

ENTRETIEN AVEC

Renseigner les démocraties, renseigner en démocratie

Jean-Claude COUSSERAN
et Philippe HAYEZ

Loi sur le renseignement
un texte d'urgence attendu depuis 25 ans

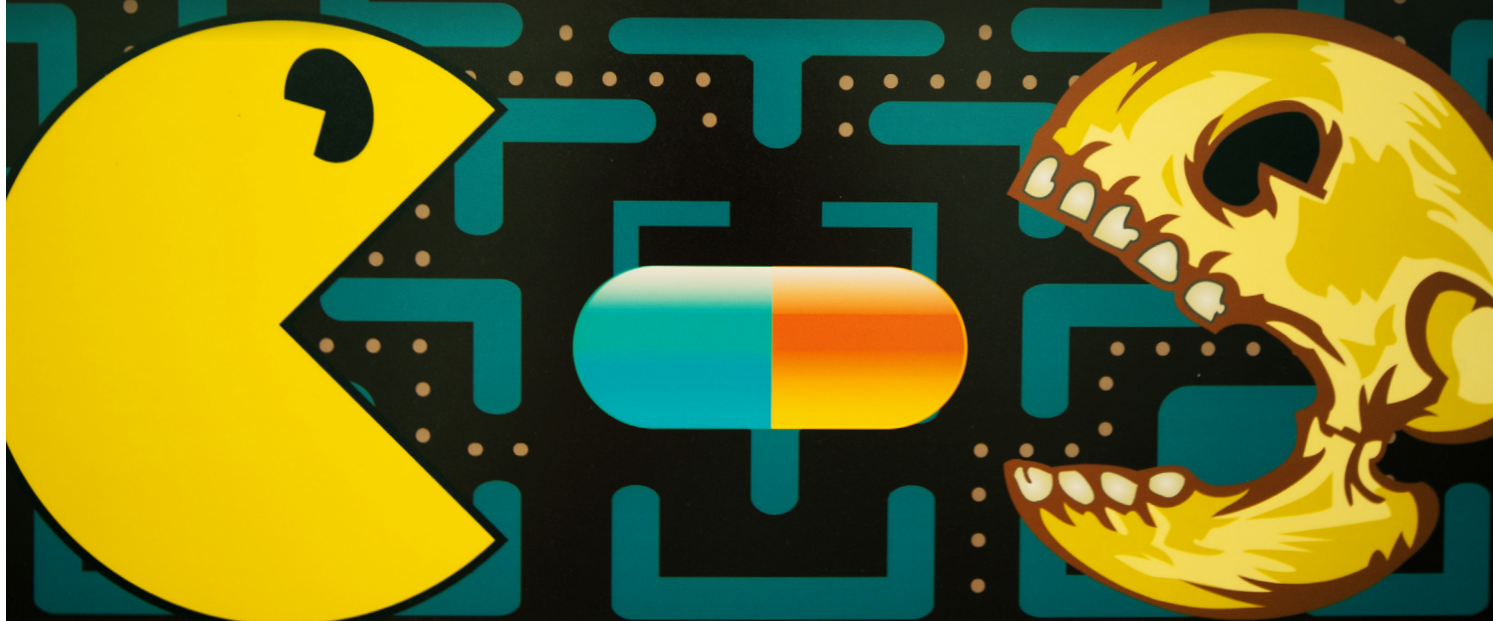
Etienne DROUARD

ENJEUX

Affronter
le cyber-crime :
la voie criminologique

EXPLORER

CRIME PHARMACEUTIQUE : UNE ÉPIDÉMIE SILENCIEUSE





Xavier RAUFER

Criminologue

Affronter le cyber-crime : La voie criminologique

En matière de cybercriminalité, nous évoluons toujours sur une *terra incognita*, ou presque. « *Hic sunt dracones* » trouvait-on prudemment écrit sur les cartes médiévales censées dépeindre le centre de l'Afrique. Or toujours plus aujourd'hui, abondent les « dragons numériques ». Face à eux, sur les terres encore infrayées du cyber-crime, la voie de l'avenir est désormais de penser, non plus en technicien, mais en criminologue. Pourquoi ?

