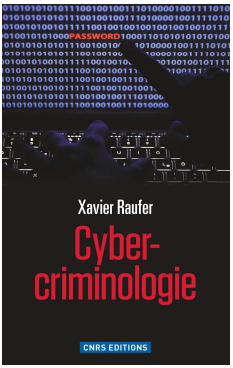
Xavier Raufer

Cyber-criminologie

CNRS EDITIONS

Présentation de l'éditeur :



L'ampleur enfin révélée de la criminalité organisée dans le cyber-monde

« L'univers cybernétique est désormais l'un des principaux domaines de la fraude et du crime », a déclaré un expert anglais à la suite du piratage de 233 millions de fiches clients d'un géant du e-commerce. Aujourd'hui, les victimes de la cyber-criminalité se comptent par dizaines de millions, des stars d'Hollywood aux habitués des réseaux sociaux ou du commerce en ligne. Comment, à partir de quels ordinateurs et de quelles techniques les nouveaux gangs du net opèrent-ils ? C'est ce que révèle le nouveau livre de Xavier Raufer. Fondé sur des informations seulement connues des spécialistes, *Cyber-criminologie* dévoile la gravité d'un phénomène qui menace le citoyen ordinaire, les grandes entreprises, les États, les banques, etc. Piratage et vente clandestine de données personnelles, maliciels pénétrant les ordinateurs publics et privés, fraudes identitaires ou à la carte bancaire, sites marchands illicites cachés dans le *dark web* : le monde du cyber-crime est aussi florissant qu'insaisissable.
Xavier Raufer explique ici comment notre société hyper-connectée a donné naissance à un cyber monde où prolifèrent hackers, mafias du net russes, chinoises ou iraniennes, *hacktivists* libertaires exploitant les failles de nos systèmes informatiques. Sans parler de la surveillance omniprésente des États comme l'affaire Prism l'a révélé. Des dangers qui vont de pair avec la croissance exponentielle du Net…

Xavier Raufer, criminologue et enseignant à l'université Panthéon-Assas, est l'auteur de nombreux ouvrages dont Les nouveaux dangers planétaires *(Biblis).*

Cyber-criminologie

Xavier Raufer

Cyber-criminologie

CNRS ÉDITIONS
15, rue Malebranche – 75005 PARIS

Du même auteur (depuis 2010)

(Ouvrages de l'auteur jusqu'à 2010 : voir le site www.xavier-raufer.com)

Criminologie – la dimension stratégique et géopolitique, Collection Sécurité Globale, Eska, 2014

Géopolitique de la mondialisation criminelle, *la face obscure de la mondialisation*, Presses Universitaires de France – 2013

Les nouveaux dangers planétaires, chaos mondial, décèlement précoce, CNRS Éditions, 2009 et Biblis, édition de poche, février 2011 – Ouvrage couronné par l'Académie française

Quelles guerres après Oussama ben Laden ? Plon, 2011

ISBN : 978-2-271-08561-0

À la mémoire de Laurence I.
qui, la première, m'entraîna dans ce monde inouï.

Sommaire

QUATRIÈME PARTIE
La cybercriminalité en action

CINQUIÈME PARTIE
À l'horizon 2020, trois questions majeures

SIXIÈME PARTIE
Prescrire

Quatre thèses fondatrices de la cyber-criminologie

• *Diagnostic 1* – Dans l'ensemble « cybercrime », crime domine. Scruter le monde cybercriminel révèle que celui-ci n'a rien inventé d'original. Dans leur propre milieu et jusqu'à présent, les cybercriminels se bornent à reproduire les variantes de la criminalité physique.

• *Diagnostic 2* – La cybercriminalité ne régressera pas grâce à plus encore de haute technologie, mais par volonté politique. Une simple fuite en avant de type blindage-et-canon provoquerait, dans ce domaine, un désastre analogue à celui de l'inepte guerre *high-tech* d'Irak.

