant » est à suspecter.

Seul un expert capable de se mettre à la place d'un intrus pourra réellement appréhender ce qui a été fait sur une serrure. Les microtraces « parlent », mais encore faut-il que l'expert « traduise » couramment le « langage » des serrures.

QUELLES SONT LES ÉTAPES D'UNE EXPERTISE ?

Une bonne expertise peut difficilement avoir lieu sans un bon prélèvement. C'est la raison pour laquelle il est idéal que l'expert puisse prélever lui-même la ou les serrure(s) sur le terrain. Il saura s'entourer des précautions nécessaires et prendre en compte pleinement l'environnement.

Lorsque ce n'est pas possible, il est préférable qu'un personnel de la police technique et scientifique (technicien en identification criminelle ou équivalent), ayant au préalable participé à une sensibilisation sur le sujet, réalise le prélèvement.

Ainsi, lors de ce prélèvement, il pourra veiller à ne rien introduire dans la serrure ou à le faire (si le démontage du canon le nécessite) en suivant les directives permettant la sauvegarde maximale des hypothétiques traces (notamment en ne touchant pas le côté extérieur). Il saura quelles prises de vue contextuelles effectuer pour que l'expert arrive à situer la serrure

> **« Il est impératif, avant de chercher les traces, de savoir quelle technique a pu être employée et de mettre en cohérence la faisabilité d'une attaque avec la réalité environnementale de la serrure. »**

dans son environnement d'origine. De même, il posera les bonnes questions aux utilisateurs de la serrure.

L'expertise se poursuit en laboratoire. Les observations préliminaires sont effectuées et la serrure est préparée en vue de l'expertise. Les différents éléments sont démontés, permettant la réalisation d'observations non destructives. Le niveau réel de sécurité de la serrure est apprécié et les traces suspectes sont recherchées.

Lorsqu'il est nécessaire d'ouvrir par une découpe l'élément expertisé et qu'il s'agit de la décision la plus judicieuse afin de mener à bien l'expertise (par exemple pour observer l'intérieur d'un cylindre à un emplacement inaccessible sans découpe), cette découpe est effectuée de telle sorte qu'elle ne puisse en aucun cas altérer les emplacements dignes d'intérêt à observer.

Des comparaisons sont effectuées entre l'élément expertisé et un élément neutre (souvent, le côté extérieur de la serrure comparé au côté intérieur). D'autres comparaisons sont réalisées entre les traces trouvées et différentes traces d'outils pouvant correspondre. Enfin, une vérification de faisabilité est entreprise lorsqu'elle est matériellement possible.

À l'issue de tous ces tests, l'ensemble des éléments sont de nouveau protégés et replacés sous scellés, afin de permettre d'éventuelles nouvelles observations ultérieures si nécessaire ou si ces observations demandent à être exposées.

COMMENT PRÉSENTER UN RAPPORT DANS UN DOMAINE MÉCONNU ?

Le rôle de l'expert, au-delà d'aider le juge à statuer en lui donnant son avis technique, est de mettre à la portée des magistrats, avocats ou parties, une meilleure compréhension de la partie technique sur laquelle on le sollicite, mais également l'explication du cheminement qui l'amène à formuler un tel avis.

Or, l'un des aspects complexes dans cette discipline réside dans la vulgarisation des techniques sensibles, parfois même secrètes. Ces techniques, potentiellement utilisées par un intrus, s'avèrent difficilement comprises, de prime abord, par une personne non avisée.

Pour ces raisons, le rapport présente en détail les observations, ce qu'elles impliquent, en développant le fonctionnement de la serrure dans telle ou telle condition. Un lexique relatif à tous les termes techniques employés est annexé au rapport, afin de vulgariser de manière simple et compréhensible une terminologie bien souvent complexe.

La pédagogie est ici essentielle pour que les lecteurs du rapport, même en l'absence de connaissances dans le domaine, puissent prendre la mesure des observations rapportées et de leurs implications.

CONCLUSION

La porte de l'appartement était fermée, mais l'a-t-elle été de l'intérieur ou de l'extérieur… Comment et par qui ? … De ces réponses plusieurs axes d'enquête peuvent découler. S'agit-il d'un suicide ou d'un possible homicide ?

Le magasin cambriolé ne porte pas de traces apparentes d'effraction… S'agit-il d'une négligence du propriétaire ou d'un mode opératoire plus énigmatique ? Et ces traces… qui semblent visiblement être le résultat d'une intrusion malveillante dans les locaux… Réalité ou mise en scène ?

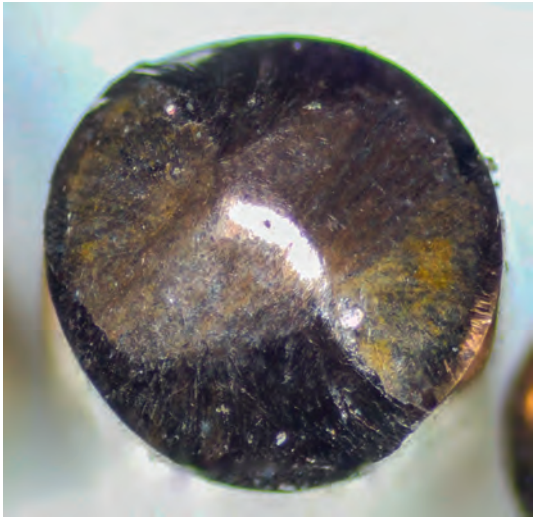
Comme nous l'avons vu, toutes les traces ne signifient pas forcément une intrusion effective et, *a contrario*, l'absence visible de traces d'effraction ne signifie pas son inexistence… Dans les cas où il est légitime d'envisager qu'une technique d'intrusion furtive a pu être employée, seule l'expertise en intrusion forensique permettra, par sa vision minutieuse et analytique, d'apporter des réponses à ces questions.

NOTES

1. Qui traite de la définition de certaines circonstances entraînant l'aggravation, la diminution ou l'exemption des peines.
2. Voir encadré sur « le faux positif ».

« Le faux positif »

Une serrure peut rester plusieurs décennies à la même place, sur une porte. Pendant cette période, de nombreuses péripéties peuvent lui arriver : insertion d'une clé qui ne lui était pas destinée, tentative de forçage non aboutie, insertion volontaire et involontaire (par des enfants par exemple) d'objets divers, etc. Dans ces situations, il peut arriver que des « traces » apparaissent dans la serrure. Pour autant elles ne signifient en rien une intrusion. Le seul moyen pour savoir si une trace est effectivement consécutive à une intrusion ou pas est donc de connaître parfaitement les mécanismes des techniques de crochetage des serrures.



Ci-contre un exemple de goupille avec des « traces » inhabituelles, non consécutives d'un crochetage (mais plutôt d'une utilisation très répétée d'une copie de la clé originale, réalisée sur une ébauche ayant un profil légèrement différent, et une butée décalée).

Une observation « naïve » aurait pu aboutir à un « faux positif » (diagnostic de positivité de l'intrusion, à tort, car les traces proviennent de tout autre chose).

MOTS-CLÉS : CAMBRIOLAGE / CROCHETAGE / DAVID ELKOUBI / EFFRACTION / EXPERTISE EN INTRUSION FURTIVE / POLICE TECHNIQUE ET SCIENTIFIQUE / SERRURE / SERRURERIE FORENSIQUE / SYSTÈME DE SÉCURITÉ / TECHNIQUE D'OUVERTURE NON DESTRUCTIVES - RÉF. : ST, D, 02, 00. WWW.REVUE-EXPERTS.COM

Innover fait partie de l'ADN des experts scientifiques de la Gendarmerie

Docteur Sylvain Hubac
Chef d'escadron à l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN), chef du département analyses génétiques Traces, expert judiciaire près la cour d'appel de Versailles, expert judiciaire agréé par la Cour de cassation

Le LAB'ADN est un dispositif d'analyses génétiques rapide et projetable de l'Institut de recherche criminelle de la Gendarmerie nationale (IRCGN). Il permet d'établir en moins de 3 heures, au profit des magistrats et des enquêteurs, le profil ADN de plusieurs dizaines d'échantillons au plus près des scènes de crimes complexes, de catastrophes ou d'attentats sans préjudice de qualité et de fiabilité des résultats afin d'identifier dans les plus brefs délais les auteurs et les victimes. Ce dispositif unique au monde repose sur deux brevets d'invention dont une licence d'exploitation a été concédée aux industriels COPAN (Italie) et TRACIP (France).

LA PROBLÉMATIQUE

La criminalistique peut être définie comme l'application de procédés techniques aux investigations judiciaires permettant l'étude scientifique des traces et des indices retrouvés sur les scènes de crimes. Parmi ces traces, l'étude des traces de nature biologique est devenue incontournable car elles contiennent la molécule d'ADN. Cette molécule est constituée de quatre éléments chimiques élémentaires, les nucléotides, nommés par les lettres A, T, G et C qui s'enchaînent des milliards de fois pour constituer une séquence unique. C'est donc cette combinaison de nucléotides, propre à chacun, qui fait de l'ADN un support d'identification performant.

