# LES CRIMES DU FUTUR

Marc Goodman. Nouveau Monde Éditions, 2017, 790 p.

*Paloma Diez, Marion Délécrin, Ludivine Mary, Augustin Noukafou, Auriane Peinaud*


Marc Goodman a travaillé au sein de la police de Los Angeles, où il était enquêteur, ainsi que pour le FBI (les services secrets américains), les Nations Unies et Interpol. Il était au plus proche des questions de la cybercriminalité. Aujourd'hui, il est consultant international sur le cybercrime auprès de plusieurs entreprises de la Silicon Valley. Il est également à la tête du *Future Crime Institute* qu'il a créé. Goodman estime que "*Plus vous produisez et stockez de données, et plus le crime est heureux d'en consommer*".

Son livre *Les Crimes du Futur* est un best-seller aux Etats-Unis. Marc Goodman y compile une multitude d'exemples de cybercrimes, allant du fait-divers au conflit géopolitique.

Dans cet ouvrage, divisé en trois parties, il tente de nous mettre en garde contre les différentes catégories de cybercrimes potentielles. Goodman souhaite réellement que nous ne regardions plus nos écrans de la même manière. Mais surtout, il considère que nous pouvons anticiper et prévenir dès aujourd'hui les crimes de demain. C'est pourquoi il donne également, à la fin de son livre, ses préconisations pour un monde numérique plus sûr.

## LES CYBERCRIMES ACTUELS

Dans son ouvrage *Les Crimes du Futur*, Goodman raconte, histoire après histoire, **comment la technologie a été utilisée à des fins illégales**. Tout semble possible dans le monde du cybercrime : d'un gang vietnamien qui achète les données personnelles des

deux tiers des Américains, à une attaque commanditée par l'État chinois dans laquelle des avions sont volés à l'armée américaine.

Pour Goodman, la plupart des gens font **trop confiance aux informations présentées sur leurs écrans**. En Californie, 450 condamnés ont été libérés de prison après une erreur du système, tandis qu'au Royaume-Uni, des ordinateurs de la police britannique ont, à tort, qualifié 20 000 innocents de criminels. Pour l'auteur, de nombreux objets et même des parties entières de notre vie pourraient être manipulées à cause de notre confiance aveugle dans les écrans.

Goodman estime que les **cybercriminels prolifèrent.** L'auteur décrit le cas d'Innovative Marketing, une petite start-up ukrainienne qui prétendait commercialiser des logiciels anti-virus sous le nom de Malware Destructor et System Defender. En peu de temps, la société a obtenu des clients dans plus de 60 pays et a embauché plus de 600 employés. Cette entreprise, en réalité, piégeait ses clients potentiels en leur faisant croire qu'ils étaient infectés par un virus. Pour l'éliminer, Innovative Marketing proposait sa solution anti-virus qui était, en fait, un logiciel espion. En téléchargeant une version de Malware Destructor, le programme antivirus légitime des personnes piégées était supprimé en silence. Puis **leurs numéros de cartes de crédit et autres informations critiques, stockées sur leur disque dur, étaient collectées et vendues au plus offrant par Innovative Marketing.**

La volonté de Goodman est **de rendre publiques les cyberattaques afin qu'il soit plus facile de développer des défenses communes contre elles.** Son objectif est que les entreprises signalent les cyberattaques dont elles sont victimes. En effet, de nombreux dirigeants refusent de le faire, par crainte des conséquences délétères sur leurs actions et leur réputation. Dans son ouvrage, Goodman affirme que **« ce silence est au cœur même de nos problèmes de cybersécurité».** En effet, les victimes ne sont pas informées des attaques qu'elles subissent, les pirates restent impunis et les compétences en matière de lutte contre le cybercrime ne sont pas développées.

Dans ce sens, Marc Goodman démontre que les criminels ont accès à nos données. A titre d'illustration, en Inde, lors des attaques terroristes de Bombay, Internet a permis aux criminels d'identifier les otages et de décider de leur sort. Un autre aspect du piratage de données est le développement massif de **l'usurpation d'identité.** En 2012, aux Etats-Unis, cette catégorie de crime représentait 21 milliards de dollars extorqués aux dépens de 13,1 millions de victimes. Les enfants et les personnes âgées sont les plus touchés par ces attaques car ils sont les plus vulnérables. **Tout ce qu'une personne publie sur les réseaux sociaux peut être utilisé contre elle.** Mais n'avoir aucune présence sur les réseaux sociaux ne constitue pas, pour autant, une protection fiable.

