Romain Hennion • Anissa Makhlouf
Préfaces du Général d'armée (2S) Watin-Augouard et Éric Lachapelle (PECB)

CYBER-SÉCURITÉ

UN OUVRAGE UNIQUE POUR LES MANAGERS

Cybersécurité & Risques selon ISO

GDPR

Ethical Hacking

Sécurité des Systèmes de Production 4.0

EYROLLES

Votre organisation est-elle protégée contre la cybercriminalité ? Êtes-vous en conformité avec la loi concernant la protection de vos informations et de vos actifs ?

Ce livre aborde la cybersécurité d'un point de vue organisationnel et managérial. Ainsi, les cybercriminels capitalisent sur les technologies émergentes (comme le big data ou l'intelligence artificielle) afin de mieux contourner les solutions classiques de cybersécurité. Et le développement du cloud computing n'arrange rien dans ce domaine.

C'est pour ces raisons que nous dépassons l'aspect technologique, pour proposer la mise en place d'un cadre de travail, qui s'appuie sur les normes ISO et les meilleurs standards du marché, afin :

- *d'une part, de protéger les informations et les actifs les plus sensibles de votre organisation, contre toute forme de cybercriminalité ;*
- *d'autre part, d'être en conformité avec l'évolution des exigences légales concernant la protection des informations sensibles. Notamment, la mise en place de la GDPR (General Data Protection Regulation), applicable dès mai 2018, un arsenal législatif européen auquel doivent se conformer toutes les organisations, sous peine de paiement de très fortes amendes. Ce domaine est amplement développé dans le livre.*

ROMAIN HENNION : auditeur ISO 27001/sécurité des SI et 22301/continuité d'activité (PECB). Il est aussi certifié Forensics (ISO 27037), Risk Manager (ISO 27005), Lead Cyber Security Manager (ISO 27032), et Certified Data Protection Officer (GDPR). Il est Directeur Gouvernance pour Global Knowledge, Formation. Il intervient régulièrement à l'Ecole Centrale de Paris en formation continue, ainsi qu'à l'EDHEC. Il est ingénieur Arts et Métiers, et titulaire du MBA et de l'AMP de Dauphine et de l'INSEAD.

ANISSA MAKHLOUF : Directrice Optimisation et Excellence opérationnelle pour Global Knowledge, Formation. Intervenante au niveau du MS Transformation des Systèmes de Production de CentraleSupelec EXED. Membre du groupe « usine du futur » de Systematic-Paris-Region. Elle est ingénieur et Docteur de l'Institut National Polytechnique de Lorraine et titulaire du Titre RNCP I, Expert en Génie Industriel et Services de l'Ecole Centrale Paris.

Préfaces du **Général d'armée (2S) Watin-Augouard**, fondateur du Forum International de la Cybersécurité (FIC), et **Éric Lachapelle**, CEO de PECB Certification.

www.editions-eyrolles.com

CYBER-SÉCURITÉ

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Création de maquette et mise en pages : Soft Office

Crédits photographiques :
p. 349, Shutterstock © Ursa Major, AF studio, Kuruneko Pavel Stasevich et AleksOrel

ISBN : 978-2-212-56893-6

Romain Hennion • Anissa Makhlouf
Préfaces du Général d'armée (2S) Watin-Augouard et Éric Lachapelle (PECB)

CYBER-SÉCURITÉ

UN OUVRAGE UNIQUE POUR LES MANAGERS

Cybersécurité & Risques selon ISO

GDPR

Ethical Hacking

Sécurité des Systèmes de Production 4.0

EYROLLES

Sommaire

Partie 2

Le GDPR (General Data Protection Regulation)

Partie 3

La gestion de la sécurité et des risques au quotidien

Partie 4

Introduction au *pen testing* et au hacking

Partie 5

La sécurité des systèmes de production 4.0

Préface [1/2]