• *Traitement 1* – Il faut au cybermonde un code de la route comme, en son temps, la société de l'automobile suscita le sien. Ce code devra être conçu et imposé par une coalition de nations puissantes, dans l'espoir raisonnable qu'il s'imposera mondialement. Autre image possible pour l'indispensable superstructure normative : celle de la tour de contrôle.

• *Traitement 2* – Le code de la route vaut pour tout véhicule, luxueux ou modeste : de même, seul un code du cybermonde sanctionnera-t-il efficacement les prédateurs, financiers maraudeurs, géants du net, etc. qui, aujourd'hui, le pillent impunément ou exploitent ses usagers.

Glossaire

Ce glossaire n'a nulle prétention encyclopédique. Il vise simplement à faciliter l'accès au texte en traduisant et/ou définissant des mots, concepts & acronymes peu familiers aux non-spécialistes.

Les définitions et expressions originales en langue anglaise (émanant de sources officielles anglo-saxonnes) ont été traduites par l'auteur.

Anonymous : Groupe hacktiviste (voir ce terme, plus bas) déstructuré et protoplasmique, sans hiérarchie ni autorité centrale. Son slogan est : « Nous sommes légion. Nous ne pardonnons pas. Nous n'oublions pas. Craignez-nous », et son icône, le masque de Guy Fawkes, est désormais bien connu. Fondé en 2003 dans un esprit libertaire de type Robin des Bois, Anonymous multiplie depuis les cyberattaques sur des cibles estimées malfaisantes ou dictatoriales : l'Église de Scientologie, informatiquement harcelée par de mauvaises blagues ; attaques DDoS (voir ce terme, plus bas) contre les systèmes de paiement en ligne, Paypal, etc. qui bloquent des contributions financières à Wikileaks et aux grands « lanceurs d'alerte » comme J. Assange, E. Snowden, etc. ; attaques des sites du gouvernement tunisien lors du « printemps arabe ». Pendant le conflit dans la Bande de Gaza en juillet-août 2014, Anonymous, indigné par les massacres de civils, attaque divers sites officiels israéliens, dont celui du Mossad, de l'armée, du Premier ministre, du Conseil national de sécurité et du ministère de la Justice.

AET (Advanced Evasion Techniques, techniques de contournement avancées) : « déguisement » pour pénétrer les cibles (sites, réseaux, systèmes) et y actionner ensuite des logiciels pirates. Logiciel malveillant (*malware*) polymorphe, aux multiples potentialités dangereuses, l'AET pénètre en douceur sa cible en plusieurs points ou plusieurs fois. Ces éléments sont d'apparence innocente et ne sont pas reconnus comme dangereux par les systèmes de protection (coupe-feu) de l'ordinateur (IDS, Intrusion Detection Systems, voir ce terme). Une fois « dans la place » et selon de multiples agencements, l'AET recompose ses divers éléments, pour ensuite saboter, piller, etc. Les premiers AET ont été signalés en 2010.

APT (Advanced Persistent Threat) : attaque informatique ciblée et sophistiquée dont les auteurs ont les moyens et le temps d'arriver à leurs fins. Complexe et menée par des pirates experts, l'APT cherche en général à siphonner des bases de données.

Backoff : redoutable maliciel (ou *malware*, voir plus bas ce terme) repéré pour la première fois en octobre 2013. Dans la mémoire d'un ordinateur cible, Backoff siphonne toutes les données concernant les cartes de paiement (qu'ensuite, le pirate n'a plus qu'à vendre), lit les frappes du clavier pour y copier les mots de passe et, surtout, installe au cœur du système une trappe pour conserver l'accès à l'ordinateur cible, s'il « crashe » ou est réinitialisé. Cette trappe rend sans cesse Backoff améliorable et modifiable.