Si les ordinateurs sont vulnérables, **les smartphones le sont encore plus.** Avec leur localisation toujours activée, leurs caméras et leurs micros pouvant être allumés à distance, les informations des téléphones peuvent être utilisées à des fins criminelles. Par exemple, dès leur entrée dans les refuges, les femmes battues doivent retirer les batteries de leurs téléphones, afin d'éviter que leurs ex-conjoints les retrouvent. **De plus, la vulnérabilité des smartphones procède de leurs systèmes d'exploitation, notamment Android** qui est accessible à tous et faiblement sécurisé. Cependant, la porte d'entrée des virus est, le plus souvent, **les applications et les paiements par téléphone.**

Les téléphones et leurs écrans peuvent tromper notre confiance. Les pirates peuvent y faire apparaître un faux nom d'appel et changer la voix à l'autre bout du fil. Cette pratique s'appelle le ***rootktit.*** Ce type d'usurpation **est à la portée de tous et permet d'avoir accès à des renseignements précieux**, en se faisant passer pour une banque ou un gouvernement fédéral. Si les écrans des téléphones sont piratables, c'est également le cas des écrans de GPS, des écrans de télévision ou encore plus grave, ceux des scanners dans les aéroports. Aujourd'hui, **763 vulnérabilités ont été recensées dans les aéroports nord-américains.** Cela pose la question de la confiance, notamment celle que nous plaçons dans les écrans.

## LES CYBERCRIMES DU FUTUR

**Crime Inc.** est l'appellation, donnée par Goodman, pour désigner le cybercrime organisé. Entre trafic de stupéfiants, vol de propriétés intellectuelles, traite d'êtres humains, contrefaçon, pédopornographie ou vol d'identités, **la cybercriminalité génèrerait quelque 2 000 milliards de dollars par an et représenterait 15 à 20% du PIB mondial.** Crime Inc. correspond au plus grand réseau illicite du monde, il ne connaît **aucune frontière** et tous les cybercriminels y restent anonymes.

Selon Goodman, nous entrons dans l'ère de **l'Internet des Objets (IoT).** Chaque domaine de l'activité humaine va être affecté et tous nos objets seront connectés et pourront être contrôlés à distance. Avec les ordinateurs miniatures qui seront placés dans nos objets**, nos données pourront être piratées et collectées.** Aujourd'hui déjà, le choix d'un mauvais chargeur de smartphone peut modifier notre micrologiciel et pirater nos téléphones. Des appareils apparemment fiables et censés nous protéger (comme par exemple un système d'alarme) peuvent se retrouver sous l'emprise d'autrui et **être utilisés contre nous de façons surprenantes et parfois mortelles**. Si un ordinateur contrôle notre voiture, il peut être contrôlé à son tour par un assaillant. Pour Goodman ***"Nous avons câblé le monde mais échoué à le sécuriser"***. Or, **nous commençons à connecter le corps humain lui-même à internet.**

**L'être-humain peut lui-même faire l'objet de cyberattaques**. Ce n'est pas seulement un fantasme hollywoodien, selon Marc Goodman. Les dispositifs médicaux implantables,

appelés IMD, communiquent avec le monde extérieur par le biais de radiofréquences. Environ 300 000 patients, aux États-Unis, reçoivent des IMD sans fil chaque année. Les défibrillateurs implantables permettent aux médecins de surveiller leurs patients à distance en temps réel. Mais encore aujourd'hui, **de nombreux dispositifs médicaux sont vendus sans aucun mécanisme de sécurité.** En cas d'attaque il est très difficile de déterminer la cause réelle du décès. Le meutre en ligne via IMD sera bientôt une réalité.

D'autre part, les nouveaux systèmes d'identification se basent désormais sur **nos données biométriques, des marqueurs d'identification permanents** qui une fois dans les mains des hackers ne seront plus jamais en notre contrôle (ex : touchID d'Apple). Avec la reconnaissance faciale, **plus aucun individu ne sera anonyme dans une foule.** Mais le risque d'erreur d'identification n'est pas négligeable.

Bientôt, la **réalité augmentée connectera définitivement les mondes en ligne et offline**. Beaucoup d'utilisateurs de jeux perçoivent déjà leurs "secondes vies" comme des "premières vies", préférant s'occuper de leurs avatars que de leurs proches du monde réel. Un couple sud-coréen s'est ainsi occupé d'une petite fille virtuelle de manière obsessionnelle, au péril de leur véritable nourrisson de trois mois qui n'a pas survécu au manque de nourriture.

Selon Marc Goodman, nous entrons dans **l'ère du soulèvement des machines,** et il parle même des robots comme étant « *la dernière invention de l'Homme* ». Qu'ils soient utilisés dans l'industrie, dans l'armement, ou tout simplement dans les foyers, **les robots sont entrés dans notre espace tridimensionnel et sont dotés de plus en plus de fonctionnalités.** L'auteur évoque les **drones.** Ils peuvent être utilisés comme **de véritables armes de guerre** et constituer un arsenal militaire puissant. Pour illustrer des dérives que cela pourrait entraîner, l'auteur cite l'exemple de ce groupe d'étudiants d'Austin qui a réussi à pirater les drones de la flotte du Ministère de la Sécurité Intérieure des États-Unis censés protéger les frontières. Il en a été de même avec le gouvernement iranien qui a usurpé les données GPS de drones américains.

