Blaise Mao Thomas Saintourens

CYBER FRAGILES

ENQUÊTE SUR LES DANGERS DE NOS VIES CONNECTÉES

Tallandier

CYBER FRAGILES

Des mêmes auteurs

Blaise Mao
Les Jeux vidéo, 10/18, 2013.

Thomas Saintourens
Quand j'étais Superman, avec Raphaël Poulain, Robert Laffont, 2011.
Le Maestro, Stock, 2012.

Blaise Mao
Thomas Saintourens

CYBER FRAGILES

Enquête sur les dangers de nos vies connectées

TALLANDIER

2 rue Rotrou – 75006 Paris
www.tallandier.com

I know the dream that you're dreaming of
I know the word that you long to hear
I know your deepest, secret fear.

The Doors, *The Spy*, 1970.

Avant-propos

Jamais le préfixe *cyber* n'avait autant fait les gros titres que ces derniers mois. *Cyberattaques*, d'abord, pour scander les intrusions et destructions d'informations subies par des entreprises ou administrations. Chaque jour, en 2015, pas moins de 177 300 offensives estampillées « cyber » ont été recensées à travers le monde[1]. *Cybercrime*, *cyberintrusions*, *cyberterrorisme*, *cyberrisque* ou *cyberharcèlement* sont des termes qui fleurissent dans les articles, les communications officielles et les textes de loi. Lorsque les intérêts diplomatiques entrent en jeu, avec des espions impliqués derrière l'écran, c'est la *cyberguerre* qui est annoncée, avec force trompettes et cris d'orfraie. Signe des temps, le texte du projet de loi budgétaire américain « Omnibus », discuté en décembre 2015, ne contenait pas moins de quatre cent treize occurrences du préfixe *cyber*, contre seulement une dizaine dans les textes précédents, a compté le magazine en ligne *The Verge*, dans un article datant du 16 décembre 2015 titré avec ironie : « The Cyberbudget of the Cyberunited Cyberstates of Cyberamerica. »

1. D'après l'organisme Internet Live Stats.

De vol de données en défiguration de site Web, d'écran noir en mails piégés, le cyber s'immisce aussi dans la pop-culture. Le mercredi 13 janvier 2016, *Les Experts : Cyber*, le *spin-off* d'une série américaine à succès, réunissait près de 5 millions de téléspectateurs sur TF1, en *prime time*. Deux jours plus tôt, *Mr. Robot*, contant les aventures d'un hacker schizophrène (gentil le jour, dangereux la nuit), remportait à Los Angeles le Golden Globe de la meilleure série dramatique. Difficile, pourtant, d'incarner avec réalisme les conflits du cyberespace. Souvent, ils sont caricaturés à l'extrême, à grand renfort de masques d'Anonymous, d'écrans grouillant de 0 et de 1 comme dans le film *Matrix* et de *geeks* encapuchonnés forcément vêtus de noir. La réalité, mouvante et sans frontières, est plus complexe – et souvent plus ingénieuse – que les scénarios de fiction.

Journalistes à *Usbek & Rica*, le magazine qui explore le futur, nous avons l'habitude d'interroger l'impact de la technologie sur nos vies, de chercher à comprendre si telle ou telle innovation est nécessairement synonyme de progrès. À force de couvrir ces sujets, nous avons eu envie d'enquêter pour voir ce qui se cache derrière ce terme nébuleux, *cyberespace*. Explorer l'envers du décor. Ne pas s'arrêter aux caricatures ni aux slogans anxiogènes. Découvrir les différentes réalités que recouvrent ce mot à la mode et ces récits prompts à entretenir la paranoïa d'une fin du monde imminente, déclenchée par quelques clics de souris. Comprendre l'origine et l'impact des attaques invisibles mais spectaculaires qui se multiplient, et dont chacun de nous peut, un jour ou l'autre, être la cible. Car la vie *smart* a bien deux faces. Côté pile, la technologie rend notre quotidien plus confortable ; côté face, elle dévoile sa part d'ombre avec, en ligne de mire, la mainmise sur nos don-

nées personnelles – qu'elles soient bancaires, médicales, ou simplement liées à nos préférences, nos recherches et nos communications en ligne.

Quelle est l'étendue exacte des menaces pesant sur nos vies connectées ? Sommes-nous tous concernés ? Quelles sont les cibles favorites des pirates et leurs différentes techniques d'abordage ? Existe-t-il des codes diplomatiques dans le cyberespace ? Comment nous rendre moins vulnérables, comment reprendre la main sur nos vies connectées ? Pour répondre à ces interrogations, nous sommes allés à la rencontre des protagonistes de la cybersécurité. Une nouvelle forme d'élite connectée rassemblant des éditeurs de solutions de sécurité (souvent qualifiés de « marchands de peur »), des hacktivistes à la pointe du combat pour la liberté sur le Net, des responsables de la sécurité nationale et des ingénieurs informatiques. Malgré leurs divergences idéologiques et sociologiques, ces différents acteurs répètent tous à loisir l'adage suivant : « Plus on est connecté et plus on est vulnérable. » Un mantra en forme d'avertissement. Un appel à ce que chacun saisisse enfin la réalité des implications d'une vie quotidienne sous perfusion technologique.