Le paysage de l'analyse génétique à des fins judiciaires a été bouleversé ces dernières années par un besoin de réponse instantanée stimulé par les événements tragiques que la France a dû surmonter, qu'il s'agisse de catastrophes majeures, d'attentats ou de scène de crimes complexes. Pour répondre à ce nouveau besoin, l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) a bouleversé la pensée traditionnelle de l'analyse génétique. Les experts de la Division criminalistique biologie génétique de l'IRCGN ont ainsi développé un nouvel écosystème à l'intérieur duquel une trace biologique est prélevée à l'aide d'un dispositif innovant puis analysée en temps réel dans un environnement contrôlé. Selon ce nouveau mode de pensée, c'est donc le laboratoire qui vient à la scène de crime et non plus les prélèvements de la scène de crime qui viennent au laboratoire.

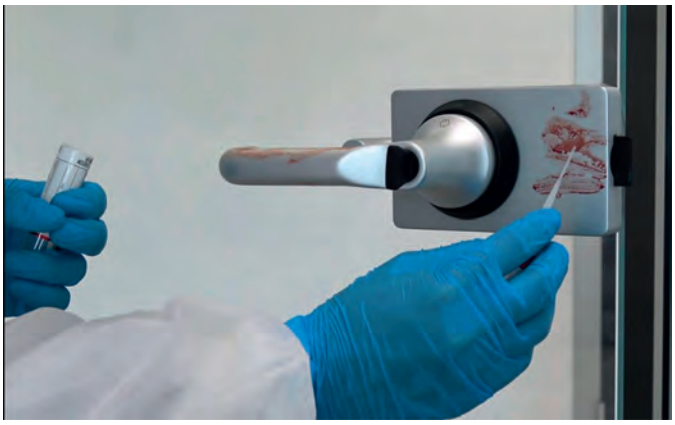
L'INNOVATION

Le processus conventionnel de détermination de profil ADN nécessite un enchaînement de quatre étapes permettant :

1. d'extraire l'ADN du matériel biolo-

Figure 1 : photographie du micro-écouvillon microFLOQ Direct.

Figure 2 : vue rapprochée des fibres du micro-écouvillon microFLOQ Direct.



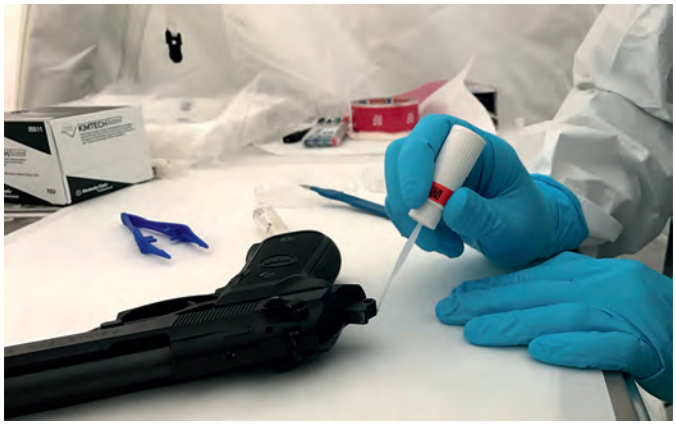


Figure 3 : Illustration de l'utilisation du micro-écouvillon microFLOQ Direct pour prélever une trace biologique sur une poignée de porte et sur une arme à feu.

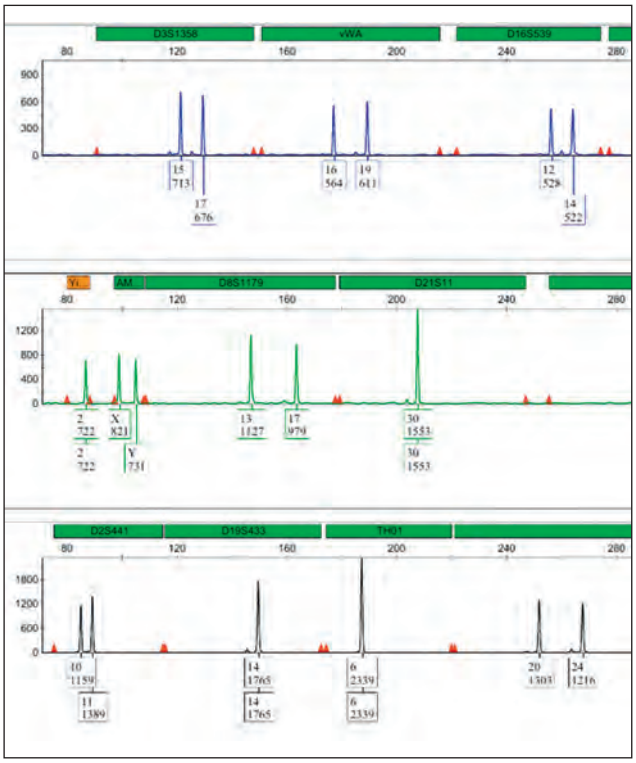
gique : il est nécessaire pour cela de détruire l'enveloppe externe de la cellule et son noyau par une action de nature biochimique afin de pouvoir atteindre l'ADN ;

2. d'évaluer l'ADN extrait afin d'en déterminer la qualité et la quantité ;
3. d'amplifier l'ADN par la technique de PCR (Polymerase Chain Reaction) afin de cibler différentes régions d'intérêts dites STR (Short Tandem Repeat) permettant de différencier les individus les uns des autres ;
4. de révéler les régions d'ADN amplifiées par la technique d'électrophorèse capillaire afin de déterminer le profil ADN.

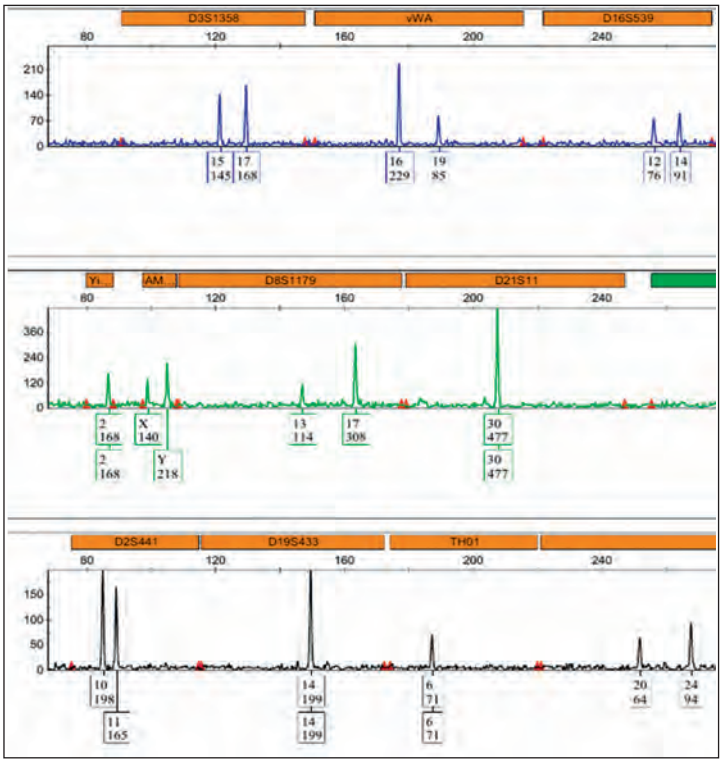
Ce processus nécessite près de 7 heures pour obtenir un résultat. Les temps d'analyse d'une vingtaine d'échantillons sont ainsi décomposés comme suit, incluant les temps de manipulations : extraction, 2 heures ; évaluation, 2 heures ; amplification, 2 heures ; révélation, 40 minutes.

Ces quatre étapes techniques sont réalisées en laboratoire dans des locaux dédiés selon le principe de la marche en avant au sein d'un environnement contrôlé de manière à prévenir tous risques de contaminations des échantillons par de l'ADN étranger. Ces risques de contaminations sont notamment prépondérants lors de l'étape d'extraction d'ADN durant laquelle l'ADN est libéré de la cellule et donc plus facilement exposé.

L'obtention d'un résultat ADN exploitable repose également en grande partie sur la stratégie de prélèvement ainsi que sur l'outil utilisé pour prélever efficacement la trace biologique en



Processus technique utilisant le micro-écouvillon microFLOQ Direct



Processus technique utilisant les méthodes conventionnelles

Figure 4 : Profil ADN obtenu à partir de 0,5 microlitre de sang dilué au 1/50ème à partir du processus technique utilisant le micro-écouvillon microFLOQ Direct et du processus technique utilisant les méthodes conventionnelles.

Figure 5 : Illustration du déplacement des instruments analytiques dans le laboratoire mobile.

fonction de sa nature et de la nature du support sur lequel elle se trouve. Cette méthode de prélèvement influençant très fortement la quantité et la qualité de l'ADN prélevé, les dernières évolutions techniques d'extraction et d'amplification par PCR s'avèrent malgré tout insuffisantes pour optimiser l'efficience d'une analyse ADN rapide à partir d'un large spectre d'échantillons biologiques.

