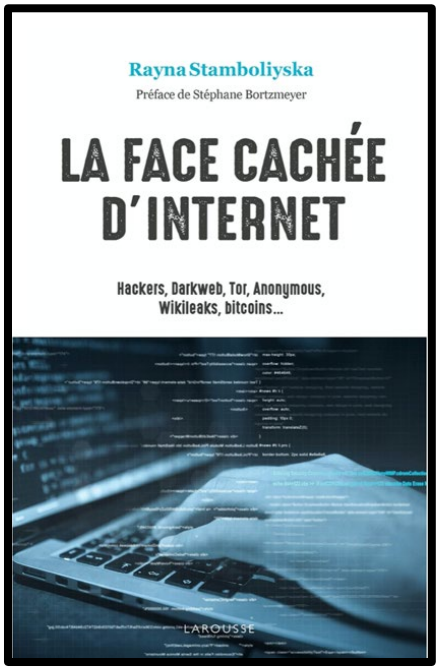
#Cultures Num
L'essentiel de la littérature numérique synthétisée
UNITEC ISIC MASTER COM

LA FACE CACHEE D'INTERNET

Rayna Stamboliyska, 2019. Larousse, 352 p.

Sylvain Lapeyre, Emilie Sadeyen, Emma Serventie, Roxane Zebina



Rayna Stamboliyska, de nationalité bulgare, est titulaire d'un doctorat de l'Université Louis-et-Maximilien à Munich puis d'un master Relations Internationales, spécialisation défense, sécurité et gestion de crise à l'Institut des Relations Internationales et Stratégiques (IRIS).

Polyglotte, elle maîtrise huit langues telles que le français, le russe ou l'anglais. Aujourd'hui, Rayna Stamboliyska est consultante auprès d'entreprises et d'organisations internationales. Elle les conseille dans leur stratégie de développement numérique et se positionne comme une experte en gestion des risques et des crises. Elle est l'auteure de *Practical D3:js* (2016) et de *La face cachée d'internet* (2017).

Dans l'ouvrage "*La face cachée d'internet*", l'auteure présente avec distance les activités illégales de l'internet et du *darkweb*. Son but étant de s'éloigner des clichés, ce livre, contrairement aux autres sur le même thème, a la particularité d'offrir un angle non sensationnel. Rayna démystifie les choses terrifiantes et le plus souvent abstraites qui nous font peur sur les activités souterraines d'internet, elle nous fait réfléchir à la démocratie en s'appuyant sur des exemples et nous incite à mieux appréhender les enjeux du numérique et notre « hygiène » numérique grâce à des outils critiques et des connaissances.

Son volume s'articule autour de trois grandes thématiques : piratages et malveillance connectée, les différentes figures du *hacker* et le *darkweb*. Cependant, nous avons fait le

choix de synthétiser cet ouvrage de façon transversale à travers quatre axes : le *darkweb*, les différentes « nuances » de *hackers* ; internet : un outil politique, et les dangers qui nous guettent, comment les limiter ?

LE *DARKWEB*, UNE NOTION CLE

En premier lieu, le *darkweb* est un thème récurrent abordé dans ce livre. Cette partie d'Internet méconnue du grand public est souvent perçue comme la partie sombre, la « face cachée » d'Internet.

Pour l'auteure, il est primordial d'opérer une distinction entre deux termes souvent confondus : « *darkweb* » et « *deep web* ». Le *darkweb* est une partie cachée d'Internet accessible anonymement via des logiciels mis en place par l'armée américaine qui permettent de se connecter à des réseaux complexes d'ordinateurs (les *darknets*). On y trouve des plateformes de contenus et de ventes non-règlementées par des gouvernements. Le *darkweb* fait peur car il est moins accessible que le web traditionnel. Cela donne lieu à un grand nombre de mythes selon l'auteure. Puisqu'il n'est contrôlé par aucune autorité, il constitue un danger potentiel seulement si on prend la décision de pratiquer des activités illégales, par curiosité ou non. Cependant, il est aussi un terrain de jeu idéal pour les journalistes et lanceurs d'alerte. Le *deep web*, quant à lui, est la partie cachée d'Internet que nous utilisons au quotidien avec des codes pour se connecter (mails, comptes en banque, pages internet qui ne sont pas référencées par les moteurs de recherche). L'auteure cherche ici à dédiaboliser les parties cachées d'Internet. Pour elle, tout ce qui est caché n'a pas vocation à être mauvais. Ce qui est dangereux, ce n'est ni le *darkweb*, ni le *deep web*, mais bel et bien ce que l'on en fait.

