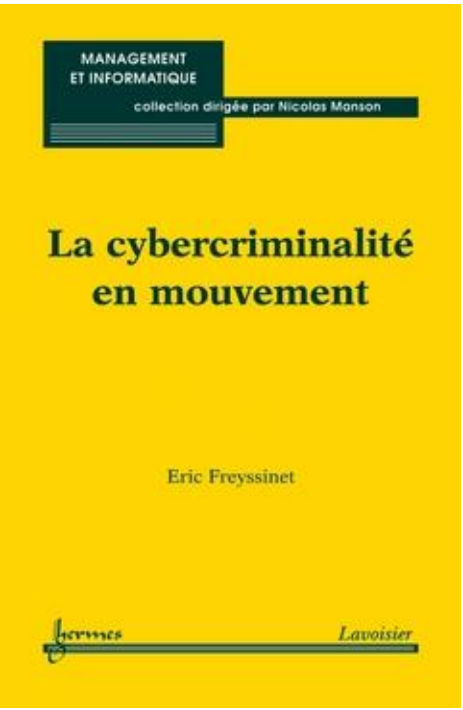
La Cybercriminalité en Mouvement



J'aborde peu souvent les publications onéreuses pour les porter à l'attention des modestes lecteurs de la Mare, estimant qu'il y a assez de ressources libres bien faites pour s'éviter d'avoir à se procurer des ouvrages payants. Ainsi, ce sont essentiellement les publications MISC qui sont portées à votre attention via le blog, lorsqu'elles sortent. En autodidactes, amateurs, simplement passionnés, le coût de la vie au quotidien est déjà assez important, pour s'éviter des frais d'une passion onéreuse. Je vais vous parler de *La Cybercriminalité en Mouvement*, d'Eric Freyssinet.

Un prix prohibitif contraire à l'esprit de l'ouvrage

Mon premier bémol ainsi sur l'ouvrage sera donc celui-ci : son prix. De 56 à 60€, sur les plateformes d'achat Web ou sur le site éditeur, l'ouvrage n'est pas à la portée de tous pour un sujet qui concerne pourtant tout le monde, et dont le contenu se manifeste avant tout à démythifier la cybercriminalité à destination de tout à chacun. Un grand regret donc pour ce prix. D'autant que l'auteur, Eric Freyssinet, officier de gendarmerie en pointe sur la cybercriminalité, ne court pas après un revenu d'appoint. Il s'agit sans doute d'une volonté éditoriale, émanant des propositions des professionnels de la publication. Le document aurait gagné en visibilité et en portée en étant distribué sous un format Libre et gratuit en version numérique, et tel quel en version papier. Un peu comme le sont les publications parlementaires, d'intérêt public.

En un peu plus de 200 pages, l'auteur nous dévoile un panorama complet de la cybercriminalité constatée, ses évolutions, et les tendances dégagées. Le contenu est à portée de tout lecteur, intelligible sans éléments techniques trop importants qui pourraient rebuter les non spécialistes. Les références sont nombreuses et permettraient de poursuivre les lectures d'un coup d'œil plus affûté techniquement.

Le primat de la source académique

Je regrette cependant les sources exclusivement académiques, ou presque. Le souci avec ce type d'ouvrages est la volonté d'acquérir ou de conserver la crédibilité du constat posé, et les chercheurs universitaires et parlementaires français ne se contenteraient pas de sources non académiques. Très certainement. C'est une tare française je pense, où la visibilité et la crédibilité ne s'acquièrent pas par des démonstrations et de preuves de faisabilité, mais par des titres et diplômes théoriques acquis en amont. La compétence dans notre système éducatif et professionnel est moins valorisée que la connaissance théorique générale sanctionnée par des examens éducatifs. L'auteur évoque à demi-mots ce constat en deux points de l'ouvrage. Ainsi, lorsqu'il aborde une énumération –indicative et non exhaustive comme il l'annonce par lui-même - des conférences de sécurité où des informations et des techniques transverses et multidisciplinaires sont abordées (page 194), et s'interroge sur la –ou non- pertinence des officiels de la lutte contre la cybercriminalité de s'y associer, il évoque l'ambiance non académique de ces rassemblements, un peu comme pour s'excuser que la compétence

y soit au rendez-vous et que malgré la non institutionnalité de ces manifestations il y ait pertinence à s'y rendre.

La notion est également abordée lorsqu'il aborde la partie 'droit' de la lutte contre la cybercriminalité, où il établit justement que l'organisation et la recherche en la matière n'est pas toujours le fait d'institutions et d'organismes établis, mais aussi le fait d'indépendants et de particuliers, de façon moins formelle, où les textes législatifs sur l'usage d'outils, et le partage d'informations sensibles, peuvent les ostraciser et les condamner suivant les transpositions établies dans les documents législatifs nationaux de la convention du Conseil de l'Europe sur la Cybercriminalité. Paradoxalement, c'est la partie qui m'a semblé la plus intéressante pour un non initié : la partie droit, applications, jurisprudences. De l'aveu de l'auteur, c'est un mille-feuilles législatif incompréhensible aux particuliers et non-initiés, qui gagnerait à être dépoussiéré et actualisé, suivant quelques pistes suggérées dans l'ouvrage.