C'est sur la base de ce constat que l'IRCGN a breveté un nouvel outil de prélèvement destiné principalement à l'analyse simplifiée, rapide et à haut débit de l'ADN. Ce dispositif, produit et commercialisé par l'industriel italien COPAN sous le nom de microFLOQ Direct, se présente sous la forme d'un micro-écouvillon de fibres synthétiques. Ces fibres sont imprégnées d'agents physico-chimiques qui permettent de réaliser in situ et de manière instantanée les deux premières étapes du processus d'analyse, à savoir l'extraction et la normalisation de la quantité d'ADN contenu dans le matériel biologique prélevé tout en le rendant directement disponible pour être amplifié. Son utilisation permet ainsi de réduire de près de 4 heures l'obtention d'un profil ADN par rapport à l'utilisation d'un écouvillon traditionnel.

Du fait de sa faible surface de contact par rapport à un écouvillon standard, ce micro-écouvillon permet de prélever avec une grande précision les microtraces biologiques et de préserver au maximum le matériel génétique présent sur le support essuyé qui peut ainsi faire l'objet soit d'un nouveau prélèvement, soit d'une exploitation d'une autre nature comme l'identification du dessin papillaire des traces digitales ou la détermination de la nature biologique de la trace.

Malgré cette surface de contact réduite qui peut cependant capter jusqu'à environ 10 000 cellules, l'absence d'étape intermédiaire entre la collecte de la trace biologique et l'amplification par PCR constitue une stratégie parfois plus efficace que les méthodes d'extraction d'ADN conventionnelles pour l'analyse de microtraces biologiques présentant une faible quantité d'ADN.

Enfin, en réalisant l'étape d'extraction de l'ADN de manière instantanée directement à son extrémité, le microFLOQ Direct préserve les échantillons de la contamination, ce qui a permis d'envisager la possibilité de réaliser ces analyses ADN non pas uniquement dans un laboratoire conventionnel mais également dans un laboratoire mobile.

Dans cet objectif, le problème technique à résoudre par les experts de l'IRCGN était donc de proposer un laboratoire transportable au plus près d'une scène de crime quelle que soit sa localisation géographique, configuré avec tout le matériel traditionnel nécessaire et adapté pour permettre de réaliser des analyses dans des conditions au moins aussi fiables que dans un laboratoire conventionnel afin de ne pas pouvoir remettre en cause la fiabilité des résultats. Ce problème a dû être résolu tout en permettant une mise en œuvre facile par un personnel réalisant traditionnellement ces opérations dans un laboratoire classique, sans besoin de formation supplémentaire, et à un coût acceptable, en particulier pour une utilisation ponctuelle.

Ce laboratoire mobile, qui a également fait l'objet de la délivrance d'un brevet d'invention, a une configuration qui permet de respecter le principe de la « marche en avant » du traitement d'un échantillon afin de prévenir toutes contaminations, à savoir :

- une première zone, dite de pré-PCR, dans laquelle l'échantillon à analyser est inséré dans le laboratoire et rentre dans la zone analytique où sont réalisées les opérations techni-

“L'IRCGN a breveté un nouvel outil de prélèvement destiné principalement à l'analyse simplifiée, rapide et à haut débit de l'ADN. Il se présente sous la forme d'un micro-écouvillon de fibres synthétiques.”

Figure 6 : Représentation du laboratoire mobile.
À gauche : vue extérieure ; à droite : vue intérieure.
La flèche illustre le principe de la marche en avant des échantillons depuis la zone de Pré-PCR jusqu'à la zone de Post-PCR.

ques préparatoires à l'amplification génique par PCR ;
- une seconde zone, dite de post-PCR, dans laquelle sont réalisés à la fois l'amplification génique par PCR et le génotypage par électrophorèse capillaire.

Ce dispositif est agréé par le ministère de la Justice pour être utilisé dans le cadre de procédures judiciaires ou extrajudiciaires. Il constitue à ce jour le seul laboratoire au monde accrédité selon la norme internationale ISO17025 relative aux laboratoires d'analyses et d'essais valorisant ainsi le savoir-faire de la gendarmerie au niveau international. Une licence d'exploitation du brevet et de ce savoir-faire a d'ailleurs été concédée à l'industriel français TRACIP du groupe DEVERYWARE pour l'industrialisation et la commercialisation de laboratoires mobiles d'analyses ADN sur le modèle de l'IRCGN.

Par cette méthode de collecte et d'analyse, le délai entre l'installation du laboratoire sur site, la collecte de la trace biologique et la détermination du profil ADN est de moins de trois heures pour les premiers 21 échantillons analysés. Le système d'analyse permet ensuite de générer au moins 21 résultats supplémentaires toutes les trente minutes. Les délais d'obtention des résultats sont ainsi considérablement réduits par rapport au temps nécessaire à l'acheminement et à l'analyse dans un laboratoire classique tout en conservant les avantages d'une production d'analyses en série de plusieurs dizaines de prélèvements.

CONCLUSION

Le laboratoire mobile d'analyses ADN et le micro-écouvillon microFLOQ Direct constituent non seulement deux illustrations concrètes de la capacité des experts de l'IRCGN à innover pour répondre aux évolutions des besoins afin d'assurer toujours mieux la sécurité des Français mais illustrent également la démarche active de la Gendarmerie nationale pour valoriser son savoir-faire auprès d'industriels ayant un rayonnement national et international.

Depuis l'obtention de son agrément par le ministère de la Justice et son accréditation par le COmité FRançais d'ACcréditation (COFRAC), ces deux innovations constituent un maillon essentiel des potentialités que peut proposer la Gendarmerie nationale en matière de projection opérationnelle pour favoriser une identification rapide des auteurs de crimes et des victimes de catastrophes ou d'attentats en tout temps et tout lieu.

Ce dispositif a notamment été utilisé avec un grand succès dans les situations d'urgence majeures que la France a connues ces dernières années dont notamment : l'attentat de Nice en 2016, l'ouragan IRMA en 2017, le crash de deux hélicoptères de combat à Carcès en 2018 et plus récemment le crash d'un mirage 2000 D à Mignovillard en 2019.

BIBLIOGRAPHIE

- A Modified Direct PCR Amplification Method Using the GlobalFiler™ PCR Amplification Kit on Bloodstains Collected Using microFLOQ™ Direct Swabs. Forensic Science International: Genetics Supplement Series, October 3, 2019
- A Practical Study on Direct PCR Amplification Using the GlobalFilerTM PCR Amplification Kit on Human Bloodstains Collected with microFLOQ™ Direct Swabs. Forensic Science International 300 (July 1, 2019): 43–50
- Collection and Direct Amplification Methods Using the GlobalFiler™ Kit for DNA Recovered from Common Pipe Bomb Substrates. Science & Justice 59, no. 5 (September 1, 2019): 580–84
- Direct Amplification of Biological Evidence and DVI Samples Using the Qiagen Investigator 24plex GO! Kit. Forensic Science International: Genetics Supplement Series 6 (December 1, 2017): e208–10
- Direct PCR Amplification of DNA from Human Bloodstains, Saliva, and Touch Samples Collected with microFLOQ® Swabs. Forensic Science International: Genetics 32 (January 1, 2018): 80–87
- Dispositif de collection de matériel biologique à partir d'une trace biologique, issued February 17, 2016. https://patents.google.com/patent/WO2016132028A1/fr
- Laboratoire mobile pour analyse génétique, issued May 9, 2017. https://patents.google.com/patent/WO2017194849A1/fr

MOTS-CLÉS : ADN / ANALYSES GÉNÉTIQUES / ÉCOUVILLON / GENDARMERIE NATIONALE / IRCGN / LABORATOIRES D'ANALYSES / MICROFLOQ DIRECT / POLYMERASE CHAIN REACTION / SCÈNES DE CRIMES / SYLVAIN HUBAC / TRACES BIOLOGIQUES - RÉF. : ST, D, 02, 00. WWW.REVUE-EXPERTS.COM

SOMMAIRE

Les cyberattaques : Un phénomène inquiétant qui exige des réponses (1ère partie)

Sommaire

Daniel Guinier
Docteur ès Sciences
Certifications CISSP, ISSMP, ISSAP, MBCI
Expert en cybercriminalité et crimes financiers devant la Cour pénale internationale de La Haye
Expert de justice honoraire près la cour d'appel de Colmar

Tandis que les cyberattaques sont courantes et lucratives pour leurs auteurs, de plus en plus astucieuses ou sophistiquées, et que la cybercriminalité s'industrialise en proposant des services sur l'Internet ou sur le "DarkNet", l'auteur propose un modèle de représentation multidimensionnelle utile à la compréhension, fondé sur des caractéristiques décomposables et sur la dynamique des cyberattaques. Il en montre l'adéquation aux plus courantes. Il indique les délais, les conséquences et la réponse attendue face aux cyberattaques, pour espérer un retour à la normale au regard d'un plan de reprise d'activité (PRA). Il conclut sur la nécessité d'une lutte au plan international et sur les responsabilités, alors que les circuits de blanchiment prospèrent de façon inquiétante au service du crime organisé.

