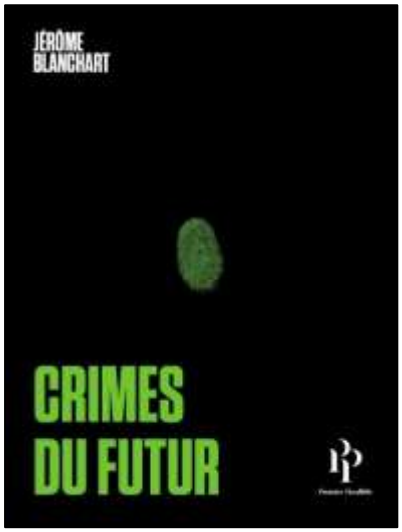

Crimes du futur

Jérôme Blanchard

Premier parallèle, 2016

Marion Cordier, Sasha Rossignol, Quentin Faure, Marie Jacachoury, Nikita Iakimov

Présentation du contexte

Jérôme Blanchart est un journaliste scientifique de 40 ans, rédacteur en chef adjoint à Sciences et Vie Junior et biologiste de formation. Dans le cadre de cette activité, il observe les mutations technologiques depuis plusieurs années. Comme dans ses précédents ouvrages, la structure de Crimes du Futur s'appuie sur des faits divers.

Dans notre société hyper-connectée, **la dépendance aux technologies** ainsi que les possibilités qu'elles proposent sont connues. Cependant, cette connaissance superficielle ne permet pas de cerner les dangers qui y sont associés.

Dans cette optique, Jérôme Blanchart nous présente un état des lieux de plusieurs thématiques liées aux technologies.

Ce livre s'inscrit dans une **démarche d'information du grand public**. Il en ressort un livre anxiogène mais néanmoins toujours ancré dans le réel, qui laisse entrevoir les possibilités quasi-infinies des **dérives des outils technologiques**.

Idées principales

Les risques liés au partage de données personnelles

« Contrairement à un numéro de carte bancaire, les datas personnelles ne se périment pas. »

« Toutes sortes de données sont susceptibles de rapporter de l'argent. »

Le partage des données personnelles implique une redéfinition de l'identité de chacun. La distinction entre le principe de vie privée et vie publique est remis en cause.

Dans le cadre des risques liés au numérique, les humains sont considérés, par l'auteur, comme étant les maillons faibles. Ce sont les victimes de ces partages massifs et inconscients des données personnelles.

Tous sont donc impactés par ces dérives mais ils sont malgré tout les acteurs responsables de leur propre malheur. En utilisant les réseaux sociaux tels que Twitter, Facebook et Instagram, chacun accepte de divulguer ses données personnelles.

Ce partage est devenu un geste banal, nous partageons sans cesse des photographies de notre vie privée, des informations sur nos activités et nos habitudes. Nous publions ces informations sans penser un seul instant que ce partage est risqué ou dangereux. On s'expose, dès lors, à des conséquences insoupçonnables. En effet, ces données personnelles peuvent être divulguées et utilisées à mauvais escient.

L'histoire de Nona Belomesoff

Nona avait 18 ans lorsqu'elle s'est faite enlever et tuer. Elle clamait sur Facebook son amour pour les animaux et sa ferveur à défendre la cause animale.

Christopher Dannevig a.k.a James Green, inscrit sur ce réseau social, lui tendit un piège en se faisant passer pour un agent de recrutement travaillant pour la sauvegarde des animaux. Après plusieurs conversations il lui proposa un poste. C'est donc tout naturellement, qu'un jour, elle monta dans la voiture d'un parfait inconnu pour décrocher le job de ses rêves et qu'elle trouva la mort.

Le casse du siècle

En 2013, des hackers de l'Europe de l'Est ont infiltré des réseaux de banque en Inde et aux Emirats arabes unis.

Ils ont réussi à voler des milliers de numéros de cartes de crédit prépayées. Pour ne pas se faire repérer par les banques, l'opération devaient être minutée. Ils ont donc été aidés par des artisans locaux dans 27 pays qui leur imprimaient de nouvelles cartes.

Grâce à ces données bancaires, ils ont pu pirater les serveurs afin de débloquer les limites de retrait et ainsi retirer des sommes illimitées dans des distributeurs de tous les continents.