Big Data : océan toujours plus illimité de données rassemblées dans le Cloud (voir ce terme plus bas). Milliards et milliards de traces numériques (chiffres, textes, images, photos, etc.) laissées par qui use d'une carte de paiement, d'un smartphone, consulte Internet, achète en ligne, etc. Big Data permet l'analyse de données par masses énormes et à très grande échelle, en théorie pour

améliorer le suivi des clients, anticiper les besoins du marché ou favoriser les échanges entre objets connectés. Mais derrière les chiffres et propos extatiques, Big Data constitue sans doute le plus grand système de surveillance jamais imaginé, au service de certains gouvernements et des géants du net. Notons que depuis août 2014, la Commission générale de terminologie et de néologie, chargée de favoriser l'enrichissement de la langue française, demande de dire « mégadonnées » et non plus big data.

Bitcoin : cybermonnaie, ou devise numérique, lancée en 2009. Dès son origine, elle séduit à la fois les internautes d'orientation libertaire et les *fans* de high-tech. Pour ses promoteurs, bitcoin est destiné à devenir un système alternatif de paiement – peut être la vraie monnaie mondialisée qu'attendrait, selon eux, le XXIe siècle. Mais en fait, bitcoin a d'abord intéressé les criminels. Fondée sur un système de pénurie organisée, intraçable et gérée par un vaste réseau centralisé, bitcoin ne dépassera jamais les 21 millions d'unités – d'où, sa forte volatilité. En juin 2014, on en comptait quelque 13 millions en circulation et un bitcoin valait environ 600 dollars.

Black Hat : dans le registre gentils/méchants, Silicon Valley reconnaît deux sortes de hackers, ou pirates, les *white hat*, n'ayant pas d'objectifs illicites mais au contraire l'intention positive d'améliorer le cybermonde ; et les *black hat*, qui eux, piratent pour voler, saboter, etc. Depuis 1997, se tient chaque année à Las Vegas une Black Hat convention – qui devrait plutôt se nommer « White Hat Convention » mais les pirates attirent les foules – où convergent des milliers d'informaticiens et d'experts en sécurité, pour présenter et vanter leurs intrusions les plus spectaculaires, étudier les cyber-risques émergents et tenter d'améliorer la sûreté des systèmes et réseaux.

Botnet : réunit les deux mots anglais roBOT et NETwork (robot et réseau). Ce dispositif informatique assemble en un

réseau des ordinateurs « kidnappés » à distance, à partir desquels les pirates accomplissent ensuite des actes malveillants, comme des envois de Spam ou des attaques type DDoS (voir plus bas ces deux termes).

Chiffrage/cryptage : le plus souvent, il consiste à transformer un texte clair en une suite de signes apparemment privée de tout sens. Conduite à l'aide d'une clé secrète, cette opération mathématique vise à produire un document final chiffré, incompréhensible à tout autre que son destinataire. Au total, le chiffrage répond à trois besoins : authentification (l'auteur est le vrai) ; intégrité (le texte n'a pas été altéré) ; confidentialité (le tiers indésirable n'y a pas accès).

Chief Information Security Officer (CISO) : Aux États-Unis, c'est le responsable de la sécurité informatique d'une entreprise, d'une administration, etc. Une petite majorité des entreprises américaines de 1 000 employés et plus possède un CISO à temps plein ou partiel. On verra plus bas que l'entreprise de grande distribution Target (la 3e des États-Unis), qui fut victime en 2013 d'un immense siphonnage ayant pu affecter jusqu'à un tiers des cartes de paiement du pays, n'a embauché un CISO qu'après la catastrophe. Attitude jusqu'ici fréquente pour des entreprises, même importantes. Voir aussi plus bas l'équivalent français RSSI : Responsable de la Sécurité des Systèmes d'Information.

Cloud : Dispositif d'informatique dématérialisé, au sein duquel les données et informations sont stockées dans des ensembles de serveurs connectés.