En 2005, avec Thierry Breton, nous avions appelé l'attention du ministre de l'Intérieur sur une cybercriminalité dont nous annoncions la redoutable expansion. L'année suivante, le rapport du député Pierre Lasbordes soulignait l'insuffisante protection des systèmes d'information, notamment de ceux mis en œuvre par l'Etat et les grandes entreprises. Son cri d'alarme prémonitoire allait connaître une concrétisation avec la cyberattaque de l'Estonie qui a paralysé le pays pendant plusieurs jours au printemps 2007. Les médias ont alors évoqué la « cyberguerre », privilégiant le sensationnel à l'analyse juridique. Mais il est vrai que ce bombardement cybernétique entravant les fonctions essentielles d'un Etat a marqué une rupture dans l'échelle des risques cyber. Depuis cette date, il est prouvé que les actes malveillants peuvent rejoindre la conflictualité dans leurs manifestations paroxystiques. De nombreux pays, dont la France, ont pris conscience d'une vulnérabilité qui fragilise les forces, les administrations, les entreprises, les individus. En 2008, le Livre blanc sur la défense et la sécurité nationale a été l'acte fondateur d'une stratégie de cybersécurité conjuguant la sécurité des systèmes d'information, la lutte contre la cybercriminalité et la cyberdéfense. Du concept à l'action, il a fallu mettre en œuvre une politique interministérielle, avec des moyens humains, juridiques, financiers. L'Etat a compris que rien ne pouvait être envisagé sans une forte mobilisation marquée par une coopération public/privé inédite.

Quels que soient les efforts accomplis, la liste des cybermalveillances s'allonge et leurs effets s'aggravent. En octobre 2016, l'attaque par le Botnet *Mirai* a bloqué, plusieurs heures durant, des serveurs DNS, privant ainsi de connexion de nombreux sites. L'an dernier, les rançongiciels *Wannacry* et *NotPetya* ont fait la démonstration de leur capacité de nuisance planétaire, entraînant parfois la disparition d'entreprises soudain privées de leur capital essentiel : les données. Janvier 2018 a été marqué par la révélation des failles *Meltdown* et *Spectre* affectant des microprocesseurs, notamment d'Intel.

Le passé justifie une posture de cybersécurité qui n'est pas un toilettage de la sécurité mais un « reformatage ». La transformation numérique que nous vivons – et dont nous devons être les acteurs – est loin d'être achevée. Bien au contraire, sa dynamique est exponentielle. En 2030, nous serons entourés de près de mille milliards de machines connectées, interagissant au sein de systèmes intelligents qui organiseront notre vie

quotidienne. La production annuelle de données sera voisine de mille milliards de téraoctets… Nous paierons alors lourdement tout retard dans la prise de conscience des enjeux. Il n'est pas trop tard pour intensifier notre action !

La nécessité d'une cybersécurité est aujourd'hui mieux partagée, en France, mais aussi en Europe. L'année 2018 est riche en actualité : le Secrétariat général de la défense et de la sécurité nationale vient de publier une Revue stratégique de cyberdéfense, tandis que le Conseil général de l'économie a remis un rapport sur la cyberrésilience. Le Parlement est particulièrement actif avec la transposition dans la loi française de la directive européenne *Network and Information Security* (NIS), l'adaptation de la loi du 6 janvier 1978 aux dispositions du règlement général sur la protection des données à caractère personnel (RGPD) et le vote prochain de la loi de programmation militaire qui devrait renforcer encore les moyens de la cyberdéfense. Lors du Forum international de la cybersécurité (FIC), en janvier dernier, Gérard Colomb et Florence Parly, respectivement ministres de l'intérieur et des armées ont témoigné d'une volonté de conduire une politique ambitieuse soutenue par ailleurs par Mounir Mahjoubi, secrétaire d'Etat chargé du numérique. L'Europe, avec le « paquet cyber », prend désormais conscience de son rôle, de ses atouts, dans un monde numérique trop partagé entre l'Asie et l'Outre-Atlantique, vivant de fait une sorte de « Yalta du numérique ».

Tout cela est bien mais n'est pas suffisant ! Il faut, en effet, diffuser la cybersécurité qui est d'abord un état d'esprit avant d'être le fruit de techniques et de bonnes pratiques. Il faut « évangéliser », irriguer le territoire, tous les secteurs économiques et toutes les catégories de la population. L'ignorant est et sera davantage encore le « maillon faible » d'un espace numérique s'étendant pour le meilleur comme pour le pire. Une personne avertie en vaut deux, selon l'adage. La connaissance est notre première arme de protection et de défense. Elle est forgée par l'action de spécialistes qui ont choisi de ne pas conserver leur savoir et leur expérience dans une « chasse gardée », que certains protègent avec un discours abscons, inaccessible, pour mieux défendre une expertise parfois douteuse.