Les ransomwares

Les premières attaques de « prise d'otage contre rançon » ont commencé en 2005 avec des cybercriminels russes. Le principe des ransomwares (ransom-softwares) est d'encrypter une grande quantité de fichiers présents sur une machine en les rendant illisibles pour l'utilisateur contre une rançon. Il existe plusieurs types de rançons : les SMS ou numéros surtaxés et la crypto-monnaie (le bitcoin).Les risques liés aux objets connectés

« Notre vie privée sera la première victime de cet internet des objets espions : imaginez un instant l'indiscrétion d'une télévision dotée d'une caméra et d'un micro branché 24 heures sur 24. Effrayant, non ? »

Au-delà du simple partage d'information que nous effectuons, il existe d'autres risques concernant notre vie privée que nous ne pouvons pas contrôler.

Les objets connectés se développent partout autour de nous. Nous vivons dans une société dite « hyper connectée », il est donc **difficile de contrôler les usages de ces objets** en tout genre. Chacun voit en eux, leurs utilités et leurs usages qui simplifient de nombreuses activités au quotidien. Il est donc impossible de différencier les bonnes utilisations des mauvaises.

Le moteur de recherche Shodan

Shodan est un moteur de recherche crée en 2009 par John Matherly. Il est spécialisé dans la recherche d'objets connectés à Internet. Comme tout système numérique, il peut être détourné à des fins douteuses. En effet, Shodan est utilisé par des pirates pour trouver des failles dans les systèmes informatiques, pour trouver des dispositifs mal sécurisés et d'en prendre le contrôle.

C'est le cas des « Baby Cams ». Certaines personnes mal intentionnées se sont amusées à prendre le contrôle de ces caméras de surveillance pour enfants, connectées à Internet et dotées d'un haut-parleur et d'un micro.

Les perturbateurs de ces machines se sont, entre autres, amusés à réveiller les enfants, et par conséquent, leurs parents, en pleine nuit avec des bruits inquiétants.

Les drones

Les drones sont les nouveaux objets connectés tendances dont l'usage et l'achat se sont généralisés au sein de la société. Or, ces gadgets désormais accessibles par tous, peuvent aussi être utilisés à des fins malveillantes. Leurs fonctions et utilisations premières ont été détournés. Ils ont notamment servi à transporter de la drogue du Mexique vers les Etats-Unis, ou à faire passer des objets à des prisonniers. On recense aussi plusieurs cas de voyeurisme.

Les risques liés à un accès généralisé aux informations

« Dans un avenir dominé par les « cybermafias », aucune action efficace n'est parvenue à enrayer l'essor du cybercrime »

Avec l'ère du numérique, Internet est considéré comme une **porte d'entrée à la connaissance et au savoir**. Malgré tout, il est également le lieu de toutes les dérives.

L'usage intensif d'Internet peut alors entraîner de graves conséquences. On assiste à une **démocratisation des procédés jusqu'alors réservés aux criminels**.

Le darknet

Le darknet est un réseau superposé qui utilise des protocoles permettant l'anonymat de ses utilisateurs. Ils peuvent alors communiquer sans craindre les entreprises ou le gouvernement. Le darknet est donc souvent associé aux activités illégales.

Sur ce réseau, on peut trouver des sites comme le SilkRoad créé par Ross Ulbricht. Qualifié d'« ebay du crime et du vice », cette plateforme virtuelle propose d'acheter des armes, des papiers volés, des cartes bancaires et des vidéos pédophiles, le tout dans l'anonymat le plus total. Ce réseau n'a pas de limite, chacun peut acheter tout ce dont il a envie et satisfaire la moindre de ses envies, qu'elles soient légales ou non.

Un nouveau site remplace désormais le Silkroad, le DarkMarket, créé par Amir Taaki. Il est plus puissant et plus difficile à enrayer. Il propose tout ce dont un criminel professionnel ou novice a besoin, on peut, par exemple, faire appel à des tueurs à gages.

Les jeux vidéos

Contre toute attente, les jeux vidéo peuvent aussi permettre un accès généralisé aux informations. D'importantes sommes d'argents circulent au sein de ces jeux vidéo.

On assiste donc à une nouvelle forme d'économie souterraine appelée "gold farmers". Cette économie souterraine est la cause de nouvelles formes de cambriolages. En ligne, les biens virtuels des joueurs peuvent être dérobés lorsqu'on pirate leurs codes d'accès. Ces biens sont ensuite échangés contre de vraies sommes d'argent. Rien ne peut être entrepris contre les malfaiteurs en raison du vide juridique.

Ces cambriolages peuvent aller plus loin et se produire dans la vie réelle. Le gang "La Firma" a déjà kidnappé un jeune joueur pour obtenir ses codes et récupérer l'argent.

Le virtuel est devenu le nouveau lieu de prédilection des criminels pour le blanchiment d'argent au travers des jeux vidéo.