CloudBot : Des hébergeurs en ligne proposent souvent (à leurs débuts) des comptes gratuits sur le cloud pour séduire de nouveaux clients ; dans ces *data centers*, des développeurs peuvent stocker leurs travaux sans encombrer leurs propres ser-

veurs. Or nombre de ces startups « Data Centers » ne demandent qu'une adresse courriel aux clients ainsi hébergés. Il suffit donc d'ouvrir une quinzaine de ces comptes puis d'assembler en un CloudBot l'espace de stockage ainsi acquis, (comme on le ferait dans le monde physique pour les wagons d'un train, derrière une locomotive), pour disposer gratuitement d'un superordinateur qui peut ensuite servir à lancer des attaques DDoS, « casser » des mots de passe, spéculer sur des monnaies numériques, etc.

Computer Network Exploitation : dans le langage de la NSA (voir la cinquième partie du livre) et du Cyber Command US, ce terme désigne toutes les cyberattaques et opérations visant à infiltrer des logiciels de contrôle dans des réseaux informatisés étrangers ; à s'y ménager des accès clandestins, pour y susciter et maintenir une présence. Objectif : en usant d'un cyber-arsenal secret, se livrer à des manipulations, sabotages, prises de contrôle, destructions, récupérations de données. Plus largement : obtenir des secrets militaires, du renseignement et intercepter des communications.

CSIRT (Computer Security Incident Response Team), ou **CERT (Computer Emergency Response Team)** : au niveau national ou régional, cellule/équipe d'alerte et de réaction aux attaques, piratages, etc.

Cyberattaques – définition du National Research Council, Washington, 2009 : « Opérations délibérées visant à altérer, perturber, tromper, dégrader ou détruire les dispositifs ou réseaux d'un système d'information et/ou les programmes résidant ou transitant par ces mêmes dispositifs ou réseaux ». Autre définition (*Yale Journal of International Affairs*, *cf.* références) : « Une cyberattaque vise à invalider les systèmes digitaux critiques des institutions centrales d'un État-nation : militaires, politiques, sociaux ou économiques ; ou encore utilise le cyberespace pour attaquer les infrastructures d'une société dévelop-

pée comme ses réseaux de transport d'énergie, ses systèmes financiers ou ses services d'urgence ». Une cyberattaque a de nombreux avantages : coût modeste, anonymat, large choix de cibles, frappes possibles de l'autre bout du monde, difficulté à identifier l'attaquant et à localiser l'origine réelle de l'attaque. À l'inverse de ces opportunités, la crainte majeure de tous les états-majors, cyber ou non, est le « Pearl Harbour électronique ».

Autre définition de la cyberattaque, en français : « agression illégale visant des ordinateurs ou des réseaux, ainsi que les informations et données qui y sont contenues, dans l'idée d'intimider ou de contraindre un gouvernement ou une population, pour un motif politique ou social. Cette attaque implique toute forme de violence contre des personnes ou des biens ; ou, au minimum, provoque assez de dégâts pour inspirer la crainte. Exemple : attaques entraînant la mort ou des blessures ; provoquant des accidents aériens, la contamination d'eau potable, des pertes économiques ou financières lourdes. Au-delà, toute attaque grave visant des infrastructures critiques ».

Cyber-baronnies (*robber barons*) : empires numériques comme Amazon, Facebook, Google, etc.

Cybercrime : Lors de sa Convention de Budapest, le Conseil de l'Europe a produit en 2001 (entrée en vigueur, 2004) le premier instrument juridique international opérationnel sur la cybercriminalité. En 2004, l'Organisation des États américains a produit une *Comprehensive inter-American strategy to combat threats to cyber-security*. Selon l'ONU Drogue & Crime (ONUDC), le « chiffre d'affaires » du cybercrime représenterait 0,8 % du Produit Brut Mondial (PBM) ; le crime organisé hors cybercrime, 1,2 % du PBM et la piraterie maritime 0,2 % du PBM.

Cyberespace : L'ultime territoire hors contrôle – mais aussi 5^{e} domaine des opérations militaires (terre, mer, air,

espace, cyberespace) et lieu d'une possible « course au cyber-armements ». Voici la définition du ministère américain de la Défense en 2008 : « Domaine global de l'environnement informatif humain, formé de réseaux interdépendants au sein des infrastructures des technologies de l'information, incluant l'Internet, les réseaux de télécommunications, les dispositifs informatiques et leurs propres systèmes de traitement et de contrôle… Le royaume des réseaux informatisés, dans lesquels l'information est rangée, partagée et diffusée en ligne ».