DIFFERENTES NUANCES DE *HACKERS*

Ce livre propose une déconstruction de plusieurs mythes autour des dangers d'internet, parmi lesquels nous retrouvons la figure du « *hacker* ». Si à l'origine le mot « *hack* » désigne un moyen alternatif de faire quelque chose, le sens a pris au fil du temps un aspect péjoratif. Rayna Stamboliyska nous explique que le *hacker* n'est pas nécessairement un dangereux hors la loi. Le bon ou le mauvais rôle du *hacker*, selon elle, dépend de ce qu'il *hack* et surtout de ce qu'il fait des informations obtenues.

« En informatique, c'est l'usage que l'on fait de la vulnérabilité qui fait la couleur du hacker » (p170)

LES TROIS CATEGORIES DE HACKER

L'auteure détermine trois catégories de *hacker* qu'elle nomme : les « *black hats* », les « *white hats* » et les « cybermilitants ». La première catégorie qu'elle désigne correspond à l'ensemble des *hackers* qui utilisent leurs aptitudes pour tromper leur victime. Ces escroqueries consistent parfois à voler des informations personnelles en piratant des boites mails ou en prenant en otage des ordinateurs entiers. A partir de là, deux scénarios se mettent en place, nous explique l'auteure. Dans le premier cas, le *hacker* récupère les données des victimes pour les utiliser lors d'activités illégales ou en les revendant sur le *darkweb* (que nous définirons plus tard). Dans le deuxième cas, le *hacker* demande de l'argent à la victime afin que cette dernière puisse récupérer ses données personnelles. Ces cas sont des exemples parmi d'autres d'arnaques mis en place par les « *black hats* ». Cette première catégorie, proposée par l'auteur, est celle qui se rapproche le plus de l'image du *hacker* qui prône dans l'imaginaire collectif.

Dans la deuxième catégorie, l'auteure nous parle des « *white hats* ». Selon elle, ce sont ceux qui se servent de leur talent de *hacker* pour apporter leur aide à la société. Par définition, le *hacker* est celui qui arrive à trouver ce qui est caché au cœur d'un système. L'auteure explique qu'un système peut contenir des failles que l'on appelle « *odays* ». Ces failles sont des portes dérobées et représentent un danger pour la structure. Lorsqu'un « *white hat* » trouve une faille, il en avertit l'entreprise ou le propriétaire du site pour améliorer la sécurité du système. L'auteure nous démontre ici que l'activité du *hacker* n'est pas nécessairement illégale et peut même être rémunérée. Des métiers se sont développés autour de cette activité : de l'expert en sécurité à l'expert judiciaire, tous portent les couleurs du « *white hat* ».

La dernière catégorie est particulière puisqu'elle se place entre les frontières de la légalité et de l'illégalité selon l'auteure. En nous parlant de « cybermilitants » ou « *grey hats* », Rayna Stamboliyska fait référence aux hackers qui utilisent des moyens illégaux pour servir une cause juste. Par exemple, certains hackers travaillent pour le gouvernement afin d'obtenir des informations sur d'autres pays. Cette capacité de révéler ce qui est caché, donne au *hacker* la responsabilité de faire connaître ou non les informations qu'il a obtenues. Cependant, l'écrivaine insiste sur le fait qu'il n'est pas toujours facile de juger si une cause est suffisamment juste pour dévoiler des informations privées.