Apprendre à créer une bombe sur Youtube

« Les groupes extrémistes emploient Internet pour leur propagande et leur recrutement »

Les algorithmes utilisés par les réseaux sociaux jouent un rôle « inconscient » dans ce recrutement. En nous proposant une « expérience sur-mesure » ou qui correspond à nos attentes, les algorithmes des réseaux sociaux mettent en lien des sympathisants de Daesh, des radicaux, avec n'importe quel individu.

Le site Web Canal-U propose des formations en ligne. C'est une véritable mine d'or. Toutefois, les terroristes peuvent utiliser cette interface en ligne pour poster leurs propres vidéos. Sur un site destiné au savoir et à la connaissance, on peut ainsi trouver, parmi des vidéos de chercheurs de l'Université d'Harvard, des vidéos pour apprendre à *« fabriquer une bombe dans la cuisine de maman »*.

Le réseau peut donc être utilisé à des fins graves et dangereuses par n'importe quel individu mal intentionné. Chacun est alors susceptible d'en subir les conséquences.

Les risques liés aux innovations biologiques et médicales

« S'implanter un objet technologique dans le corps, capable d'agir sur nos fonctions vitales, n'est pas seulement un progrès, c'est aussi une porte ouverte à de nouvelles menaces. »

Le monde médical a profité des avancées scientifiques pour améliorer ses usages. D'après l'auteur, le marché des objets connectés destiné au milieu médical connaît actuellement une croissance qui s'explique par un réel engouement pour des services de santé numériques accessibles en tout temps et en tous lieux.

Ce lien établi entre le monde médical et le monde du numérique nous ouvre les yeux sur le progrès scientifique et les menaces et les risques qu'il pourrait engendrer dans un futur proche.

Les nouveaux virus

Les dispositifs médicaux implantés dans le corps d'un patient peuvent désormais communiquer avec le médecin via la Wi-Fi et les SMS. Mais serait-il possible que ce progrès soit à la portée des hackers par exemple ? Que se passe-t-il s'ils peuvent contrôler ces dispositifs et donc décider de programmer la mort d'un individu ?

Le progrès médical peut donc être un danger s'il tombe lui aussi entre de mauvaises mains.

La balle magique

Et si les dégâts causés par la chimiothérapie pouvaient être améliorés ?

Élaborée chez Oncos Therapeutics en Finlande, cette balle magique peut être introduite dans l'ADN d'une seule cellule tumorale. Ce "bon virus" se propage et explose en tuant uniquement les cellules touchées par le cancer.

Mais quelles sont les conséquences si cette balle magique est détournée pour tuer uniquement les bonnes cellules du corps humain ?

L'imprimante 3D

Après avoir découvert la possibilité de fabriquer des armes grâce aux imprimantes 3D, le professeur chimiste Lee Cronin de l'université de Glasgow nous informe que le plastique n'est pas le seul matériau à pouvoir être assemblé au sein de l'imprimante 3D. Il peut s'agir de n'importe quel type de molécule organique pour ainsi pouvoir fabriquer, par exemple, de la drogue chez soi.

Chacun d'entre nous, en achetant une simple imprimante 3D, pourrait devenir un créateur ou un dealer de drogues. Chacun peut donc devenir le nouveau Walter White de la série Breaking Bad !

Avis et mise en perspective

« Notre analphabétisme technologique nous pousse à ignorer les menaces croissantes qui pèsent sur nos vies connectées. »

Ce livre permet de s'interroger sur notre avenir, et de **remettre en question** toutes les technologies qui nous entourent. Le but est de faire **prendre conscience des risques technologiques** encore inconnus pour beaucoup d'entre nous. En effet, ces menaces sont difficiles à enrayer à l'échelle humaine car on ne connaît pas les rouages du numérique. Il donne ainsi l'occasion à chacun de remettre en question ses usages concernant la publication et la diffusion de ses données personnelles.

Les exemples de l'auteur nous permettent **d'ouvrir les yeux sur la société qui nous entoure** et sur nos usages. C'est peut-être une manière de nous faire réfléchir à la façon dont les générations futures seront confrontées à ces risques et dangers, et donc de mettre en place une éducation préventive.

A la lecture de ce livre, nous l'avons trouvé globalement **anxiogène et pessimiste**. Jérôme Blanchart s'interroge sur le futur visage des criminels et des terroristes de demain. La société que nous sommes en train de construire est marquée par une forte floraison technologique qui laisse la possibilité à n'importe qui d'accomplir le crime de son choix.

En somme, ce livre se parcourt comme un roman policier qui nous fait frissonner en nous livrant un aperçu des crimes et des dangers de demain.