Crise / Crime organisé / Cyberattaques / Cybercriminalité / Information / Pénal / Plan de reprise d'activité / Réaction / Risque - ST, D, 02, 00

With cyber attacks becoming common and lucrative for their instigators, who have become more and more clever and whose methods are more and more sophisticated, and cyber criminality being commercialized through offers of services on the Internet or the Dark Net, the author proposes a multidimensional representative model that is easy to understand and is based on the analyzable features and dynamics of cyber attacks. He demonstrates the most common, indicates the time frames, consequences and expected responses to cyber attacks in the hope of a return to normal under a business continuation plan. In light of the money-laundering circuits for organized crime that prosper in a worrying manner, he concludes on the issue of the necessity for an international prevention and liabilities plan.

L'environnement électronique, lié à la généralisation de l'Internet et aux milliards d'objets connectés, représente un véritable enjeu mais aussi un terrain privilégié pour les cyberattaques qui participent d'un phénomène criminel sournois sans précédent. L'essor est lié à l'apparence d'anonymat et à la dimension internationale, avec des enjeux juridiques, économiques et politiques qui résident au cœur de la cybercriminalité économique et financière. Ceci concerne notamment les fraudes, les extorsions, les faux ordres de virement internationaux, les vols de données personnelles et confidentielles, les atteintes aux secrets industriels et commerciaux, avec des cyberattaques sophistiquées au cœur même des entreprises, etc. Les monnaies virtuelles, les circuits sophistiqués du blanchiment et le "*DarkNet*"[1] jouent ici un rôle important.

Nous sommes en fait tous bien plus exposés que nous l'imaginons, par des déficits chroniques[2] de sécurité au sein des organismes et des vulnérabilités longuement ouvertes[3]. Ce contexte représente un paradis pour les attaquants et l'enfer pour les victimes. Au cours des deux dernières années[4], les cyberattaques relèvent des menaces les plus courantes. En France, 77 % d'entre-elles visent les organismes de moins de 250 employés[5]. Alors que la cybercriminalité a doublé au cours de ces deux dernières années, 73 % des entreprises s'attendent à subir une cyberattaque dans les 2 ans[6] et 50 % déclarent ne disposer d'aucun plan de réaction.

1.DÉFINITION

Si une attaque peut être vue comme un mouvement offensif violent mené avec des armes, destiné à prendre le dessus sur l'adversaire et remporter une victoire, une cyberattaque sera menée avec des moyens numériques ou électroniques contre des éléments du cyberespace constituant la cible, pour en tirer profit ou nuire à la victime.

Il existe bien des tentatives de définition du terme "cyberattaque", mais elles sont incertaines et aucune n'est retenue au plan international. Les quelques définitions officielles, pourtant récentes, sont trop orientées ou restreintes à l'informatique[7]. Il s'agirait en fait de la réalisation de menaces, par l'exploitation de vulnérabilités de cibles constituées d'éléments variés du cyberespace (objets connectés ou non, données, infrastructures, etc.), avec des intentions malveillantes, entraînant un préjudice pour les victimes et un avantage pour les auteurs[8].

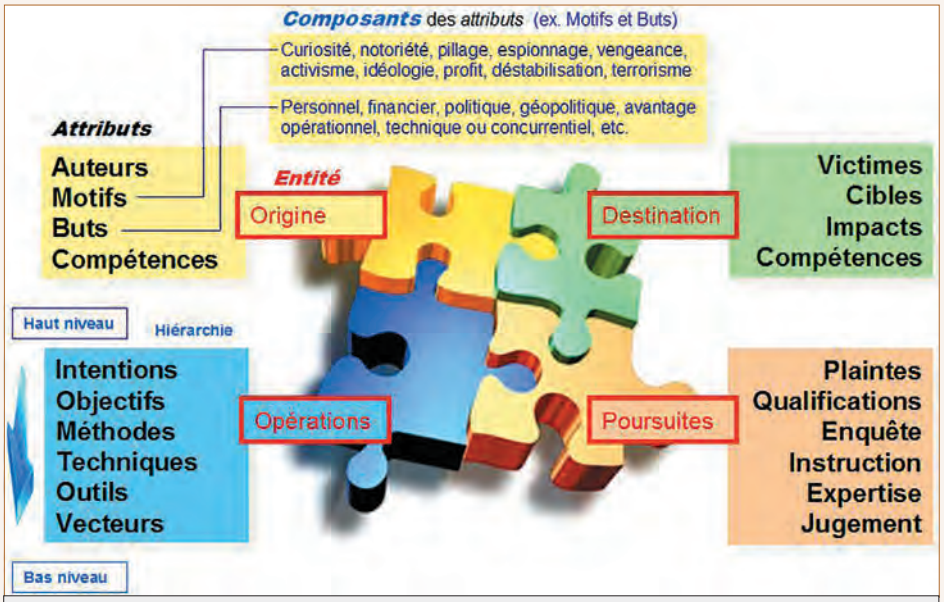


Figure 1. Caractéristiques statiques d'une cyberattaque

En outre, en 2015, l'étude de la littérature scientifique permet de dénombrer plus de 25 classifications incomplètes, pour les cyberattaques[9].

2.CARACTÉRISATION D'UNE CYBERATTAQUE

Nous avons privilégié l'aspect multidimensionnel en liant des caractéristiques structurées à la dynamique, pour proposer un modèle favorable à la compréhension des cyberattaques dans leur ensemble[10], qu'elles soient existantes ou à venir.

2.1.Caractéristiques statiques

Les entités sont constituées par un ensemble structuré où les attributs sont rattachés à l'entité qu'ils caractérisent. Eux-mêmes disposent de composants pouvant comporter plusieurs éléments[11]. Les caractéristiques statiques sont ainsi représentables sous forme d'un catalogue structuré par entités-attributs et leurs composants, avec la possibilité de plusieurs niveaux hiérarchisés d'abstraction selon quatre entités : « Origine »[12], « Destination »[13], « Opérations »[14] et « Poursuites »[15] (figure 1). Ainsi, une entité fait référence à un groupe d'attributs qui partagent son thème, un attribut représente un groupe de composants qui ont des points en commun, et un composant matérialise un ensemble spécifique du même attribut ; ce dernier pouvant être constitué d'éléments élémentaires indivisibles[16]. Ceci constitue un catalogue de structure stable présentant diverses options possibles, lesquelles peuvent être mises à jour.

Les principaux vecteurs sont les clés mémoire USB, les réseaux sociaux, les « spams ». Il suffit alors de disposer d'une cible, d'une adresse de messagerie, d'un minimum d'ingénierie sociale pour tromper le destinataire, d'une pièce jointe infectée par un cheval de Troie indétectable, ou encore d'un lien vers un site qui exploite les vulnérabilités du navigateur.

2.2.Représentation de la dynamique

Une cyberattaque se révèle être un processus en plusieurs étapes (8, au maximum), et pas un simple événement. Chacune peut être totalement caractérisée par le catalogue structuré précédent et par sa dynamique, alors qu'elle est variée du fait de diverses options et de leur combinaison. Par cette connaissance, elle pourrait ainsi être détectable à toute étape pour obliger l'attaquant à revoir sa stratégie.

En effet, selon le principe de Locard[17] où *"nul ne peut agir sans laisser des marques multiples de son passage"*, des traces numériques forment des indices dès les premières étapes, - de la phase de préparation à celle de réalisation -. Leur enregistrement et leur analyse régulière devraient permettre la détection pour une réaction appropriée, afin de tenter de la stopper sinon d'en réduire les impacts, directs et indirects. Ces traces sont observables par la surveillance d'anomalies de comportements, identifiables par les logs[18] (connexions, trafic, etc.) et les résidus rémanents, analysables avec des compétences et des outils appropriés, mais aussi fragiles et fugaces, et nécessitent d'être fixées de façon *ad hoc*.

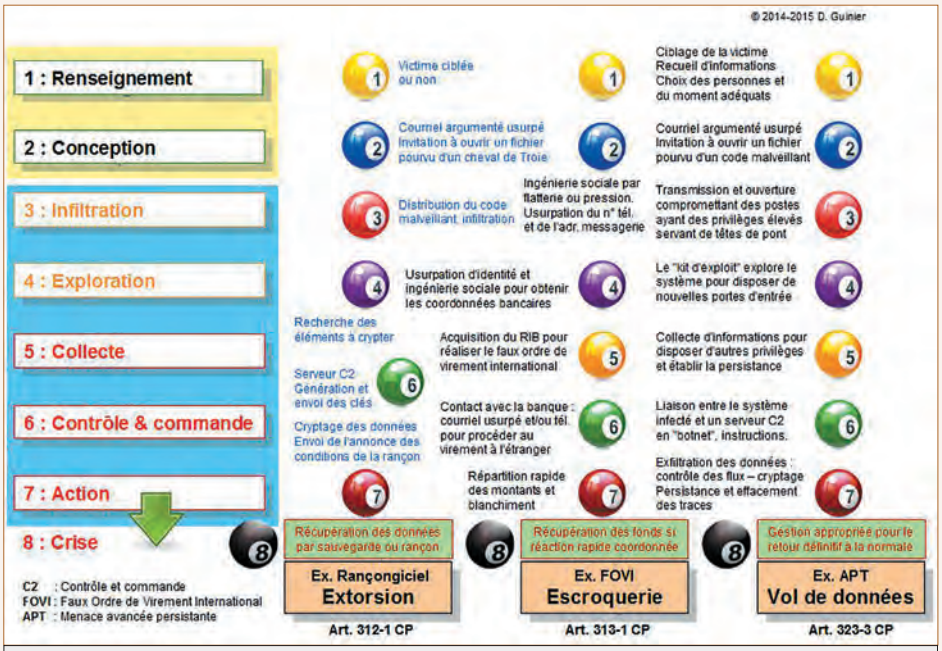


Figure 2. Présentation comparée de la dynamique de trois cyberattaques typiques.