« Dans chaque cas, décider de la moralité de l'action n'est pas chose aisée » (p.172)

LE ROLE DU HACKER

Peu importe la catégorie dont le *hacker* fait partie, ses actions poussent à s'interroger sur le fonctionnement de notre société. Selon l'auteure, l'activité principale du *hacker* est de

trouver ce qu'on veut lui cacher. Mais la question est de savoir pourquoi certaines choses sont cachées ? Rayna Stamboliyska parle de l'activité du *hacker* comme une remise en question du gouvernement ou, comme le dit l'auteure, du « pouvoir central ». Il est évident que de nombreuses informations sont réservées à une élite. Selon elle, le hacker, par son activité, remet en cause la légitimité de ces données, inaccessibles à la majorité des citoyens. Si certaines informations doivent rester privées pour le bien des citoyens, comment être sûr que le pouvoir central ne cache pas d'autres choses ? Le pouvoir central utilise-t-il toujours le numérique pour protéger ses citoyens ? De plus, selon l'écrivaine, l'activité du *hacker* a pour mérite d'informer la société sur les dangers liés à la sécurité des données. Aujourd'hui il est possible de gérer son argent via internet cependant rien ne nous garantit une sécurité sans faille. La présence du *hacker*, d'après Rayna Stamboliyska, nous pousserait à être plus vigilant concernant la sécurité de nos informations sur un plan personnel. De même lorsqu'il s'agit de structures importantes comme les banques ou les assurances, il faut pouvoir garantir à ses clients la sécurité des données pour la pérennité de l'entreprise.

En redéfinissant l'image du *hacker*, l'auteur veut mettre en lumière nos préjugés sur internet et ses acteurs. L'imaginaire social est fait de peurs qui ne sont pas toujours si effrayantes en réalité. Rayna Stamboliyska rappelle qu'internet et le *darkweb* ne sont que le reflet de la réalité.

« Quand toutes les activités humaines sont sur Internet, les activités négatives et/ou illégales le sont aussi. » (p.221)

INTERNET, UN OUTIL POLITIQUE

Pour plusieurs motifs, Internet est devenu un véritable instrument politique. S'il permet aux citoyens de pouvoir s'exprimer, il représente un outil très efficace pour les gouvernements. Révolution du Printemps arabe, élection présidentielle aux Etats Unis, censure et espionnage d'opposants au Bahreïn, tous ces éléments ont été ou sont orchestrés via Internet avec des stratégies parfois surprenantes.

INTERNET S'INVITE SUR LES BULLETINS ELECTORAUX

« Des investigations par ThreatConnect ont montré que la marque de certains « hackers » repentis ayant rejoint les services secrets {russes} a été identifiée dans quelques attaques assez louches en Allemagne, Turquie, Ukraine et dans celle contre le parti Démocrate en 2016 » (p.75)

L'auteure étudie en premier lieu le cas des élections américaines de 2016 remportées par Donald Trump. Sa victoire est pour de nombreux spécialistes due à une cyberattaque dirigée depuis le Kremlin à Moscou par le président russe, Vladimir Poutine. L'auteure nous rappelle que des e-mails compromettants concernant Hillary Clinton et des membres de son parti ont été rendus publics sur Internet. Les accusations se sont vite orientées vers la Russie à cause de la préférence de Poutine pour Donald Trump. De plus, selon Rayna Stamboliyska, ce pays a développé une véritable culture de la cyberattaque géopolitique avec déjà des actions d'ampleur à son actif.

L'auteure nous fait part de la difficulté à identifier le coupable de cette manipulation car il semble impossible de le retrouver de manière informatique. Aussi, les enjeux politiques sèment le doute quant à la nature de l'opération. En effet, le gouvernement russe a accusé des nationalistes ukrainiens voulant faire offense à son pays de réaliser des actes en adéquation avec les préférences de Poutine pour qu'il en soit tenu responsable.