Les « évangélistes », eux, ont la lourde tâche de rendre simple ce qui est complexe. Romain Hennion et Anissa Makhlouf sont des « sachants » pédagogues qui expriment clairement ce qu'ils ont conçu aisément. Leur ouvrage couvre l'ensemble du champ du savoir tout en approfondissant deux questions essentielles : celle des données – et plus particulièrement des données à caractère personnel – et celle du « hacking éthique ».

Les données méritent, en effet, une attention particulière, car la couche « cognitive » de l'espace numérique est sans doute la plus stratégique. Qui maîtrise les données, domine le monde et, sans aucun doute, chacun des êtres humains qui le peuple. Cette couche, c'est celle du sens. Elle est au cœur de l'écosystème numérique. Le règlement général de protection des données (RGPD) est encore vécu comme une contrainte alors qu'il sera demain un formidable outil au service de la confiance et de

la performance. Mais, au-delà des règles qui régissent leur collecte, l'exploitation ou le profilage qu'elles permettent, ces données doivent être stockées, traitées par des systèmes de traitement automatisé de données eux-mêmes protégés contre l'action des prédateurs. L'intelligence artificielle, les megadonnées (big data) peuvent agir en amont dans la mise en œuvre d'une analyse de la menace (*threat intelligence*). Enrichie par une cybersécurité cognitive portant sur l'interprétation des données non structurées, elle permet de détecter les signaux faibles, les comportements anormaux. Mais rien ne remplace l'humain dans la lutte contre les cybermalveillances. La ressource provient évidemment des universités et des grandes écoles, dont les promotions sont encore très insuffisantes en nombre au regard de besoins croissants. La satisfaction de ces derniers peut alors être atypique et prendre sa source dans le vivier des *hackers*, parfois injustement montrés du doigt alors qu'ils ont la compétence, l'esprit d'innovation, l'intuition qui en font de remarquables chasseurs de failles. Les pentesters agissant notamment dans le cadre de *bug bounties* sont une composante essentielle d'une stratégie de cybersécurité qui ne doit écarter aucun maillon faible, notamment les systèmes industriels (SCADA), animés par une informatique de production souvent insuffisamment protégée, ou le *cloud* qui offre des garanties très inégales.

Vous qui allez lire cet ouvrage, n'ayez pas peur ! ou juste ce qu'il faut pour connaître la sagesse. La description des risques, des menaces, des effets est toujours un peu anxiogène. Mais au fil de votre parcours, vous comprendrez que la cybersécurité repose sur quatre principes fondamentaux : la confiance, la loyauté, la solidarité, la responsabilité. Confiance à l'égard des systèmes et en ceux qui les mettent en œuvre, en garantissent la confidentialité, la disponibilité et l'intégrité ; loyauté des plateformes, des algorithmes qui doivent dire ce qu'ils font et faire ce qu'ils disent ; solidarité des acteurs publics et privés, aucun ne pouvant gagner sans l'autre ; responsabilité partagée de tous, personnes physiques ou personnes morales, administrations ou entreprises, la cybersécurité de tous étant la résultante de l'action de chacun.

Ces quatre principes fondamentaux sont la trame de la démonstration de Romain Hennion et d'Anissa Makhlouf. Leur contribution à la cybersécurité, à la diffusion de son esprit et de ses savoir-faire, doit être saluée !

Général d'armée (2S) WATIN-AUGOUARD
Fondateur du Forum International de la Cybersécurité (FIC)
Directeur du Centre de recherche de L'EOGN

Préface [2/2]

Il y a plusieurs années, lorsque j'ai commencé ma carrière professionnelle, la sécurité de l'information était surtout perçue sous ses aspects technologiques. Un bon professionnel de la sécurité de l'information était d'abord et avant tout quelqu'un qui maîtrisait les aspects technologiques de la sécurité informatique. À vrai dire, on faisait peu la différence entre sécurité de l'information et sécurité informatique. Les deux termes étaient interchangeables. Le professionnel de la sécurité de l'information se préoccupait de la sécurité informatique et d'autres professionnels se chargeaient des autres aspects de la sécurité, tels que la sécurité physique, la sécurité des ressources humaines ou les aspects légaux de la sécurité. Ces divers professionnels de la sécurité coexistaient mais sans vraiment se parler.