L'enjeu n'est donc pas seulement technique. Il est sociétal. Politique, aussi, et nous concerne tous. C'est ce qui nous intéresse ici. Nous avons écrit ce livre pour les usagers, les citoyens connectés. Le défi : dépasser le jargon technique, prendre de la hauteur sur les flots d'informations qui se succèdent et se chevauchent pour comprendre les enjeux profonds de la sécurité – et de nos libertés – en ligne. Des enjeux qui impactent nos vies quotidiennes autant que les systèmes économiques et politiques dans leur ensemble. Il s'agit d'essayer de tordre le cou aux idées reçues et aux

arguments marketing, afin de comprendre la réalité des menaces donnant corps à ce préfixe *cyber*, qui dicte toujours plus les usages de notre quotidien.

Ne pas fermer les yeux pour laisser opérer la magie technologique et les promesses d'un monde connecté, si rapide, si confortable. Les ouvrir, au contraire, et observer les arguments des hackers – qu'ils soient pirates, corsaires ou les deux à la fois. Plonger dans la chronique vertigineuse des crimes et délits numériques, des applis pour smartphones aux automates industriels faisant tourner les usines, des ordinateurs de bureau aux voitures connectées. Pour comprendre enfin combien notre mode de vie est désormais à la merci des fragilités d'une surconnexion non maîtrisée.

Introduction

Il était une fois… les hackers

Au commencement était un club d'amateurs de trains électriques. Le Tech Model Railroad Club (TMRC) avait trouvé refuge dans une salle du prestigieux MIT de Boston, en 1959. Ce petit groupe de jeunes gens passionnés par la technique passait son temps libre à démonter et remonter ses joujoux, tout en louchant sur les derniers supercalculateurs (IBM 704, puis TX-0, à plusieurs millions de dollars l'unité) utilisés par des confrères universitaires dûment accrédités dans les salles voisines. Ces ordinateurs géants avaient la possibilité d'être trafiqués, améliorés, reprogrammés afin d'être utilisés, par exemple, pour améliorer les systèmes de contrôle du trafic de leurs petits trains. Les bidouilleurs du TMRC devinrent, par leurs prouesses, les premiers « hackers » – de l'anglais *to hack*, « mettre en pièces ». Et quand quelques insectes (*bugs*) venaient se loger sous le capot du calculateur géant (les cafards aussi siégeaient en nombre au MIT), une opération de « débuggage » (souvent à la pince à épiler) était nécessaire pour retirer les indélicats locataires et remettre les systèmes en ordre de marche.

Bientôt, les apprentis chefs de gare font des émules dans le corps académique. Surtout, les travaux sur l'intelligence

artificielle et les réseaux informatiques sont le prolongement logique – et officiel – de leurs expérimentations nocturnes. C'est en mettant littéralement les mains dans la machine que les équipes de chercheurs, à l'université ou à domicile, sont parvenues, de bug en bug, de faille en faille, à améliorer la technique, et à façonner les premiers « ordinateurs personnels » d'une révolution numérique dont les hackers seront les pionniers. De leurs expériences naîtra aussi *Spacewar !* – le premier jeu vidéo, en 1962. Et les prémices de l'Internet, avec le réseau ARPAnet, servant en premier lieu à convoyer des informations entre des universités américaines (4 en 1969, 111 en 1977), avant de revêtir un enjeu stratégique avec un *military network* lancé en 1980.

Pendant ce temps-là, à l'autre bout de l'Amérique, on ne trouve pas des ordinateurs à tous les coins de rue, mais bien des cabines téléphoniques. Pas besoin d'arborer la jaquette du MIT ou de Harvard pour s'adonner aux joies de la bidouille. La cible : les appels entre postes fixes, dont le système et la tarification sont aux mains d'un oligopole de grands opérateurs. De quoi attiser l'esprit de défi d'ingénieux techniciens non conformistes baptisés les *phreakers*, contraction de *phone* (téléphone) et de *freaks* (marginaux). Bien vite, l'un d'entre eux va bénéficier d'une aura légendaire. Son nom : John Draper. Plus connu sous son pseudonyme : « Captain Crunch ». Cet ingénieur hirsute tient ce sobriquet d'un hack originel, élevé au rang du mythe par les amateurs de bricolage électronique. Cap'n Crunch, ce sont des céréales de petit-déjeuner, de forme ronde, nappées de sucre glace. Dans les boîtes de ces corn-flakes distribués par Quaker Oats est offert un jouet pour enfants. Le petit cadeau de l'époque était un banal sifflet en plastique. Mais Draper, déjà porté sur les astuces pour importuner les opé-