Regardons ! Ouvrons les yeux !

Début 2015, la publicité sur Internet (25% du marché) dépasse désormais celle consacrée à la presse (24%). Aujourd'hui, les usagers de *Facebook* sur terminal mobile sont près d'1,2 milliard - plus 74% depuis 2012.

Toujours plus, l'humanité est connectée - standardisée, formatée, téléguidée. Ce, dans les pays développés et les mégapoles, et sur une planète où le stable s'effiloche au profit du mouvant. Dans cette société de la perpétuelle accélération, la griserie de la vitesse se ressent toujours plus fort.

Que de pièges ! Car derrière les féeries propagées par les titans du Net, la technologie n'est pas neutre et les algorithmes, subtilement partiels. Voilà d'ailleurs ce que nous dit sur ces fabuleuses mutations le sociologue britannique Zygmunt Bauman : « Contrairement aux corps solides, les liquides ne peuvent pas conserver leur forme lorsqu'ils sont pressés ou poussés par une force extérieure, si mineure soit-elle. Les liens entre leurs particules sont trop faibles pour résister... C'est précisément le trait le plus frappant du type de cohabitation humaine caractéristique de la « modernité liquide ».

On parle de maîtrise ? C'est de perte de contrôle qu'il s'agit. On encense le *high-tech* émancipateur ? La cyber-servitude

progressive. D'évidence, tout ceci est criminogène : fragilisation, désorganisation et perte d'attention sont une aubaine pour les filous et les fraudeurs. Tels sont les périls intrinsèques, tenant au système même. Mais existent aussi des criminels purs et durs, des cyber-prédateurs n'agissant pas par étourderie ou cynisme - mais pour le profit le plus immédiat et le plus juteux possible.

A titre d'exemple, observons l'un de ces cyber-gangs russo-ukrainien, l'un parmi bien d'autres dans l'ex-Bloc de l'Est, dépeint fin 2014 par la SSI IB-Fox it. Nommé « Carberp » du nom du « Cheval de Troie » éponyme, ce cyber-gang infiltre depuis le début 2013 les systèmes de ses cibles par le biais de mails piégés, émis par de soi-disant partenaires de confiance (Banque centrale de Russie, etc.), puis en pille les comptes bancaires. Désormais, il vise en outre les systèmes eux-mêmes, lourds et inertes, myopes - voire aveugles ; ou même les logiciels des distributeurs automatiques de billets.

Depuis sa création, « Carberp » a pillé 50 banques et dispositifs de cartes bancaires de l'Europe de l'Est, pour un butin de 25 millions de dollars. Dès l'été 2014, « Carberp » s'enhardit et assaille des commerces et banques d'Europe occidentale et des Etats-Unis. Ce, grâce à un nouveau « malicieux » du nom d' « Anunak », qui agrège une dizaine d'outils voués à voler des mots de

passé, casser des codes, piloter à distance le cyber-pillage, etc. «Carberp» pratique enfin le délit d'initié criminel, en volant et exploitant les informations sensibles des entreprises visées, afin de les exploiter ensuite sur divers marchés financiers, Bourses, etc...

Silencieux, invisibles, des grands fauves à la «Carberp» parcourent une cyber-jungle où les humains peinent toujours et encore à les affronter. Ainsi, le cybercrime a d'évidence, de beaux jours devant lui. Et face à lui, que peut la simple technique ? Pas grand chose. On l'a constaté encore récemment, quand des pirates ont ravagé tous les systèmes numériques de TV 5 Monde, sans qu'aucun des «experts» anti-piratage informatique n'y ait rien vu, ou pu.