LE DARKWEB AU CHEVET DE LA LIBERTE D'EXPRESSION

Pour l'auteure, le *darkweb* ne présente pas uniquement des inconvénients, comme celui de profiter à des cyberpirates. Il permettrait aux citoyens d'exprimer leurs opinions politiques dans des pays où la censure des réseaux sociaux est de rigueur. Ces derniers sont souvent prohibés et il est impossible d'y accéder via la version "claire" d'Internet. Seuls les utilisateurs du *darkweb* peuvent créer un compte personnel. De plus, il assure l'anonymat aux opposants politiques qui, même avec un faux compte, peuvent être repérés. Les algorithmes du *darkweb* brouillent les pistes et les gouvernements n'ont pas les moyens de remonter jusqu'à leurs adversaires. Par mesure de sécurité, les rivaux vivent systématiquement hors de leur pays d'origine pour éviter d'être attaqués physiquement par des mercenaires au service de l'Etat, comme ce fut le cas lors du Printemps arabe selon les explications de l'écrivaine. Cependant, ils se doivent d'être vigilants et discrets selon l'auteure dans le cas où ils rentreraient chez eux ou pour éviter à leur famille de subir des châtiments. De plus, certains états traquent leurs opposants résidant à l'étranger.

LE CYBERESPIONNAGE ORGANISE DES ETATS

« Et encore faudrait-il que les gouvernements, des acheteurs potentiels de ces vulnérabilités, légifèrent sur la publication desdites failles dont ils sont souvent les usagers » (p.47)

Enfin, l'auteure explique qu'Internet permettrait aux états de récolter des informations personnelles sur les citoyens. De nouveau, la Russie se distingue par le recrutement de *hackers*, souvent traînés en justice pour des manipulations frauduleuses, qui se voient proposer une rémunération contre une collaboration étroite avec le pouvoir en place. Les journalistes et les opposants sont les cibles principales de cet espionnage en continu, même si des informations sur chaque citoyen sont récoltées. Rayna Stamboliyska nous rappelle par exemple que le gouvernement français détient les empreintes biométriques de tous les habitants. Le plus embarrassant est que ces données sont stockées, selon l'auteure, dans des fichiers qui ne sont pas toujours sécurisés et qui pourraient faire l'objet d'une cyberattaque.

Même si le *darkweb* permet une certaine liberté d'expression sur les réseaux sociaux dans des pays où la censure est extrême, l'auteure nous amène à nous interroger sur le rôle d'internet en politique. Devant la compétence des *hackers* employés par les états, il est sûr que des failles peuvent être exploitées et fausser totalement des élections. L'arrivée du vote électronique en France est d'ailleurs largement remise en question en raison des risques de voir le logiciel piraté et les résultats truqués. De plus, l'auteure rappelle que la diffusion d'informations privées sur les candidats peut orienter l'opinion des citoyens sur des critères apolitiques, à l'image des présidentielles américaines. Internet est donc devenu un nouveau moyen de bousculer l'échiquier politique mondial largement utilisé par les états, qui y voient une opportunité d'influencer l'environnement politique en leur faveur.

LES DANGERS SUR INTERNET ET COMMENT LES LIMITER

Rayna Stamboliyska cite les dangers et donne quelques solutions simples pour nous protéger.

LE DEEP WEB, CONVOITE PAR DES PERSONNES MALVEILLANTES

L'auteure met en garde le lecteur : le *deep web* est plus dangereux que le *darkweb* pour la plupart des personnes, tout simplement car nos comptes et données sensibles attirent sans cesse des personnes mal intentionnées. Rayna Stamboliyska insiste donc sur le fait que nous avons tous des données à protéger. Une prise de conscience est nécessaire car les gens ordinaires tendent à croire qu'ils n'ont rien à cacher et ne mettent donc rien en place pour se protéger.

Nous sommes tous menacés par des méthodes qui visent à subtiliser nos données sensibles telles que le "*phishing*" (méthode de vol de données consistant à envoyer de faux

emails d'organismes de confiance afin d'obtenir les mots de passe de l'utilisateur), les "*ransomwares*" (programmes malveillants dissimulés dans un logiciel, cryptant les données de l'ordinateur jusqu'à ce qu'il envoie de l'argent) ou l'"ingénierie sociale" (pratique de manipulation psychologique en ligne, à des fins d'escroquerie). Toutes ces méthodes mises en place par les pirates et l'intérêt qu'ils y trouvent sont largement expliqués dans l'ouvrage.