Ce modèle de représentation multidimensionnelle, fondé sur des caractéristiques décomposables par niveaux et la dynamique par étapes, est applicable à des cyberattaques très variées, comme les attaques par rançongiciel[19], les faux ordres de virement international (FOVI), et le vol de données, qui entrent dans son cadre, etc., et qui, réciproquement, sont qualifiables de cyberattaques.

Concernant les cyberattaques avancées, les RATs (*Remote Access Trojans*), sont en mesure d'offrir aux cybercriminels un accès distant aux machines qu'ils auront pu infecter. Utilisant les privilèges d'accès de la victime, ils permettent d'accéder et d'exfiltrer des informations sensibles. Ainsi, la plupart des attaques avancées APT (*Advanced Persistant Threat*) en tirent profit pour outrepasser l'authentification forte, propager l'infection, accéder aux informations sensibles recherchées et les exfiltrer. Les RATs sont disponibles sur l'Internet ou le « *DarkNet* » (ex. *Dark Comet*, *njRAT*, *Net Bus*, *Poison Ivy*, *BlackShades*, etc.). Ils peuvent être installés sur les machines-victimes par simple téléchargement ou en utilisant des techniques d'ingénierie sociale de type « *spear phishing* », qui sont utilisées à plus de 90 % dans les attaques ciblées. ■

Notes

1. J.A. Wood J. A. (2010) sur la définition de "DarkNet", et D. Guinier (2015) sur les monnaies virtuelles et le cas Bitcoin.
2. G.-Y. Kervern et P. Rubise (1991), et D. Guinier (1991, 2013).
3. 99 % des vulnérabilités compromises relèvent de celles non corrigées plus d'une année après publication de la CVE correspondante (Common Vulnerability and Exposure), accessibles à tous.
4. "Cyberattack top business threat for second year running" - BCI - Horizon Scan Report 2016.
5. "2014 Internet Security Threat Report" - Symantec - Global Intelligence Network.
6. "Global Economic Crime Survey 2016" - PwC.
7. Définitions du Cyber Security Strategy for Germany (2011), du NIST (2013), de l'OTAN (2014).
8. D. Guinier (1995, 2013) et G.N. (2011).
9. C. Joshi et al. (2015).
10. D. Guinier (2016).
11. Selon la chaîne hiérarchisée : Entité_Attributs_Composants_Eléments.
12. L'entité "Origine" comporte quatre attributs associés à leurs composants : Auteurs : individu, groupe ou organisation : activiste, criminelle, terroriste, etc., agence d'Etat, etc. ; Motifs : curiosité, notoriété, pillage, espionnage, vengeance, activisme, idéologie, profit, déstabilisation, terrorisme, etc. ; Buts : personnel, financier, géopolitique, avantage opérationnel, technique ou concurrentiel, etc. ; Compétences : individuelles, académiques, Internet, "dark Web", collaboration avec : "hackers", "hacktivistes", crime organisé, etc., Etat, etc.
13. L'entité "Destination" comporte quatre attributs associés à leurs composants : Victimes : individu, groupe, organisme privé : financier, banque, entreprise, etc., ou organisme public, Etat, etc ; Cibles : matériel, composant, logiciel, service, infrastructure, données, compte, objets, processus, etc. ; Impacts directs : perturbation ou interruption de service, perte financière et de données, etc., indirects : réputation, image, confiance, clientèle, partenaires, actionnaires, perte d'opportunité, d'affaires et d'emplois, dommages faits à autrui, etc. ; Compétences : internes, externes : privées et publiques : ANSSI, forces de l'ordre, etc.
14. L'entité "Opérations" comporte six attributs hiérarchisés par niveau, servant la dynamique, dans les phases de préparation et d'exécution, jusqu'à la crise qui débute à la phase de découverte.
15. Avec des plaintes possibles au pénal comme au civil. On notera diverses qualifications pénales, notamment pour : accès frauduleux à un système de traitement (Art. 323-1 et suivants du CP, notamment l'Art. 323-3 pour le fait d'extraire, de détenir, de reproduire, et de transmettre frauduleusement des données), usurpation d'identité numérique (Art.226-4-1 al. 2), extorsion (Art. 312-1), chantage (Art. 312-10), escroquerie (Art. 313-1), etc.
16. Parmi d'autres, 2 éléments : BredoLab et Madness-Pro-Ddos-v1-13, du vecteur : "Botnet" de l'entité : "Opérations".
17. E. Locard (1877-1966).
18. Des enregistrements d'événements qui ont eu lieu sur une machine depuis ou vers cette machine ou un organe de communications.
19. Un rançongiciel (ransomware), est un logiciel malveillant qui crypte les données et fournit la clé de décryptage moyennant une rançon payable en Bitcoins, sans laquelle le décryptage est impossible (ex. CTB-Locker, TeslaCrypt, Cryptowall, Locky, CryptXXX, Peyta).

SOMMAIRE

Les cyberattaques : un phénomène inquiétant qui exige des réponses (2e partie)

Sommaire

Daniel Guinier
Docteur ès Sciences
Certifications CISSP, ISSMP, ISSAP, MBCI
Expert en cybercriminalité et crimes financiers devant la Cour pénale internationale de La Haye
Expert de justice honoraire près la cour d'appel de Colmar

Tandis que les cyberattaques sont courantes et lucratives pour leurs auteurs, de plus en plus astucieuses ou sophistiquées, et que la cybercriminalité s'industrialise en proposant des services sur l'Internet ou sur le "DarkNet", l'auteur propose un modèle de représentation multidimensionnelle utile à la compréhension, fondé sur des caractéristiques décomposables et sur la dynamique des cyberattaques. Il en montre l'adéquation aux plus courantes. Il indique les délais, les conséquences et la réponse attendue face aux cyberattaques, pour espérer un retour à la normale au regard d'un plan de reprise d'activité (PRA). Il conclut sur la nécessité d'une lutte au plan international et sur les responsabilités, alors que les circuits de blanchiment prospèrent de façon inquiétante au service du crime organisé.

CRISE / CRIME ORGANISÉ / CYBERATTAQUES / CYBERCRIMINALITÉ / INFORMATION / PÉNAL / PLAN DE REPRISE D'ACTIVITÉ / RÉACTION / RISQUE - ST, D, 02, 00

With cyber attacks becoming common and lucrative for their instigators, who have become more and more clever and whose methods are more and more sophisticated, and cyber criminality being commercialized through offers of services on the Internet or the Dark Net, the author proposes a multidimensional representative model that is easy to understand and is based on the analyzable features and dynamics of cyber attacks. He demonstrates the most common, indicates the time frames, consequences and expected responses to cyber attacks in the hope of a return to normal under a business continuation plan. In light of the money-laundering circuits for organized crime that prosper in a worrying manner, he concludes on the issue of the necessity for an international prevention and liabilities plan.

2.3. Délais liés à une cyberattaque

Pour les attaquants, le délai de préparation varie de plusieurs heures à plusieurs jours, dans environ la moitié des cas. Il nécessite toutefois plusieurs mois pour 30 % des attaques les plus avancées, lesquelles nécessitent alors une stratégie et des développements complexes. Le délai d'exécution se situe entre plusieurs minutes jusqu'à plusieurs jours dans les trois-quarts des cas[1].

> Pour les victimes, le délai de découverte d'une cyberattaque exige des semaines, voire des mois, dans les trois quarts des cas, avec un délai moyen de découverte de 7,5 mois.

Pour les victimes, s'il peut être instantané, lorsqu'il est volontairement notifié par une annonce ne laissant aucun doute[2], le délai de découverte exige des semaines, voire des mois, dans les trois quarts des cas, avec un délai moyen de découverte de 7,5 mois[3], et un maximum observé supérieur à six ans ! Souvent les victimes sont avisées par un tiers. Le délai de maîtrise, constaté par le retour à la normale associé à la fin de la crise, varie de plusieurs jours à des semaines, dans les trois quarts des cas. Des poursuites sont évidemment possibles après la découverte. Elles évoluent jusqu'à la fin de crise mais aussi par après, dans la période de post-crise. Cette dernière peut à son tour durer des années, jusqu'à la fin des procédures judiciaires et à l'issue du jugement définitif. Il existe une asymétrie de temps, puisque la découverte et la maîtrise prennent des semaines voire des mois, alors que le délai de début d'exécution d'une cyberattaque est très inférieur.