La norme ISO 17799, qui allait plus tard donner naissance à la norme ISO 27001, venait d'être publiée et le concept de sécurité holistique et stratégique pour l'information commençait à peine à se répandre dans la communauté des professionnels en sécurité de l'information. Cette norme et ses concepts annonçaient un changement de paradigme : le professionnel de la sécurité de l'information ne devait plus seulement se préoccuper des aspects techniques de la sécurité, mais il se devait également d'être spécialiste des aspects non technologiques de la sécurité tels que la gestion des risques, la sécurité physique, la continuité des activités et l'humain. Cette norme forçait les professionnels de la sécurité à se parler, à concevoir l'information sous toutes ses formes et *via* tous ses médias. La fonction de professionnel de la sécurité de l'information ne serait plus comme avant.

L'adoption du règlement général sur la protection des données (RGPD, ou GDPR en anglais) et son entrée en vigueur cette année, annonce un autre changement de paradigme pour le professionnel de la sécurité de l'information. En effet, le RGPD et d'autres réglementations ajoutent maintenant la dimension des données à caractère personnel et la libre circulation des données aux domaines couverts par le professionnel de la sécurité de l'information. Le professionnel de la sécurité de l'information ne doit plus se préoccuper de seulement protéger les données mais d'en manager l'appartenance, et les propriétaires de ces données sont désormais des tierces parties externes à l'organisation. Évidemment, ces préoccupations existaient bien avant le RGPD, cependant ce règlement vient les porter à l'avant-scène des préoccupations

en sécurité de l'information. Et malgré le fait que le RGPD soit une réglementation européenne, son contenu affecte les entreprises non européennes. Son impact est donc mondial et affectera la pratique internationale en sécurité de l'information.

L'ouvrage de mon ami Romain Hennion et d'Anissa Makhlouf se veut ambitieux. Cette œuvre magistrale définit et explique les liens entre gestion de risques, sécurité de l'information, législation et cybersécurité. Il s'agit, à ma connaissance, de la seule lecture disponible en français qui s'attaque à ces domaines irrémédiablement reliés. Je la recommande à tous ceux qui cherchent une lecture holistique de ce domaine, qu'ils soient néophytes ou professionnels de longue date en sécurité de l'information, qu'ils recherchent une introduction à ce domaine ou une revue exhaustive du sujet.

Éric Lachapelle, Chief Executive Officer – PECB

Remerciements

Un immense merci à Éric Lachapelle (CEO de PECB, audits de certifications ISO et spécialiste de la sécurité de l'information) pour son soutien et son aide précieuse dans la rédaction de cet ouvrage, ainsi qu'au Général d'armée (2S) WATIN-AUGOUARD, Fondateur du Forum International de la Cybersécurité (FIC), pour sa confiance.

Merci à tous mes collègues de Global Knowledge, à mes étudiants de Centrale Paris et de l'EDHEC.

Merci à tous mes clients avec qui nous construisons chaque jour.

Merci à Éric Baussand pour son engagement et sa confiance, Claude Durand, Thierry Chamfrault, Yves Caseau.

À mon éditrice, Marguerite Cardoso, pour ses conseils précieux et son approche constructive de la rédaction d'un ouvrage (écrire une thèse de doctorat est bien plus facile !). Un immense merci à Clotilde de Royer pour sa relecture et la mise en forme de l'ouvrage, ainsi qu'à Oriane Gambatesa et Aude Duverger pour les illustrations et la couverture.

À ma tribu : Agnès, Arthur, Théodore, Clémence.

À mes parents et grands- parents.

Une pensée profonde pour Guy et Françoise.

À propos des auteurs

Romain Hennion est auditeur ISO 27001 (sécurité des SI) et 22301 (plan de continuité d'activité) pour PECB. Il est également certifié Forensics (ISO 27037), Risk Manager (ISO 27005), Lead Cyber Security Manager (ISO 27032), et Certified Data Protection Officer (GDPR).