L'auteur prend un autre ton lorsqu'il s'emploie à parler de **l'intelligence artificielle.** Il s'intéresse aux **progrès positifs de ces nouvelles technologies, surtout dans le domaine de la médecine et des biotechnologies,** grâce auxquelles il est désormais possible de créer des tissus humains, des organes etc. Des progrès saisissants ont été **réalisés au niveau de l'interface cerveau-ordinateur**, soit des neuroprothèses. Un individu pourrait aujourd'hui contrôler un bras robotisé uniquement par la pensée grâce à un implant neuronal ou un casque électroencéphalogramme. Comme tous les objets connectés, celui-ci pourrait également être piraté et faire l'objet d'une utilisation malveillante.

Mais Marc Goodman n'a de cesse de **nous mettre en garde.** Ainsi, lorsqu'il définit l'impression artificielle d'ADN, il nous répète que tout est piratable, même notre ADN. **De**

**nouveaux modèles de hackers pourraient alors voir le jour, ils seront bio-profanateurs, harceleurs ADN ou bio-terroristes.** Toutes les cellules humaines et autres données biologiques pourront être hackées et utilisées de manière malveillante**. Toutes les traces d'ADN que nous laissons chaque minute derrière nous pourront être vendues, dupliquées et séquencées à volonté.**

## LES PRECONISATIONS

Marc Goodman s'est penché dans son ouvrage sur **la prévention des crimes.** L'auteur invite les utilisateurs à interpeller les **ingénieurs pour qu'ils élaborent des codes et logiciels plus sécurisés.** Il propose aussi de rémunérer les hackeurs qui auraient décelé des failles**.** Il estime que cela pourrait minimiser les dommages et empêcher les hackers de livrer ces secrets à des organisations mafieuses.

De nos jours**, plus de 90% de mots de passe habituels peuvent être hackés et livrés à des organisations criminelles.** Face à ce constat, Marc Goodman conseille dans son livre, l'installation de **la sécurité biométrique sur les téléphones**. Pour lui, la définition de longs mots de passe pour ses multiples comptes permet à un utilisateur de bien se protéger. Le livre cite aussi d'autres moyens pour se constituer de bons mots de passes, notamment **« l'identification à deux facteurs »** que proposent d'ores et déjà Google, Microsoft, Paypal et bien d'autres. Enfin, le **cryptage** est évoqué dans *Les Crimes du futur* comme une **couche supplémentaire de sécurité et de protection des données personelles.**

Pour éviter des piratages potentiels, il est préférable de **choisir des sites officiels de téléchargement comme l'App Store.** Le livre conseille de s'assurer de la provenance des mails reçus avant de les ouvrir. Marc Goodman recommande la **désactivation du « démarrage automatique » d'un ordinateur pour s'assurer qu'aucun virus ne s'exécute automatiquement et infecte l'appareil.** Il conseille aussi la navigation en « mode furtif ». Cela permet de bloquer les connexions entrantes indésirables. Et lorsque **l'ordinateur n'est pas utilisé Marc Goodman estime qu'il devrait être éteint.** En effet, cela permet l'exécution des mises à jour lors du démarrage. De plus, l'ordinateur n'est pas accessible aux pirates lorsqu'il est éteint.

Dans son livre Marc Goodman insiste sur ce qu'il appelle la **« cyberhygiène ».** Il s'agit pour tout utilisateur de **protéger ses ordinateurs, ses téléphones, ses gadgets digitaux pour éviter de s'exposer et d'exposer les autres à d'éventuelles attaques.** Grâce à l'installation d'une liste blanche d'applications les systèmes d'exploitation peuvent être protégés et les fichiers exécutables inconnus sont bloqués. En appui, Marc Goodman propose **la création d'une organisation mondiale de la cybersanté.** Selon lui, cela pourrait permettre aux Etats de contrer la propagation de potentielles menaces technologiques. Cette organisation fournirait aux populations des méthodes de

cyberhygiène, détecterait les apparitions de malicielles dans le cyberespace, utiliserait des méthodologies de santé publique pour étudier la propagation des préjudices numériques.

## AVIS ET MISE EN PERSPECTIVE

À la lecture de cet ouvrage, nous avons eu la sensation de découvrir un **monde parallèle dont nous ignorions presque tout et qui évoluerait trop vite.** L'ambition de Marc Goodman est d'identifier les risques relatifs à la technologie. Pour lui, l'ambivalence technologique, qui présente des côtés positifs et négatifs, pourrait **pencher définitivement du côté obscur.**

Son œuvre contient énormément de données chiffrées, mais également beaucoup d'exemples qui illustrent le tout et rendent **le texte accessible à un large public.** Le livre peut sembler **répétitif** mais cela s'explique par le souci pédagogique de l'auteur.

D'autre part, nous lui avons trouvé un côté **alarmiste.** En effet le texte est teinté de la culture nord-américaine, et l'auteur adopte dans ses exemples **un vocabulaire familier et souvent hyperbolique, et s'appuie sur la force de l'exemple pour légitimer son propos.** Toutefois, cela rend l'ouvrage moins lisse, moins neutre, et peut-être plus facile à s'approprier qu'un texte purement scientifique.