2.4.Conséquences liées à une cyberattaque

Si les victimes de cyberattaques n'ont pas toujours la capacité d'en supporter les coûts directs, elles ont également à faire face à d'autres conséquences négatives liées à la remise en ordre de la situation. Il s'agit de surcoûts en rapport avec les personnels et heures supplémentaires, les experts et consultants externes à engager, les mesures techniques de sécurité à mettre en place dans l'urgence, après l'attaque. À ceci, viennent s'ajouter les changements organisationnels, la réparation des dommages causés aux systèmes, infrastructures, logiciels et données, la perte de revenus et de clientèle, et en complément, les efforts pour maintenir la relation avec la clientèle. D'autres conséquences sont en rapport avec la responsabilité pour les montants ou les données volés lors de l'attaque, et pour les dommages causés à des tiers, notamment pour non-respect des obligations légales ou contractuelles. L'ensemble peut conduire à des litiges portés en justice et compromettre la réputation et l'image de l'organisme, et entamer la confiance des clients comme des partenaires. Enfin, au vu des options possibles et de la diversité des résultats produits, les techniques et outils avancés d'attaque peuvent engendrer un conflit avec d'autres parties en délivrant des leurres.

2.5. Chiffres relevant des cyberattaques

Pour tous, le sujet est sérieux... mais pas les chiffres. Cet état de fait, connu sous le vocable de « chiffre noir », révèle un écart important entre la réalité fondée sur les infractions commises, et les attaques supposées, sur la base de réponses fournies à des questionnaires. Les causes principales sont liées à des incertitudes sur la détection des pertes, aux critères d'évaluation insatisfaisants et à la présence de biais. En effet, nombre d'organismes n'ont pas détecté de pertes ou leur importance n'est pas connue ou mal estimée. D'autres n'ont pas de critères d'évaluation des pertes directes et indirectes ou n'en ont signalé aucune, par méconnaissance ou par méfiance, pensant ainsi préserver leur image. Enfin, ceux qui n'ont pas détecté de pertes répondent facilement, tout comme ceux dont les pertes sont déjà publiquement connues, tandis que ceux dont les pertes ne sont pas dévoilées évitent de répondre.

Dans le monde[4] : 42,8 millions de cyberattaques ont été recensées dans le monde en 2014. Ce chiffre est en augmentation de 48 % par rapport à 2013, avec un coût annuel moyen de 2,7 millions d'euros par entreprise. Par ailleurs, il est constaté une augmentation de 86 % des cyberattaques menées par des États, en particulier sur les secteurs de l'énergie, de l'aéronautique et de la défense.

> Une évaluation rapide et précise de l'incident est nécessaire pour le choix du type d'investigation, qui dépendra de la nature de l'incident, de l'objectif et de la cible, mais aussi de son origine : interne ou externe.

En France[5] : Une étude partielle menée auprès de 29 organismes indique qu'en 2014, le coût annuel moyen des cyberattaques en France a atteint 4,8 millions d'euros par entreprise, - allant jusqu'à 19 millions d'euros -, en progression de plus de 20 % en un an. Les secteurs de l'énergie, des services publics, des services financiers et des technologies sont les plus touchés, avec un coût par employé plus élevé pour les organismes de petite taille : 2 834 euros, contre 324 euros pour les autres. Les cyberattaques représentent plus de 45 % des coûts de la cybercriminalité. Le coût moyen est de 561 533 euros ; chiffre en croissance de 200 % par rapport à l'édition 2013 du rapport.

Les rançongiciels[6] occupent la deuxième place parmi les attaques les plus répandues en France. Si elle ne dispose pas de sauvegarde adéquate, la victime n'aura pas d'autre solution que de payer la rançon, de 400 à 4000 euros au départ, pour retrouver ses données décryptées. Elle prend cependant le risque de payer, sans avoir l'assurance de recouvrer ses données, et ainsi d'être victime une seconde fois.

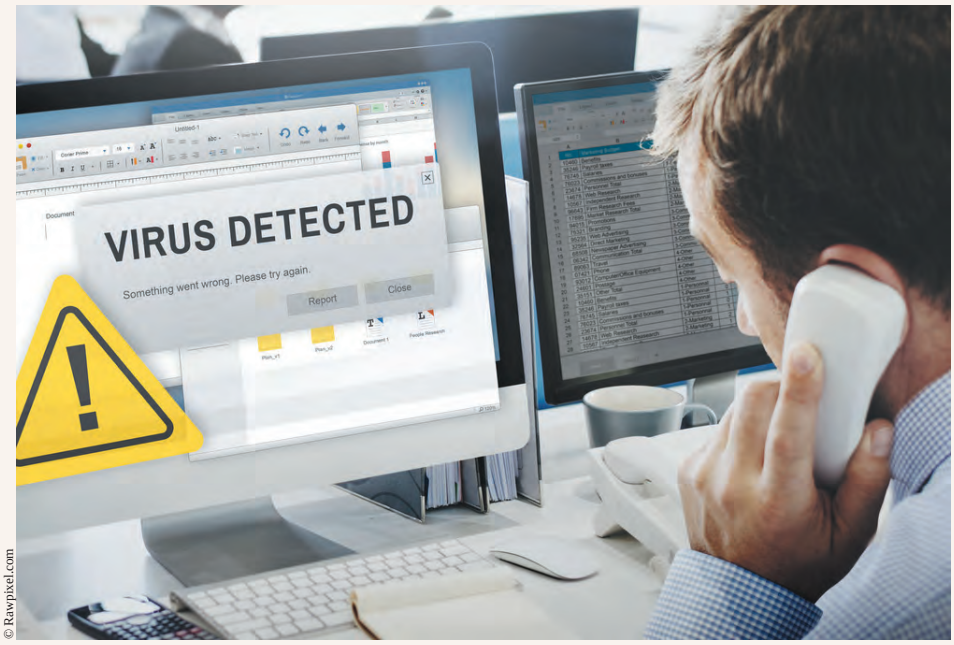
Les faux ordres de virement international (FOVI) représentent un montant supérieur à 300 millions d'euros pour 700 tentatives, avec des pertes allant de 72 000 euros à 17 millions d'euros, au vu des plaintes déposées en France en 4 ans.

3. RÉACTION ATTENDUE

3.1. Réponse à un incident en rapport avec l'audit

Une évaluation aussi rapide et précise que possible de l'incident est nécessaire pour l'orientation du choix du type d'investigation, laquelle dépendra de la nature de l'incident, de l'objectif et de la cible, mais aussi de son origine : interne ou externe, qu'il s'agisse d'accès non autorisé, de comportement malveillant ou frauduleux, de vol de données stratégiques, d'atteinte aux données et à la propriété intellectuelle, etc. Il en ressort des investigations de trois types qui porteront sur les données volatiles, l'investigation légale et l'audit étendu.

Concernant les données volatiles, l'investigation a pour but la recherche de codes



© Rawpixel.com

malicieux (ex. : « virus », cheval de Troie) ou d'activités anormales, qui doivent être détectés au plus vite, pour savoir si une seule machine ou un « *botnet* » est impliqué de l'extérieur et si la cible est l'activité de l'entreprise, son infrastructure en réseaux, un serveur ou un seul poste de travail. Il sera notamment porté attention aux changements de configuration, aux corrections effectuées, ainsi qu'aux anomalies de fonctionnement et à la mise hors tension des ordinateurs et autres organes affectés. Toute trace d'évidence initiale devra être acquise et conservée de façon inforensique[7] et documentée, pour être admise en tant que preuve légale, si nécessaire par après. En fonction des premiers constats, une procédure devrait permettre sans ambiguïté de décider de la suite à donner et des mesures à prendre pour éviter tout prolongement de l'exposition au risque concernant les données sensibles et les éléments vitaux de l'entreprise, tandis qu'une notification s'impose au responsable juridique, pour développer une stratégie et se rapprocher rapidement des autorités pour un éventuel dépôt de plainte. Selon le cas, il s'agira de se diriger ou non vers l'audit étendu avec l'emploi de technologies et méthodes inforensiques pour conduire un audit technique des réseaux potentiellement affectés et identifier l'ensemble des machines compromises.

> En cas de violation de la loi, d'intentions malveillantes ou frauduleuses, les preuves numériques sont critiques. Il y a lieu de contacter au plus vite la police nationale ou la gendarmerie.

L'investigation légale s'adresse à une personne ou un groupe de personnes identifiées ou non, ou dont l'identité aurait été usurpée. Elle est engagée suite à une violation de politique de sécurité, tel que l'accès non autorisé à des données sensibles, la modification non autorisée de celles-ci, ou suite à une conduite inappropriée. Dans le premier cas, le DRH devra être informé des opérations qui seront menées, et dans le second, le DRH et le responsable juridique devront approuver ces dernières, qui devront rester dans la légalité[8] pour confirmer rapidement la suspicion et légitimer la suite des investigations. Il pourrait être fait appel à un huissier de justice pour instrumenter, avec un expert disposant de compétences et d'outils inforensiques *ad hoc* pour respecter le contexte de la preuve numérique. Un rapport sera rédigé et selon les résultats et les implications, des sanctions peuvent être prises en interne. Il peut également être nécessaire de reprendre le processus avec d'autres machines et personnes incriminées. En cas de violation de la loi, d'intentions malveillantes ou frauduleuses, les preuves numériques sont critiques. Il y a lieu de contacter au plus vite les autorités, en particulier la police nationale ou la gendarmerie, selon la zone dont dépend l'entreprise, pour réagir au mieux, déposer une plainte avec les bonnes qualifications au regard du code pénal, et permettre l'avancement de l'enquête, sur la base des éléments précédemment fournis, ou ceux acquis par les enquêteurs spécialisés dont le bon niveau de formation et d'équipement mérite d'être souligné (ex. : enquêteur numérique N'TECH de la gendarmerie nationale ou enquêteur spécialisé en criminalité informatique ESCI de la police nationale). Leur aide sera précieuse.