Il est également directeur de la gouvernance pour Global Knowledge, entreprise de formation.

Il intervient régulièrement à l'École centrale de Paris en formation continue, ainsi qu'à l'EDHEC.

Il est ingénieur Arts et Métiers, et titulaire du MBA et de l'AMP de Dauphine et de l'INSEAD.

Anissa Makhlouf est Directrice Optimisation et Excellence opérationnelle pour Global Knowledge, Formation et intervenante au niveau du MS « Transformation des systèmes de production » de CentraleSupelec EXED.

Membre du groupe « Usine du Futur » de Systematic Paris-Region.

Elle est ingénieur et Docteur de l'Institut National Polytechnique de Lorraine et titulaire du Titre RNCP I, Expert en Génie Industriel et Services de l'École Centrale Paris.

Introduction

L'information : l'actif le plus valorisé

En 2016, les actionnaires de Coca-Cola estiment la valeur financière de cette entreprise à plus de 200 milliards de dollars. Les comptables estiment sa valeur réelle à 25 milliards de dollars. Comment expliquer un tel écart ? Les comptables estiment la valeur réelle des actifs de l'entreprise : ses bâtiments, son parc informatique, sa recette secrète du Coca-Cola. C'est là tout le pouvoir de l'information. Souvent copiée, rarement égalée, cette recette fait l'objet de toutes les convoitises. Si celle-ci est diffusée, Coca-Cola n'existe plus. Ce n'est qu'une recette, mais elle vaut quand même 25 milliards de dollars, et valorise toute l'entreprise à 200 milliards de dollars. Il y a de quoi la protéger !

Dans le même état d'esprit, les journaux et les médias ont le monopole de la publicité. Parce qu'une seule version du journal est imprimée, et que le choix des chaînes télévisées reste somme toute limité, c'est la même version qui est diffusée à l'ensemble des lecteurs et spectateurs. Les professionnels du marketing et de la publicité avançaient que la moitié de leur budget était gâchée. Car il n'y avait aucune personnalisation des messages.

Au contraire, Facebook, qui compte environ 1,5 milliard d'utilisateurs actifs au quotidien, récolte des informations personnelles qui valent de l'or : votre nom, vos coordonnées, votre date et votre lieu de naissance, votre lieu d'habitation, votre e-mail, parfois votre téléphone, etc. Au quotidien, Facebook connaît les restaurants que vous fréquentez, les équipes sportives que vous encouragez, les vidéos que vous regardez ou les livres que vous lisez, les sites Web que vous visitez, les entreprises que vous aimez, votre humeur, les appareils informatiques à partir desquels vous vous connectez, dans certains cas les détails de votre carte de paiement…

Au contraire de la presse écrite et de la télé, la valeur du marché potentiel énorme de Facebook réside dans la personnalisation des données collectées, permettant une publicité spécialisée et spécifiquement ciblée. Ainsi, à chaque fois que vous vous connectez sur votre compte, des publicités s'affichent. Celles-ci sont censées être déterminées avec précision par des algorithmes qui associent votre profil aux offres publicitaires. Certes, ce n'est pas encore parfait. En ce qui nous concerne, beaucoup de publicités ne nous correspondent absolument pas !

Dans ce contexte, qu'est-ce que l'information ? Il s'agit du contexte et du sens que nous attribuons aux faits et aux données. Dans certains cas, ce sont les hommes et les femmes qui donnent du sens. Dans d'autres cas, ce sont des algorithmes.

La valeur de l'information réside dans la manière dont vous interprétez et appliquez ces faits, pour fabriquer des produits (comme Coca-Cola) ou bien fournir des services (comme Facebook et ses publicités personnalisées au profil de chacun).

Puisque pour Coca-Cola et Facebook cette information a autant de sens, chacun comprend qu'aucune de ces entreprises ne cherchera à la partager. Ces informations doivent rester confidentielles. Coca-Cola ne partage pas sa recette. Facebook ne partage pas les informations récoltées sur ses utilisateurs.