Face à cette cyber-criminalité trop méconnue encore ; et aujourd'hui capable de frapper quand elle veut, à sa guise, la cyber-criminologie doit s'imposer.

Une nouvelle criminologie, vouée à la mobilité. Une cyber-criminologie délaissant le stable et le fixe pour les flux et les réseaux. Une cyber-criminologie du mouvement et du déplacement, nageant à son aise dans la fameuse «modernité liquide» de Z. Bauman. Une cyber-criminologie vouée à mieux comprendre, apprendre et affronter les cyber-dangers émergents - et seule capable de le faire.

Que veut, que peut la cyber-criminologie ?

Dire ce que font les criminels dans le cybermonde, tel est l'objet même de la cyber-criminologie, dont voici, les quatre thèses fondatrices :

- *Diagnostic 1* - dans l'ensemble «cyber-crime», 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.

Une infrastructure numérique mondiale agile ? Non : fragile

Dès aujourd'hui, le système global de traitement automatisé des données constitue une superstructure mondiale. Le cyberspace représente un continent nouveau, un monde neuf. Et ces nouvelles technologies de l'information et de la communication (NTIC) altèrent la façon qu'a la population de penser, de croire, de se comporter, d'apprendre.

Toute la population : celle des honnêtes gens mais aussi, des malfaiteurs. Or comme toujours quand l'homme conquiert un nouvel espace, on ne tarde pas à y constater vols, fraudes, crimes, actions de propagande, truquages et mensonges, entre autres formes de déviance aux normes sociales. Il y a bel et bien un cyber-crime, donc des cybercriminels : dès 2013, Interpol constate qu'à l'échelle mondiale, plus de 80% de la criminalité en ligne émane de sociétés criminelles transfrontières.

Ce cyber-crime est aujourd'hui le Graal pour tout malfaiteur. Jugeons-en :

- une totale dissociation du temps et de la distance offrant la capacité à commettre un crime à 10 000 kilomètres de distance (cyber-braquage),
- une jeunesse hypnotisée, facile à berner ou pirater, tant elle voit «Le monde comme un ensemble d'applications; leur propre monde comme une chaîne d'applications - voire parfois, comme une seule application étendue du berceau au tombeau»,
- des cerveaux cybercriminels, chefs de gangs ou têtes de réseaux, à l'impunité quasi garantie - aujourd'hui, seuls sont arrêtés de lointains comparses,
- des coûts limités pour des butins considérables,
- une méthodologie simple, exploitant deux fondamentaux : les faiblesses humaines (naïveté, etc.) et les vulnérabilités techniques (failles, etc.).

Enfin, dans le monde ambiant de l'Internet, rien ne concerne le crime. On y parle parfois des effets du crime (attaques, intrusions...), jamais ou presque des criminels de chair et d'os de qui ils sont ou de ce qu'ils font vraiment.

Cet oubli est dramatique. Car s'il est une évidence, c'est la nécessité de nommer d'abord ce que l'on souhaite ensuite comprendre, puis traiter. Formidable est ainsi le discret pouvoir de la nomination : « *Le nom fait faire connaissance... Nommer dévoile... Par la vertu de l'exhibition, les noms attestent leur souveraineté magistrale sur les choses* », disait Martin Heidegger.

En médecine, par exemple, ne pas nommer une maladie grave condamne le patient ; en stratégie, encore, ne pas nommer précisément une menace condamne le plus souvent l'attaqué.

Cybercrime, cyberterrorisme : les trois grandes questions

Le cybercrime est-il plus dangereux que le terrorisme ?

Récemment encore, James Comey, le patron du FBI, déclarait : « Le péril cyber-sécurité est si grave que, pour la seconde année consécutive, (...) ce péril surpasse à la fois le terrorisme, l'espionnage et, même, celui représenté par les armes de destruction massive. » Est-ce sérieux ? Comprendons le patron du FBI : il vit dans une société formatée par, et droguée à, la surenchère médiatique. Devant le gratin de la *Silicon Valley*, toute annonce en dessous de la première guerre (numérique) mondiale déclenche forcément des bâillements d'ennui.