rateurs, va en faire une arme de piratage à grande échelle. En obturant un trou du sifflet au moyen de glu, il obtient un son de fréquence 2 600 hertz. Soit la même que celle signifiant un appel gratuit dans les cabines Bell. Le phreaker à moustache, avec cette manipulation enfantine, vient de pirater le réseau téléphonique. Fidèle à l'éthique des premiers hackers, Captain Crunch ne cherche pas à faire fortune avec sa trouvaille. Il multiplie, au contraire, les blagues et expérimentations, fédérant autour de lui une communauté de phreakers qui apprécie de discuter des heures sans dépenser le moindre dollar, et sans se faire repérer.

Le hacking est alors à la fois technique et politique. Un défi contre les systèmes hiérarchiques fermés. En Californie, au sein du Homebrew Computer Club, le Captain compte des lieutenants zélés. Si la plupart poursuivent cette activité comme un hobby – aussi pointu soit-il –, d'autres se greffent, petit à petit, à l'écosystème informatique en gestation, en particulier aux abords de San Francisco, haut lieu de la liberté, dans la Silicon Valley, berceau de l'industrie des semi-conducteurs et pépinière des premières startups de la micro-informatique. Parmi les bidouilleurs les plus prometteurs de la communauté, un olibrius à la tignasse épaisse et aux joues rondes, surnommé « Woz ». Steve Wozniak formera plus tard le duo fondateur d'Apple, aux côtés de Steve Jobs, lequel sera bien plus frileux que son compère quant aux incursions hors la loi, mais très inspiré en revanche lorsqu'il s'agira d'imaginer les applications marchandes des premiers ordinateurs de bureau bricolés par son compère.

Car le hack à l'ancienne va être soumis à de rudes turbulences, à mesure que l'informatique s'enracine dans les vies des entreprises, des États et des particuliers. Il est possible d'en tirer des fortunes colossales en s'adaptant à l'économie

de marché. Bill Gates, qui traitera les hackers du Homebrew Club de « voleurs » dans une lettre de 1976 restée célèbre, sera l'un des plus éminents symboles de cette génération de géniaux bidouilleurs devenus capitaines d'industrie.

La connaissance des systèmes permet aussi d'utiliser les techniques d'intrusion pour d'autres desseins que les canulars téléphoniques ou l'amélioration des machines existantes. En 1983, réalité et fiction se télescopent. Dans les salles obscures, le film *WarGames* met en scène un adolescent capable de déclencher une guerre thermonucléaire en s'infiltrant dans le supercalculateur de l'armée américaine. Dans la vraie vie, Kevin Poulsen, un blondinet de 17 ans surnommé « Dark Dante » sur les réseaux, est reconnu comme le premier hacker officiellement accusé d'espionnage après avoir infiltré le réseau ARPAnet de l'UCLA (université de Californie à Los Angeles). Il sera l'un des petits génies les plus médiatisés d'un mouvement qui passera bientôt de l'underground à une certaine popularité. Jusqu'à ce que des ados sans grandes habiletés techniques ni sens moral – surnommés les *script-kiddies* – s'amusent à essayer de déstabiliser les systèmes d'entreprise par tous les moyens, testant mots de passe et lignes de code comme on joue à piquer des chewing-gums au *grocery store*.

D'autres programmeurs doués poussent le jeu dans des eaux plus troubles, ciblant les banques et les administrations, jusqu'à ce que le *Computer Fraud and Abuse Act* de 1986 entérine cette menace nouvelle. Mais le texte de loi ne suffit pas – loin de là – pour parvenir à mettre la main sur ces nouveaux criminels connectés. Parmi les exceptions, mentionnons Robert Tappan Morris, un jeune diplômé de Harvard qui crée en 1988 le premier ver informatique (le « ver Morris »), assez puissant pour infecter six mille machines au travers d'un Internet alors réservé à quelques

fonctions stratégiques. Le jeune informaticien, pionnier de la diffusion de vers et de virus comme moyen de déstabilisation, sera repéré et condamné à quatre cents heures de travaux d'intérêt général… avant de devenir un professeur vedette du MIT et de voir le disque original où il créa son ver exposé au musée des sciences de Boston.