Un propos lisse et consensuel –ou presque

Fort de sa crédibilité et de son autorité institutionnellement incontestée sur le domaine, je déplore le contenu parfois trop lisse du document et des propos. A la façon d'un rapport parlementaire (qui n'en est pourtant pas un), des éléments sont abordés, sans appréciation personnelle, d'une façon monocorde et sans éclats. Nul doute pourtant qu'un coup de gueule salutaire aurait été parfois utile et entendu, surtout venant de sa part. Ainsi, quelques éléments m'ont fait bondir à la lecture de l'ouvrage.

Par exemple, il évoque en page 36 l'un des fameux 'ransomware' de l'année 2012, aux logos institutionnels de la Gendarmerie (des variantes Police, d'organismes européens institutionnels ou privés, d'autres pays de la zone euro existent aussi) et parle d'une remontée sur les espaces d'échanges officiels des spécialistes à la mi-décembre 2011. Les versions d'autres langues laissaient présager des versions françaises à venir ; sur les forums de désinfection où les amateurs désintéressés aident à nettoyer les ordinateurs à distance par l'énumération de consignes, ces infections étaient présentes déjà depuis plusieurs semaines aux langues et logs d'autres nations et organismes. Malekal Morte, Xylit0l, acteurs privés non institutionnels, via MalwareScene, évoquent les premiers échantillons français dès décembre (les premières variantes –allemandes- dès avril pour Xylit0l, Kaspersky dès Mars). **J'avais cru pouvoir discerner là une dissonance temporelle entre les remontées officielles et le constat privé, mais non je me trompe, comme me l'a fait remarquer l'auteur**.

En revanche aucune observation personnelle sur le refus de certaines petites entités judiciaires (des gendarmeries isolées par exemple) refusant d'enregistrer la plainte d'utilisateurs lésés (l'auteur évoquant cet exemple en revanche dans des suggestions de remontées public/justice plus affûtées mais moins protocolaires afin de préserver la primeur de l'information sans alourdir la prise en charge des plaignants par les entités) ; il en a donc conscience, mais ne le commente pas.

En page 105, il aborde l'exemple d'un *scareware* géré en Ukraine, traité par les autorités américaines à l'amiable finalement, avec un dédommagement important (8 millions de dollars) pour l'arrêt des poursuites. J'aurais aimé un parallèle avec un exemple français et une observation personnelle. Je pense à l'affaire Viguard par exemple, où le débat juridique a ignoré le mensonge de l'outil pour inciter à l'achat mais s'est porté sur la façon dont le chercheur a démontré l'arnaque, pour finalement le condamner. Je n'ignore pas qu'on ne commente pas une décision de justice, mais je crois qu'on peut apprécier et mettre en perspective des jurisprudences. Je sais que ces faits sont clivants, et font débattre encore aujourd'hui, suivant le point de vue adopté. Mais justement, à mon sens l'auteur est en mesure de donner le 'la' institutionnel sur la façon d'aborder ces éléments, je regrette qu'il n'en profite pas. J'ai conscience que nous ne sommes pas exactement dans le même cas de figure, avec un vrai *scareware* incitant à l'achat, via de fausses menaces détectées. Mais

nous sommes dans le même type de bulle mercantile mensongère. Sur ce type de recherches, où le droit des affaires (via les conditions générales d'utilisation) s'oppose à l'intérêt général (par le décorticage illégal des fonctionnalités d'un outil informatique), pas une observation.

En page 118, l'auteur aborde la future fameuse obligation de notification des incidents de sécurité. Nulle part l'auteur ne commente l'obligation de notifier les utilisateurs, se contentant de commenter et prendre acte de la notification aux CNIL. Là encore, sa parole aurait du poids et pourrait permettre peut-être d'influencer les législateurs par une prise de position argumentée. Mais pas de prises de position sur ce sujet non plus. N'y a-t-il que moi pour m'offusquer que les utilisateurs ne soient pas notifiés de la fuite de 'données personnelles' les concernant, quels que soient la nature des fuites et les moyens mis en place ensuite ?