Il n'empêche : le péril cybercriminel est réel. Aujourd'hui, le monde numérique, c'est la Banque de France, moins les coffres forts : d'ordinaire et le plus souvent, les pirates de tout poil n'ont qu'à se servir. L'an passé, un géant américain de la distribution s'est fait subtiliser quasiment toutes les données confidentielles personnelles de soixante-dix millions de cartes de paiement (en fait, toutes celles de son immense clientèle) - soit un tiers de toutes ces cartes en usage aux Etats-Unis. Récemment, on a vu le piratage de TV5 Monde : des heures durant, la capture d'un grand réseau télévisé, de ses serveurs et canaux de diffusion, de ses comptes sur les réseaux sociaux, etc. Pour la France, un « choc stratégique » aussi important dans le monde virtuel, que les tueries de janvier passé (Charlie Hebdo, Hyper-Cacher, etc.) dans le monde physique.

Après le piratage de la chaîne TV5 Monde : la France est-elle bien protégée ?

La France manque d'un organe de détection précoce des dangers et menaces. Trop souvent, nos services officiels réagissent à un drame en cours, ou déjà commis, mais n'opèrent pas - ne savent pas encore, donc ne peuvent opérer - dans le registre du préventif. Or, la génération spontanée n'existe pas plus dans le domaine stratégique

qu'en biologie. Tous les préparatifs d'un acte sanglant comme l'attaque de Charlie Hebdo (dans le monde physique) ou de TV5 Monde (dans le cybermonde) laissent forcément des traces ; ce qu'on appelle des signaux faibles ou des « ruptures d'ambiance », analogues à ce que la sagesse grecque antique appelait des « épiphanies ».

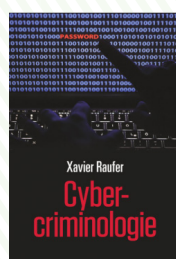
C'est cela qu'il faut savoir déceler *avant* le drame. Dans les mois précédant le 11 septembre 2001, de multiples signes avant-coureurs furent signalés aux autorités. Mais ces signes n'ont pas été compris à temps. Pour l'essentiel, on a réalisé ce qu'ils annonçaient à partir du 12 septembre, la catastrophe survenue. C'est cela qu'il faut éviter. En matière stratégique, il faut simplement permettre à la France d'appliquer dans le concret un proverbe tiré de la sagesse populaire « Mieux vaut prévenir que guérir ».

Des médias extatiques nous parlent souvent de « cyber-prédiction » : est-ce sérieux ?

Question de génération : ceux qui nous gouvernent connaissent mal le cybermonde et les périls qu'il renferme. Notamment, ils ignorent tout de l'idéologie pernicieuse de Silicon Valley, un fort toxique cocktail de scientisme (Max Planck : « seul le mesurable est réel ») et d'un hyper libéralisme (dit « libertarien ») frisant l'anarchisme pur et simple. Dans la propagande de cet anarcho-capitalisme, domine l'idée que seule l'informatique nous protégera des périls du monde. C'est affirmé avec une force inouïe : « *There Is No Alternative* » - en abrégé TINA. Ainsi - dit la Silicon Valley - l'avenir est dans le prédictif informatisé.

Or, c'est bien sûr absurde - car la véritable incertitude n'est pas plus modélisable aujourd'hui que du temps d'Aristote - sinon, tout le monde gagnerait à la loterie ou au tiercé. Ce sont ces fariboles, proches de l'escroquerie intellectuelle, que les géants de la Silicon Valley vendent aux gogos. Tout cela, je l'expose en détails dans mon livre « Cyber-criminologie ». Lisez-le, vous serez édifiés ! ■

POUR ALLER PLUS LOIN :



CYBER-CRIMINOLOGIE,
Xavier Raufer, CNRS-Éditions, 2015