À la fin des années 1980, la « communauté » des hackers, déjà protéiforme, se fracture encore un peu plus devant le potentiel de nuisance qu'offrent de simples intrusions discrètes dans les méandres d'une micro-informatique encore juvénile. Le rôle social des spécialistes en programmation et codage fait débat : devenir les garants d'un système basé sur la confiance, ou profiter des failles pour s'enrichir et semer le trouble ? Les idéaux originels, tant potaches que démocratiques, sont mis à mal par certains inoculateurs de virus alléchés par les dollars faciles. Ils aiment frapper, à l'aveugle ou de manière ciblée, ici au porte-monnaie, là pour dérober des documents confidentiels.

Les années 1990 consacrent ainsi l'apparition de nouveaux spécimens sur le trombinoscope des « ennemis publics ». Des types qui affichent à leur palmarès des casses de grande ampleur, le plus souvent sans la moindre trace d'effraction. En 1994, l'informaticien russe Vladimir Levin parvient à transférer 10 millions de dollars des réserves de la Citibank jusqu'à des comptes à l'étranger… avant d'être condamné à trois ans de prison une fois ses complices démasqués[1]. Quant à Kevin Mitnick, *alias* « le Condor », ex-ado star des phreakers, il s'introduit, entre autres, dans les systèmes informatiques de Motorola, Fujitsu et Sun Micro-

1. « Russian Hacker is Sentenced to 3 Years in Citibank Heist », *The Wall Street Journal*, 24 février 1998.

systems, usant et abusant de son savoir-faire pour duper les enquêteurs à ses trousses, avant d'être finalement repéré par un hacker concurrent, en 1995, puis condamné à passer cinq ans sous les verrous[1]. À sa sortie de prison, « le Condor » reçoit l'ordre de ne pas toucher de téléphone pendant deux ans, ni d'ordinateur connecté à Internet… À sa suite, encore, de sombres héros émergent, développeurs de virus et de sites piégés. En 2002, un ingénieur système britannique au chômage, Gary McKinnon, s'introduit dans les systèmes informatiques de la Nasa et des principales administrations militaires américaines avec l'objectif, selon ses dires, de vérifier la présence d'objets volants non identifiés, qui serait cachée aux citoyens par un complot de grande ampleur. Les dégâts sont évalués à 800 000 dollars.

Mais tous les experts en piratage ne poursuivent pas des chimères. Les objectifs se rationalisent. Les méfaits numériques sont préparés avec minutie, selon une nouvelle géographie du crime, numérique celle-là. La Russie, les pays d'Europe de l'Est et quelques destinations asiatiques deviennent les tanières préférées des assaillants. Mais aussi des couvertures utilisées par ricochet, pour brouiller les pistes, en suivant des serveurs fantômes, par des cybermalfaiteurs américains, chinois, israéliens, européens ou venus d'autres horizons. Loin des défis facétieux des hackers de petits trains, une nouvelle catégorie de pirates informatiques s'acoquine avec le crime organisé et entretient, à distance, un sentiment de paranoïa généralisé.

Chapeau noir ou chapeau blanc ? Une classification simpliste et duale s'opère généralement entre, d'un côté, les « *white hats* » et, de l'autre, les « *black hats* ». À main gauche,

1. « Mitnick Released from Prison », *CNET*, 24 mars 2002.

une catégorie de bidouilleurs aux airs de chevaliers blancs, loyaux et respectant un code éthique. À main droite, un axe du mal de cyberdélinquants, prêts à tout par appât du gain, quitte à utiliser leurs compétences techniques pour récupérer et revendre des données hors de tout cadre légal. En réalité, chaque hacker définit ses limites personnelles. La distinction entre « chapeaux noirs » et « chapeaux blancs » cadre mal avec toutes les nuances de gris d'une catégorie de techniciens qui, loin d'être une corporation homogène, œuvre sur le fil du rasoir, poussant les machines à leurs limites. Et la légalité et la morale avec.

Au-delà du hack, le travail de *blogging*, de dénonciation ou de lobbying s'est ajouté aux prérogatives des « hackers éthiques », gardiens de la dimension politique de l'action, dont beaucoup travaillent main dans la main avec des « lanceurs d'alertes » popularisés ces dernières années par les figures de Julian Assange, créateur de la plate-forme *WikiLeaks*, et Edward Snowden, ex-ingénieur informatique travaillant pour la National Security Agency américaine ayant dénoncé en 2013 le programme d'écoutes et d'interceptions massives mis en place par son ancien employeur. Logiciels libres, neutralité du Net et contrôle des technologies par les citoyens font partie des chevaux de bataille de cette nouvelle génération de hackers. Un esprit d'ouverture bien éloigné des motivations de ceux qui opèrent dans l'opacité la plus totale, assurant précautionneusement leur impunité. Pour faire fleurir leur business, ces derniers doivent entrer en relation avec des clients et des commanditaires. Selon les règles du marché. L'offre et la demande. Loin, très loin de l'esprit des pionniers du MIT, ces Géo Trouvetou chercheurs de failles parce qu'amoureux des machines.

Table