En page 130 est abordé le fameux sujet des 0-Day, leur divulgation, leur exploitation, la mise en place d'outils, etc. Très succinctement à vrai dire. Il y aurait eu matière à développer les notions de *full-disclosure* et son opposé, la légalité ou illégalité, l'idéal à atteindre, les moyens coercitifs de contraindre les acteurs à sécuriser ou non des outils et accès grands publics, les obligations de sécurisation (existantes pourtant pour les particuliers, cf. Hadopi) de prestataires d'hébergement ou de services Web. Pas un mot sur ces aspects, pourtant très largement encore débattus aujourd'hui. L'auteur avait abordé ces notions sur son blog, sans jamais réellement exprimer d'opinion personnelle, juste un point de vue d'officiel sur les éléments. Au delà des 0-Day, et des latences des éditeurs à corriger des vulnérabilités notifiées, j'aurais souhaité là encore lire des observations personnelles sur le fait qu'un portail institutionnel possède des identifiants *admin/admin* valides et sur le signalement de telles aberrations qui parfois légitime des plaintes.

En page 136, l'auteur évoque la légalité et la libéralisation des techniques cryptographiques, en 2000. Pas un mot là non plus sur ce retard à l'allumage de la législation française alors qu'en amont d'ouvrage en faisant la genèse de la cybercriminalité, la nécessité de préserver les échanges était démontrée bien plus tôt. Pas un mot sur cet aspect encore, et la désuétude des textes, là aussi en dissonance avec l'époque.

En page 138, en abordant l'encadrement des moyens légaux d'interception et de surveillance des communications informatiques, introduit dans l'arsenal législatif par LOPPSI (appelée LOPPSI2 par habitude, mais les 2 p désignant déjà la 2^{e} mouture, il y a redondance, la première étant LOPSI), sans doute pour rassurer, l'auteur rappelle que *ces matériels sont soumis à autorisation ministérielle pour la détention et la commercialisation et que ces dispositifs sont placés sous le contrôle d'une commission consultative et la responsabilité administrative de l'ANSSI*. Le propos se veut rassurant.

Je ne peux toutes fois m'empêcher de faire un parallèle entre ces dispositifs « localisés » à destination d'une machine, et d'autres plus « globaux » à destination de services étatiques étrangers qui n'ont paraît-il pas d'existence sur notre territoire. L'auteur ne peut ignorer les révélations et les affaires (Amesys par exemple), que beaucoup de ses contacts Twitter relaient sans relâche (fo0, Bluetouff, Kitetoa, etc.). Paradoxalement, en voulant rassurer sur l'emploi et l'encadrement juridique de ces techniques et matériels, j'aurais tendance à considérer que l'auteur désavoue malgré lui les prises de positions officielles de la diplomatie française. Je mélange peut-être tout là dans un mauvais procès, mais que l'on reconnaisse ou non la dualité de ces technologies d'interception à grande écoute, cela reste des moyens légaux d'interception et de surveillance, non ?

Page 171, en rapportant les échanges avec Wout de Natris sur '*qui développe la réglementation Internet*', l'auteur semble faire sienne l'opinion exprimée, à savoir la proposition consensuelle de dialogue et de compréhension mutuelle comme préalable à tout dialogue et évolution des réglementations internationales afin de lutter contre la cybercriminalité. Là encore, je regrette qu'il ne détaille pas certaines dispositions

législatives françaises, passées en force sans recherche de consensus, et qu'il ne s'exprime pas personnellement.

Dans la partie *Le partage comme arme*, en page 187, l'auteur énumère quelques initiatives institutionnelles et privées de remontées d'informations accessibles au grand public (comme *phishing-initiative*, par exemple). Là encore, pas d'observations personnelles sur le fait que certaines initiatives privées auraient dû l'être bien en amont des autorités institutionnelles, si elles avaient pris la mesure des soucis en temps et en heure. *Je m'étonne que l'auteur ne s'en étonne pas* en fait, pourrais-je dire avec malice.

Enfin, en page 203, dans l'annexe A, une énumération rapide des acteurs institutionnels de la lutte contre la cybercriminalité est abordée. Encore une fois, je regrette qu'il n'aborde pas les budgets associés (toujours trop faibles) et ne pointe pas certaines iniquités dans le budget alloué au traitement des infractions (je pense au budget de l'Hadopi par exemple). J'aurais souhaité lire l'auteur, acteur principal de la lutte contre la cybercriminalité, prendre position ou ne serait-ce que commenter la disparité des budgets alloués. Encore une fois, je reste sur ma faim.

« *En effet, l'espace numérique est le même pour tous. Les personnes et les organisations (…) sont les mêmes et, pour l'essentiel, leurs outils quotidiens sont identiques. Les motivations et l'intensité recherchée peuvent varier, mais les armes sont presque toujours semblables : un escroc, un espion, un terroriste ou même un manifestant numérique, nous l'avons vu, utilisera des outils similaires. Bien entendu, il ne faut pas tout mettre sur le même plan et la réponse doit être adaptée aux risques réellement encourus et aux motivations* ». C'est une partie de la conclusion, empreinte de bon sens, et rassurante. Mais l'actualité judicaire, à mon sens dément ce point de vue. L'affaire Triskel/EDF pourrait l'illustrer par exemple. Il y aurait eu matière aussi à développer l'aide pas toujours légale –je pense, au regard du droit international- de certains *clusters* à la diffusion d'informations et la position d'un officiel de la Gendarmerie –à défaut de connaître LA position officielle des institutions. Là encore, je pense à certains de ses contacts Twitter, membre affichés de Telecomix, et sur lesquels l'auteur ne peut pas ne pas avoir d'observations personnelles.