« Pour reprendre une phrase que l'on croise parfois, dire que l'on n'a rien contre la surveillance car on n'a rien à cacher, c'est comme dire qu'on n'a rien contre la censure parce qu'on n'a rien à dire. » (p.306)

LE PREMIER DANGER SUR INTERNET, C'EST SOI-MEME

En somme, à la fin de cet ouvrage, l'auteure espère montrer que le premier danger sur Internet, c'est soi-même car l'humain est un facteur de risque, une faille. En effet, certains de nos propres comportements dans la vie réelle peuvent compromettre la sécurité de nos données. Le simple fait d'utiliser une clé USB inconnue, de laisser son ordinateur ouvert dans le train ou encore de consulter son compte en banque en étant connecté sur un réseau public représente un énorme risque pour la sécurité de nos données. De plus, nous vivons dans un monde où les objets connectés sont de plus en plus courants. De l'enceinte connectée au réfrigérateur intelligent en passant par les outils de domotique, nous faisons confiance à un nombre grandissant de technologies. Cette connectivité des machines ou IoT (Internet of Things) a augmenté le risque d'être attaqué en multipliant le nombre de failles : plus on utilise d'objets connectés, de sites et d'applications, plus on est exposé à des failles de sécurité. Au cours des dernières années, les experts en sécurité se sont offusqués à « l'annonce de la Barbie connectée au WiFi peut-être aussi compromise » ou encore le réfrigérateur connecté « qui laissait les identifiants et les mots de passe de comptes Gmail voyager en clair ».

Nous sommes alors le premier garant de la sécurité de notre identité et de nos données et nous sommes donc le premier facteur de risque. Pour l'auteur, il est important d'adopter au quotidien une hygiène numérique irréprochable.

QUELLES SOLUTIONS ?

Rayna Stamboliyska expose plusieurs points sur lesquels nous pouvons travailler pour améliorer notre hygiène numérique. Tout d'abord, il faut s'assurer d'avoir un mot de passe complexe (comportant chiffres, lettres et caractères spéciaux) et qui soit changé tous les 6 mois afin de prévenir les actions de personnes malveillantes qui auraient obtenu nos

identifiants. De plus, il faut limiter le nombre de comptes et d'objets connectés que l'on possède afin de s'exposer à un minimum de failles. Il convient aussi selon elle de ne pas laisser son ordinateur ouvert dans un lieu public et de ne pas se connecter à des comptes sensibles comme celui de notre banque via un réseau public.

NOTRE AVIS

Rayna Stamboliyska aborde la face cachée d'internet de façon claire, précise et transparente. Elle vulgarise le phénomène, ce qui rend la compréhension et la lecture plus simple. Ce livre est donc adressé à la fois aux débutants mais aussi aux confirmés avec des exemples approfondis.

Cet ouvrage, au-delà de mieux nous présenter les acteurs et le contexte de certaines activités illégales qui se passent sur internet et sur le *darkweb*, nous a permis de casser nos préjugés, révélant des aspects positifs et des risques insoupçonnés. On pourrait d'ailleurs se demander si cette démystification très prononcée n'est pas une volonté de l'auteure de préserver et défendre intensément son domaine : celui d'une passionnée de cybersécurité.

Cet ouvrage nous a beaucoup apporté et a eu des effets sur notre usage quotidien des TIC. Changement des mots de passe, sauvegarde sur nos disques durs, vigilance aux abords de certains sites web, chacun d'entre nous se sent aujourd'hui plus informé et acteur de son utilisation du web. C'est pourquoi, en plus de comprendre plus en détails certains événements (élections américaines, polémiques, etc…), nous le recommandons à notre entourage, aux étudiants et aux professionnels.

#CulturesNum est un programme réalisé par les étudiants du **Master Communication des Organisations de l'Université Bordeaux Montaigne** sous la direction d'**Aurélie Laborde**, en collaboration avec **UNITEC**. Depuis 2016, des ouvrages récents sur la société numérique sont synthétisés pour mieux appréhender les questions de fond pour notre société : big data, smart-cities, post humanisme, avenir du travail et de la consommation, etc...