> Pour pouvoir déterminer la réalité de la situation supposée, il s'agit d'en retracer le déroulement, afin de s'assurer qu'il s'agit bien d'une cyberattaque, et si elle se poursuit ou non.

L'investigation relative à l'audit étendu, proactif ou réactif selon le cas, s'adresse à un ensemble de machines et relève de plusieurs types d'audit, essentiellement dirigés vers le vol de données sensibles, la compromission et les codes malicieux, l'exploration légale avant procès, la violation de politiques de sécurité, etc. En cas de violation, la détermination de l'intention, malveillante ou non, sera déterminée en se redirigeant vers l'investigation légale.

3.2. Sortie de crise suite à une cyberattaque

Pour pouvoir déterminer la réalité de la situation supposée, il s'agit d'en retracer le déroulement, afin de s'assurer qu'il s'agit bien d'une cyberattaque, et si elle se poursuit ou non. Le catalogue et sa dynamique seront déterminants comme indicateurs, tout comme la criticité des services et des processus touchés, pour juger de l'état de crise. Ceci implique la classification des processus, des actifs, des systèmes et des données, associée à un suivi régulier pour la mise à jour, sans omettre l'application de bons réflexes[9].

Au seul plan technique, une infrastructure et un logiciel dédiés à la surveillance des événements, tout comme l'analyse visuelle et automatisée des logs d'accès, de connexion et de trafic, et le constat d'anomalies de comportement, devraient permettre la détection précoce de cyberattaques par corrélation d'événements, ainsi que la suggestion de corrections et d'améliorations à apporter. Ceci est malgré tout insuffisant pour l'assurance de restaurer le système d'information avec un retour à l'activité normale sans trop d'impacts. La réussite tient du niveau de préparation et de la bonne gestion de la situation, tandis que l'échec résulte de la précipitation liée à un manque

de maturité. Il est nécessaire de procurer une réaction adaptée à l'état de la crise et à la variété des cyberattaques en respectant les bonnes pratiques, selon l'état de l'art et les procédures en vigueur. Cette réponse se doit donc d'être planifiée, coordonnée et contrôlée, mais aussi accompagnée d'une communication *ad hoc*. Ceci suppose de disposer de compétences suffisantes, tant internes qu'externes, avec une expertise en termes de management, d'organisation, techniques et juridiques[10]. L'intégration au plan de reprise d'activité (PRA)[11] dans un chapitre destiné à la gestion d'une cyberattaque est naturelle, au vu de la norme sur les exigences du système de management de la continuité d'activité ISO 22301:2014. Celle-ci spécifie les exigences pour planifier, établir, mettre en place et en œuvre, contrôler, réviser, maintenir et améliorer de manière continue un système de management documenté afin de se protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et de s'en rétablir lorsqu'ils surviennent.

CONCLUSION

Les organismes ont des difficultés à appréhender de telles attaques, malgré les efforts consentis, le plus souvent en corrigeant des symptômes et en se limitant au plan technique. Il existe des déficits chroniques et des causes plus profondes. Leur caractère pathologique est en rapport avec la faiblesse intrinsèque des systèmes et des objets connectés et la résilience des organismes pour assurer la continuité des activités en cas de sinistre ou de crise. Leur caractère éthologique relève de comportements qui peuvent être observés comme prompts aux cyberattaques. Les plus courantes restent l'extorsion suite à un rançongiciel - en présence de sauvegardes inadéquates ou incomplètes -, l'escroquerie aux faux ordres de virement international (FOVI) - en l'absence de procédures ad hoc et de signature électronique -, le vol de données - très souvent aussi par des attaques recourant à l'ingénierie sociale -, avec le déni de service (DoS) et la défiguration de sites Web.

À l'évidence, la sécurité est insuffisante tandis qu'une cyberattaque est quasi certaine pour tous, sans savoir ni où elle se portera, ni quand elle aura lieu. Le pire, c'est lorsqu'elle a lieu à l'insu de l'entreprise : elle est discrète et souvent persistante. On peut seulement imaginer pourquoi, lorsqu'elle vise les actifs vitaux et sensibles : finances, informations, savoir-faire, ressources, etc. Comment ? C'est ce qui a été présenté en caractérisant pleinement les cyberattaques, selon un catalogue structuré et la dynamique de leur processus par étapes, formant un modèle utile à la compréhension des entreprises, des spécialistes de la sécurité comme des enquêteurs, notamment pour la détection précoce d'indices pour stopper l'attaque et entamer une action judiciaire. Pour cette dernière, un dépôt de plainte est attendu au plus vite, notamment pour espérer le blocage des fonds transférés à l'étranger en cas d'escroquerie ou d'extorsion. Nous sommes tous impliqués et attendus pour agir, chacun à notre niveau. Il en va de notre responsabilité.

Il faut enfin noter que la cybercriminalité s'industrialise[12] en proposant des services « *Cybercrime as a Service* » à d'autres groupes ou cybercriminels, et notamment des offres en « *Pay-Per-Install* » sur l'Internet et des plateformes spécialisées sur le « *DarkNet* » (ex. : *Darkleaks*) ; il est aussi constaté que « le crime organisé monte de toutes pièces des structures puissantes, véritables entreprises du crime numérique... ». Il faut y répondre en disposant de moyens d'investigation à la hauteur des enjeux internationaux, en passant du discours à l'action, en application d'une stratégie[13]. C'est à ce prix que le pillage systématique des actifs des entreprises et des données attachées à l'innovation, au patrimoine scientifique et technologique, et au savoir-faire national, pourra être évité. De plus, avec le blanchiment, le crime organisé dispose de moyens de plus en plus considérables, exprimés en centaines de millions de dollars, capables d'alimenter la corruption et d'affaiblir l'économie et l'autorité des États démocratiques. ■

Bibliographie

- ANSSI (2012) : Les bons réflexes en cas d'intrusion sur un système d'information. Note d'information du CERT-FR
- G.N. (2011) : "Analyse prospective sur l'évolution de la cybercriminalité de 2011 à 2020". Version 1.0, 55 pages
- https://www.signal-spam.fr/sites/default/files/Prospective%202020%20v1%200_0.pdf
- Guinier D. (1991) : *Sécurité et qualité des systèmes d'information - Approche systémique "La part de l'homme"*. Masson, Paris, 310 pages
- Guinier D. (1994) : *Catastrophe et management - Plans d'urgence et continuité des systèmes d'information*. Masson, Paris, 323 pages
- Guinier D. (1995) : Development of a specific criminology dedicated to information technologies - In *relationship with computers, networks and information highways, 7th Ann*. Canadian Information Technology Security Symp., Ottawa, GoC/CSE-CST, 16-19 mai, pp. 21-45
- Guinier D. (2003) : Ingénierie du plan de reprise d'activité – Spécification rationnelle du PRA et approche par composants et rôles. 15th Ann. Canadian Information Technology Security Symp., Ottawa, GoC/CSE-CST, 12-15 mai
- Guinier D. (2006) : Dispositif de gestion de continuité - PRA/PCA : une obligation légale pour certains et un impératif pour tous. *Expertises*, n° 308, Nov., pp. 390-396
- Guinier D. (2012) : L'inforensique et sa part dans la lutte contre la criminalité organisée et le blanchiment. *La Revue du GRASCO*, n° 3, octobre, pp. 44-50
- Guinier D. (2013) : Les déficits chroniques des entreprises face aux nouvelles menaces - Apport des sciences du danger et des systèmes à la cybersécurité. 6° Forum du Rhin supérieur sur les Cybermenaces (FRC 2013), Strasbourg, 5 novembre
- Guinier D. (2015) : Monnaies virtuelles - Le cas Bitcoin - Risques et rapports à la cybercriminalité et au blanchiment. *Expertises*, n° 400, Mars, pp. 96-100 ; et Le cas Bitcoin - Pourquoi tant d'emballement ? *La Revue du GRASCO*, n° 12, avril, pp. 37-52.
- Guinier D. (2016) : Cyberattaques : Modèle de représentation structurée et dynamique, mesures essentielles et gestion de crise. *La Revue du GRASCO*, n° 14, janvier, pp. 68-80
- Joshi C. et al. (2015) : A review on taxonomies of attacks and vulnerability in *Computer and network system*. IJAR CSSE, Vol. 5, N° 1, pp. 742-747.
- Kervern G.-Y. et Rubise P. (1991) : *L'Archipel du danger : introduction aux cindyniques*. Economica
- Quéméner M. (2015) : *Criminalité économique et financière à l'ère numérique*. Economica, 506 pages
- Wood J. A. (2010) : Darknet : A digital copyright evolution. *Richmond Journal of Law and Technology*, Vol. 16, n° 4