Une mauvaise grille de lecture personnelle

En conclusion de ma modeste fiche de lecture très subjective, j'en conviens, et tous mes propos sont légitimement discutables et contestables, cet ouvrage est un panorama des moyens criminels et des outils de lutte contre la cybercriminalité. Je n'ai rien appris à la lecture de cet ouvrage, je ne suis pas pourtant un professionnel du domaine, juste un intéressé. En revanche, j'ai redécouvert des éléments que j'avais perdus de vue et que j'avais lus ailleurs. C'est le point fort du document : condenser en un texte intelligible à tous, en français, des informations disparates que l'on retrouve sur une multitude de plateformes et sources d'informations différentes. C'est à mon sens un état de lieux presque exhaustif de la cybercriminalité aujourd'hui, en cela la masse d'informations compilées, digérées et reformulées est impressionnante. Et c'est comme cela qu'il faudrait prendre l'ouvrage en amont, avant même de commencer à le parcourir : comme un état des lieux, émanant d'une autorité institutionnelle ou législative officielle. Pas de Monsieur Freyssinet, qui ne s'exprime presque pas personnellement. C'était mon erreur d'appréciation avant même de commencer l'ouvrage. Le devoir de réserve militaire a la vie dure, et il n'y a –je crois- de pire censure que celle que l'on s'impose. S'il y a bien quelqu'un qui possède la légitimité à s'exprimer sur ces sujets, c'est l'auteur de l'ouvrage. « *Car oui, au risque de passer pour le naïf de service, je suis convaincu, à le lire, qu'il a les fesses entre deux chaises* » écrivait déjà Bluetouff en 2010.

Ma grille de lecture était faussée, parce que je pensais découvrir des observations personnelles d'un officiel de la lutte contre la cybercriminalité. Mais quasiment tout l'ouvrage reste consensuel dans les points de vue

abordés, et sans étonnement on constatera, comme l'a fait observer M. Bortzmeyer via une fiche de lecture sur son blog, que le point de vue de l'enquêteur est celui exclusivement retenu –avec le souhait de voir la législation abonder en ce sens (ce qui ne manquera certainement pas d'arriver) malgré quelques timides recommandations de préserver le nécessaire anonymat des internautes en certaines circonstances. Sans indiquer quelles pistes de réflexion permettraient de préserver cela.

Vu l'intérêt public de la portée de l'ouvrage -et le contenu accessible à tous démontre la finalité avouée de pouvoir être compréhensible de tout à chacun- il me semble qu'il aurait gagné en visibilité à être distribué numériquement gratuitement, à peut-être disposer de sa propre plate-forme (qui existe déjà pourtant, lcem.fr, sans doute d'une initiative privée de l'auteur) permettant de consulter l'ouvrage complet en directe lecture. C'est un de mes grands regrets, le prix le restreignant à un nombre limité de lecteurs, déjà sensibilisés à la thématique, et qui ne sont pas le public avoué -vu l'écriture- de l'ouvrage. Je crois qu'ainsi cet ouvrage passera à côté de son public ; les seuls investissant une telle somme le seront d'une majorité de professionnels, qui finalement ne découvriront rien de ce qu'ils ne sachent déjà. Mais il est à lire et, encore une fois, d'intérêt public.

Pour terminer, je dois souligner la démarche volontaire et participative de M. Freyssinet. Ce qui me permet aujourd'hui –presque effrontément- de porter un œil critique et subjectif sur cet ouvrage, en amateur avoué et déclaré, alors que l'auteur est officier de Gendarmerie, polytechnicien, hyper compétent dans ses domaines de prédilection (la lutte contre la cybercriminalité), c'est son accessibilité et sa démarche innovante de visibilité sur les réseaux sociaux (blog personnel, compte Twitter personnel, participation –encore personnelle- à des évènements non institutionnels comme PSES2012, etc.) et les plateformes informelles d'échange. Cette proximité est une réelle innovation et traduit un engagement humain et personnel au-delà de l'image institutionnelle presque figée.

Cet homme est brillant jusque dans son accessibilité aux autres ; cela traduit –à mon sens- une franche démarche de constante remise en question, personnelle et professionnelle. Comme la technologie. Cet homme est de son temps, de notre époque. Cela est rassurant.