À la rigueur, pourquoi ne pas laisser la recette de Coca-Cola dans un coffre-fort, dont vous jetez la clef ? Ou bien, plus radical, détruire toutes les copies de cette recette ? Dans ce cas, les investisseurs cessent d'acheter des actions de Coca-Cola. Car cette recette est la source de toute forme de création de valeur. La recette, aussi **confidentielle** soit-elle, doit toujours être **accessible**. Finalement, que se passe-t-il si la recette change ? Les consommateurs arrêteraient probablement d'acheter du Coca-Cola. La recette doit donc rester **intègre**.

La confidentialité, l'intégrité et la disponibilité (CIA, pour Confidentiality, Integrity et Availibility) sont donc les trois piliers de la sécurité de l'information.

Cet exemple illustre la complexité de la cybersécurité. Il s'agit d'une discipline très vaste : elle couvre l'ensemble des technologies et pratiques utilisées pour protéger les réseaux informatiques, les ordinateurs et les données contre toute forme de violation.

La cybersécurité est-elle une science ou un art ?

Chacun de nous est concerné par la cybersécurité : les gouvernements, les entreprises, les universités, les citoyens. Notre approche de la cybersécurité est très généralement empirique. L'objet de ce livre est de tenter d'apporter un minimum de « comment » et de « pourquoi » mettre en place des contrôles de sécurité.

Notre volonté au sein de cet ouvrage est d'aborder la cybersécurité selon l'angle organisationnel et légal. Beaucoup d'ouvrages sont déjà consacrés à la sécurité du point de vue technique et technologique. Avec l'arrivée du General Data Protection Regulation (GDPR), un ensemble de lois européennes qui devront être appliquées par toutes les organisations dès 2018, la cybersécurité prend une tournure juridique, que l'on peut gérer d'un point de vue organisationnel, grâce spécialement à l'apport des normes ISO 27000.

Changer de mot de passe tous les quarante-cinq jours est un très bon exemple de sagesse populaire en termes de cybersécurité. Beaucoup considèrent cette démarche comme une meilleure pratique. Cependant, l'art et la pratique de la gestion des mots de passe conduisent à des conclusions différentes. La force de votre mot de passe s'appuie sur les propriétés mathématiques d'algorithmes de chiffrage des données. Vous pouvez changer votre mot de passe aussi souvent que vous voulez, nous disposons de programmes pour craquer les mots de passe. Plus celui-ci est simple, plus celui-ci sera facile à trouver.

C'est pour cette raison que dans ce livre nous nous appuyons non seulement sur notre expérience, mais aussi faisons en permanence référence au standard et cadre de travail du marché : les normes ISO notamment, les travaux du National Institute of Standards and Technology (NIST), de la Commision nationale de l'informatique et des libertés (Cnil), etc. L'objectif est d'apporter un minimum de rigueur scientifique et surtout un cadre de travail. Car la cybersécurité concerne chacun de nous, et la protection de notre vie privée est un enjeu citoyen de plus en plus menacé. L'Europe en a pris conscience avec la réglementation sur la protection générale des données, exposée dans cet ouvrage, et qui entrera en vigueur en mai 2018.

Nous avons aussi tenté de partager avec les lecteurs notre plaisir, notre intérêt, notre curiosité, ainsi que nos doutes, sur cette discipline appelée « cybersécurité ». C'est probablement le domaine qui fait appel à tout un ensemble très varié de disciplines aussi bien scientifiques qu'humaines. Scientifique : par exemple, les algorithmes de chiffrement. Humaine : par exemple, les attaques sous forme d'ingénierie sociale, exploitant la naïveté des gens pour leur voler des informations.

La cybersécurité exige de penser aux comportements humains les pires, aux événements les plus rares, qu'il faudra modéliser de manière réaliste. Cette discipline comprend des systèmes énormes, décentralisés et complexes. Et le scientifique que je suis peut vous dire que nous n'aimons pas la complexité et le chaos, du moins en science. Pourtant, ce sera désormais notre lot quotidien. Nous y travaillons dans des environnements multicouches, et multiparties, comprenant de nombreux systèmes utilisateurs interconnectés et souvent chaotiques. Notre approche scientifique est obligatoirement systémique et non plus déterministe. Les variables à identifier sont très complexes, si tant est que vous réussissiez à les identifier ; car vous aurez à peine identifié une variable que le système aura déjà évolué.