Notes

1. 2013 Verizon data breach investigations report.
2. Ex. "*You have been hacked*!", pour : "Vous venez d'être piraté!".
3. 2014 Mandiant threat report.
4. Etude PwC, réalisée en ligne auprès de plus de 9 700 chefs d'entreprises, responsables de la sécurité, RSSI, de 154 pays.
5. Ponemon Institute 2014 - HP Enterprise Security
6. 2015 Lab. Antivirus Bitdefender : TorLocker est distribué sur le "*DarkWeb*" sous affiliation et son créateur perçoit un pourcentage de la somme extorquée. Il comporte des clés renouvelables permettant de chiffrer les fichiers de la victime, sans être connecté à l'Internet.
7. Discipline portant sur les connaissances, les méthodes et outils, ayant pour objectif la collecte, la conservation, et l'analyse de données électroniques avec la garantie de présenter les résultats en tant que preuves légales. Voir D. Guinier (2012).
8. Dans le respect de la vie privée et des données personnelles des employés et du droit du travail, avec l'exigence de présence de l'utilisateur dans certains cas.
9. ANSSI (2012).
10. Des actions importantes relèvent de la collecte de données de preuves et d'investigations, ce qui nécessite une expertise technico-juridique, et le recours à des méthodes inforensiques plus ou moins complexes, tant pour la sauvegarde et que pour l'analyse pour être judiciairement admissibles. D'autres relèvent aussi de la sauvegarde et de la restauration de données fiables.
11. D. Guinier (1994, 2003, 2006).
12. Comme il a été vu par l'analyse prospective sur la cybercriminalité de 2011 à 2020 (voir G.N. (2011), p. 30).
13. En référence à la stratégie nationale pour la sécurité du numérique présentée par le Premier ministre et aux propositions du rapport du groupe de travail interministériel de lutte contre la cybercriminalité du 30/06/14, visant à améliorer la sensibilisation des publics, la prévention des infractions et la réponse répressive. Voir également M. Quéméner (2015).

SOMMAIRE

Mary-Hélène BERNARD
Rédactrice en chef

Démêler le vrai du faux

Le vrai est « scientifiquement prouvé », le faux est ce qui n'est pas vrai : cela semble simple.

« Je suis ici et pas ailleurs » : oui et non – le téléphone transporte la voix, le cinéma et la télévision l'image ; visioconférences, WhatsApp et autres sont maintenant à la portée de tous.

Lors d'une expertise sur dossier, les pièces transmises sont-elles « vraies » ? Traduisent-elles la réalité ?

Le vrai, quel est-il ?

Ce que l'on voit ? Mais les mirages sont bien connus, fruits d'effets d'optique et de l'imagination.
Ce que l'on entend ? Mais les mots peuvent trahir la réalité et mentir.
Ce que l'on sent ? Mais les odeurs de rose peuvent n'être que des molécules synthétiques.
Ce que l'on ressent ? Mais ces jeux vidéo dans lesquels on se fracasse ne sont qu'illusion.

Avec les démonstrations scientifiques, nous avions cru résoudre le problème du vrai et du faux ; mais avec les années et l'émergence d'autres découvertes, vérité d'hier n'est plus celle de demain.

Le doute dans certains cas, même s'il dérange, est un facteur d'honnêteté intellectuelle et, à condition d'être solidement argumenté, il doit être recevable s'il est expliqué, même et surtout en expertise.

Ce qui est « scientifiquement prouvé » est rassurant pour le citoyen lambda, un excellent argument de vente pour le commercial et un élément de crédibilité pour l'expert, mais crédibilité à un instant donné, sachant que l'état de la science est susceptible d'évoluer.

« Le chat de Schrödinger » (1935) nous en a donné une éclatante démonstration : grâce au raisonnement de la mécanique quantique, le chat est vivant et mort à la fois, ce qui n'est pas pour rassurer notre cerveau « classique » !

Les fameuses « fake news », anciennement « fausses rumeurs », sont devenues un phénomène de société, et leurs contenus – diffusés à grande échelle et à des vitesses vertigineuses via les réseaux sociaux – sont susceptibles d'influencer en masse les honnêtes gens.

Tout cela est décidément bien compliqué.

Et si je vous disais, en conscience : « Est vrai ce que je crois » ?

SOMMAIRE

DIU NATIONAL D'EXPERTISES EN ACCIDENTS MEDICAUX

Objectifs

Fournir les bases théoriques et pratiques nécessaires à l'élaboration des expertises en matière de responsabilité médicale à la demande des commissions de conciliation et d'indemnisation des victimes d'accidents médicaux ou des tribunaux

Personnes Concernées

Médecins titulaires d'une thèse régulièrement inscrits à l'ordre des médecins
Pré requis : un DU de réparation juridique du dommage corporel ou DU d'expertises médicales
A défaut, des autorisations d'inscription pourront être délivrées par le comité de direction en fonction du cursus du candidat

Thématiques Proposées

Responsabilité médicale et dommage corporel / droit médical

Durée, Calendrier, Horaires et Nombre de Participants

Cours **facultatif** en distanciel commun avec le DU expertises du 15 au 17 novembre 2023
Pour ceux qui veulent revoir la nomenclature Dintilhac
2 séminaires sur le droit médical à BORDEAUX avec le Pr Bloch du 8 janvier au 12 janvier 2024
en présentiel (du mardi au jeudi, 9h/12h30 et 13h30/17h30 et vendredi 9h/12h30 et 13h30/16h)
3 jours de cours en distanciel en janv/fév 2024 d'expertises médicales en responsabilité par AMIENS
18 et 19 mars 2024 en présentiel, 9h30/17h30, à la Faculté de Droit 35 place Pey Berland à BORDEAUX
3 jours de cours en distanciel - Mars/avril 2024 (9h/18h)
5 jours de cours en mai 2024 (9h/18h, 17 h le vendredi) en présentiel à Amiens

Chaque inscrit devra justifier d'avoir assisté au minimum 5 expertises avant l'examen de juin 2024.
Les étudiants sont invités à contacter directement des médecins experts de leur région.
50 étudiants maxi

Responsables

Pr C. MANAOUIL (Amiens) et L. BLOCH (Bordeaux)

Renseignements

Pr MANAOUIL Cécile – Service de Médecine Légale et Sociale
CHU AMIENS PICARDIE - 80054 Amiens cedex 1,
Tél : 03 22 08 77 54 fax 03 22 08 97 93 - manaouil.cecile@chu-amiens.fr

Lieux

BORDEAUX et AMIENS

Inscriptions

Les demandes d'autorisation d'inscription (avec coordonnées, adresse e-mail, court CV, photo, lettre de candidature et de motivation, justificatifs de diplôme en particulier d'un DU d'expertise) sont à adresser avant le 15/10/2023 au Pr Cécile MANAOUIL par mail.
Après autorisation du responsable, inscription auprès de Mme DUMONT Dominique, U.F.R. de Médecine d'Amiens, 3 Rue des Louvels - 80036 Amiens cedex 1 - Tel : 03 22 82 54 30

Conditions d'Inscription, Coûts, Validation

Individuel 595,43 € + 90 € (Droits Universitaires) + 100 € (CVEC)
Formation continue financée par l'employeur 1100 € + 90 € (Droits Universitaires)
ou non financée par l'employeur 940 € + 90 € (Droits Universitaires) + 100 € (CVEC)

Validation

Assiduité + épreuves écrites (pas de mémoire) en juin 2024 à Amiens ou à BORDEAUX
Possibilité de passer l'examen à l'ARS pour les candidats des DOM-TOM

Mots Clés

EXPERTISES – ACCIDENT MEDICAL – COMMISSION DE CONCILIATION ET D'INDEMNISATION - RESPONSABILITE MEDICALE- ONIAM RESPONSABILITE ORDINALE

SOMMAIRE

Rejoignez-nous à la CNEMJ !

https://cnemj.fr/

La CNEMJ est une compagnie nationale, association Loi de 1901, regroupant entre autres, des membres actifs, médecins experts de toutes spécialités, et aussi des membres associés ou correspondants, professionnels de santé non médecins, experts inscrits sur une liste de Cour d'appel, de Cour administrative d'appel, agréés ou non par la Cour de cassation, membres ou non d'une compagnie régionale pluri disciplinaire d'experts, et des conseillers spéciaux.

Vous adhérerez à la CNEMJ pour :

- **Être épaulés et défendus en cas de difficultés dans la gestion de certaines missions d'expertises parfois bien délicates,**
- **Communiquer avec d'autres médecins experts, des professionnels de santé experts, français, européens et internationaux sur des sujets qui nous préoccupent, sur certaines jurisprudences,**
- **Écouter des orateurs particulièrement éclairés dans des domaines spécifiques à l'expertise,**
- **Échanger sur le thème des expertises à partir de rapports anonymisés entre experts, magistrats, avocats et professionnels du Droit,**
- **Et tout autre sujet utile pour valider vos actions de formation avec attestations de présence sur demande.**

Notez dès à présent :

A Reims

Vendredi 13 octobre 2023

Crime et expertises, à la cour d'appel avec dîner dans le caveau de champagne MUMM :

A Paris

Vendredi 24 novembre 2023

Le secret en expertise, au cours d'un Entretien Expert de Cochin :