Cyber-espionnage – définition du FBI : « Usage ciblé des ordinateurs visant à obtenir un quelconque secret ».

Cyberguerre – définition de l'US Air Force : « Capacité à détruire, interdire, dégrader, perturber ou tromper… Tout en se protégeant de pratiques hostiles au sein du cyberespace visant à un identique objectif ».

Cybernétique : science dont procèdent l'informatique et Internet. En grec ancien, *kubernesis* est l'art de tenir un gouvernail, plus largement de piloter les navires. Aujourd'hui, c'est la science des systèmes autorégulés et des interactions entre systèmes gouvernants (contrôle) et gouvernés (opérations).

Cyberterrorisme – définition du FBI : « Attaque préméditée et politiquement motivée visant des systèmes informatiques ou des dispositifs informationnels, des logiciels et des données, le tout résultant en des violences subies par des cibles civiles ; ces attaques étant commises par des entités humaines ou par des opérateurs clandestins ».

Dark wallet : service, logiciel, etc. illicitement conçu pour rendre et maintenir invisible toute transaction digitale (financière, d'abord).

Dark web ou web profond : apprentis sorciers voulant « chevaucher le tigre » ? Cyniques ? Comme on le verra tout au long des parties IV et V de cet ouvrage, le « web profond » fut créé par l'Amérique officielle, comme réseau entièrement privé et anonyme. Dix ans plus tard, ce paradis électronique du cybermonde – équivalent contemporain de la « cour des miracles » du Moyen Âge – regroupe une infinité de bases de données, forums et sites illicites, inaccessibles depuis les usuels moteurs de recherches. Sans doute trois fois plus vaste en volume que le web de surface, le *Dark web* est un cauchemar pour les États car, dans un anonymat quasi-parfait, il permet toutes les transactions criminelles sur les stupéfiants, les armes, la pédophilie, etc.

Data broker (fournisseur de données informatiques) : opaque et intrusive « industrie » de vente des données personnelles de citoyens ou consommateurs en vue d'actions de marketing.

DDoS (Distributed Denial of Service) : désormais classique, cette attaque informatique consiste à bombarder de messages non désirés, jusqu'à le submerger, un système cible, ses fonctions et connexions à Internet ; ce, grâce à des « cybermeutes » (*Botnets*) rassemblant jusqu'à des milliers d'ordinateurs « capturés » et mis en ordre de bataille par des pirates. L'attaque DDoS peut aussi servir de cheval de Troie à des intrusions plus subtiles ; ou permet de les masquer. Produit par la société de sécurité informatique NSFocus, le rapport *DDoS threat focus*, annonce avoir mondialement recensé en 2013, 245 000 attaques DDoS, soit un peu plus de 670 par jour, ou 28 par heure.

« Fullz » (« complets » en argot anglais des hackers, sans doute par analogie avec « full » ou « full house » au poker, soit un brelan et une paire). Il s'agit de reconstituer toutes

M – *International Herald Tribune*, 22/08/2013, « Facial scanning makes advances »

M – *Dark reading*, 28/01/2014, « DDoS just won't die »

M – *Dark reading*, 2/06/2014, « Global effort disrupts GOZeuS botnet, Cryptolocker, one indicted »

M – *Krebs On Security*, 10/07/2014, « Crooks seek revival of GameoverZeuS botnet »

M – *New York Times International*, 2/07/2014 (pages spéciales Russie), « Aiming to secure the cyber-future »

M – *Agence France Presse*, 6/08/2014, « Des pirates informatiques russes auraient volé plus d'un milliard de mots de passe »

M – *New York Times International*, 6/08/2014, « Hackers steal huge trove of virtual data »

M – *BBC News*, 11/08/2014, « Do quantum computers threaten global encryption systems? »