Prenons l'exemple d'Amazon, qui gère jusqu'à 1 440 000 colis par jour[1]. Amazon a lancé une étude pour déterminer la taille des boîtes en carton afin d'anticiper son

1. https://www.francebleu.fr/infos/societe/noel-vers-un-nombre-record-de-colis-expedies-ce-lundi-chez-amazon-1482132893

stock. L'étude a été impossible à réaliser parce que les objets vendus changent trop régulièrement.

Jamais la science n'aura été aussi belle que grâce à la cybersécurité. Lorsque nous étions étudiants, nous avions appris que la science consiste à résoudre des problèmes en confirmant des hypothèses. L'idée de la science évolue. S'agit-il encore de prouver qu'une hypothèse scientifique est correcte ? Ou bien de réfuter l'hypothèse ? C'est le problème de la réfutabilité soulevé par Karl Popper, dans *La Logique de la découverte scientifique*[2]. Étant donné qu'il est impossible de juger de la vérité d'une théorie, celle-ci serait due à une hypothèse de travail ou à une supposition adaptée à un moment donné des observations. En conséquence, si quelque chose est falsifiable, cela ne signifie pas à la base que cette chose soit fausse. Cela signifie en revanche que l'hypothèse de base est fausse et que vous pouvez donc démontrer que c'est faux. Par exemple, si un quotidien indique que la Chine est la plus grande menace en cybersécurité, c'est non falsifiable parce que vous ne pouvez pas prouver que c'est faux. Et même si cette affirmation est fausse, tout ce que vous trouverez c'est une absence de preuve. Il n'existe pas de moyens empiriques de tester cette hypothèse.

Il existe encore peu d'axiomes en cybersécurité. Il reste énormément de choses à construire. De nombreux laboratoires en recherche-développement cherchent à établir les principes scientifiques de la cybersécurité, pour apporter la rigueur propre à la démarche scientifique. Par conséquent, nous pouvons nous appuyer sur la démarche scientifique pour concevoir et déployer une démarche de cybersécurité. Ainsi, la méthode scientifique contient cinq éléments essentiels : poser la bonne question, formuler des hypothèses, faire des prédictions, tester de manière expérimentale les prédictions, analyser les résultats. C'est sur cette base que sont conçus l'ensemble des méthodes et standards utilisés dans ce livre. Les expériences doivent être objectives, falsifiables, reproductibles, prévisibles et vérifiables.

Mais, et c'est un grand « mais », les éléments humains de la cybersécurité sont critiques pour la conception et l'application des pratiques de cybersécurité. Et malgré toute la rigueur de la méthode scientifique, il y aura toujours des vulnérabilités au niveau de vos équipes.

Ainsi, en octobre 2017, 145 000 agents du ministère des Finances (Bercy) ont reçu des e-mails expédiés par Emma Bovary et Jean-Baptiste Poquelin pour gagner des places de cinéma[3]. Il s'agissait d'une fausse opération de fishing pour tester les pratiques des agents. Ceux-ci étaient supposés avoir reçu une formation pour ne pas répondre à ce type de mail. Mais 30 000 personnes ont cliqué sur les liens entre 10 heures

2. Karl Popper, *La Logique de la découverte scientifique*, Payot, 2017.
3. http://www.lefigaro.fr/secteur/high-tech/2017/10/03/32001-20171003ARTFIG00010-bercy-pirate-lui-meme-les-e-mails-de-ses-agents.php

et midi le lundi matin. Le lien renvoyait en réalité vers une page Web affichant des recommandations d'usage sur les e-mails et les précautions à prendre (notamment, ne pas ouvrir les pièces jointes des e-mails ou cliquer sur les liens Internet contenus dans le corps du message).

Goethe, en son temps, aurait dit que « *ce qui retarde le plus les sciences, c'est que les hommes qui s'en occupent sont des esprits inégaux. Ils ont du zèle, mais ils ne savent pas ce qu'ils doivent en faire.* »

Avec la cybersécurité, peut-être faut-il faire évoluer les principes fondamentaux de la science. Je vous suggère l'approche de Pierre Dac, immense scientifique reconnu dans le monde entier, qui n'a pas hésité à inventer de nouvelles disciplines comme l'astro-gastronomie, la science de la découverte des étoiles des relais gastronomiques.