Avant-propos

Être simple,
c'est compliqué

L'information est à la base de toute interaction entre deux êtres doués d'intelligence : de variations chimiques entre cellules à l'échange de signaux électriques entre machines, des informations sont échangées depuis la nuit des temps. Le lecteur attentif se demandera si des cellules et des machines sont vraiment douées d'intelligence, mais qu'est-ce que l'intelligence si ce n'est notre capacité à *relier* les idées entre elles ? Le mot « intelligence » est en effet composé du suffixe latin *inter-* pour « entre » et du radical *ligare* pour « lier ». Information et intelligence semblent ainsi converger vers cette idée de « relier », que ce soit des êtres, par échange d'informations, ou des idées, par intelligence.

Le langage va dans ce sens, aussi bien que l'écriture : tous deux supportent l'échange d'informations dans un système d'information. Un système d'information peut être considéré comme un ensemble de ressources numériques et humaines organisées afin de traiter, diffuser et stocker des informations (Reix, 2002). En Europe, l'Église a longtemps conservé une mainmise sur l'écrit, mais l'activité commerciale augmentant durant les XI^{e} et XII^{e} siècles, l'écriture s'est imposée et intégrée pour la gestion des affaires et le partage d'information source de connaissances. Au XV^{e} siècle, Gutenberg a accéléré la diffusion des informations en inventant l'imprimerie. Cette première rupture sera suivie, à la fin du XIX^{e} siècle, d'une autre rupture lorsque Hollerith, avec la *Tabulating Machine Company*, a accéléré non pas la diffusion mais le traitement des informations. Afin d'aider au recensement de la population américaine de 1890, il a proposé de coder les informations

concernant chaque citoyen américain sur des cartes perforées avant de les traiter (figure A.1). L'information devient alors traitée de manière automatique, c'est l'informatique (information-automatique). Au début du XX^e siècle, la *Tabulating Machine Company* devient la *International Business Machines Corporation* (IBM).

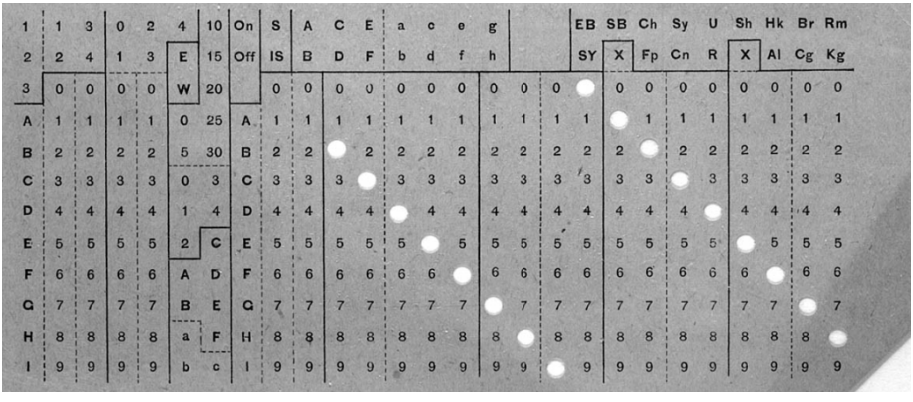

Figure A.1. *Une carte perforée Hollerith en 1890 (source : The Library of Congress, American Memory)*

L'informatisation massive des systèmes d'information au cours de la seconde moitié du XX^e siècle a conduit les pays engagés dans ce processus d'informatisation à réfléchir à l'éthique et à la sécurité de tels systèmes. En effet, les tabulatrices Hollerith auraient permis au régime nazi de recenser des milliers de personnes et ainsi faciliter leur déportation. En 1974, en France, le projet de Système automatisé pour les fichiers administratifs et répertoire des individus (SAFARI) a suscité une vive émotion dans l'opinion publique alors qu'il était question pour le ministère de l'Intérieur de créer une base de données centralisée de la population commune à tous les fichiers administratifs et bancaires. En réponse à cette initiative contestée, la Commission nationale de l'informatique et des libertés (CNIL) a vu le jour en 1978 afin de définir un cadre pour que l'informatique soit « au service de chaque citoyen » et pour qu'elle « ne [porte] atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques » (République française, 1978). Aux États-Unis, la construction de modèles permettant aux concepteurs d'appréhender la « confiance » a même été expérimentée (TCSEC, 1985). Le règlement européen sur la protection

des données (RGPD) de 2016 est également une initiative de régulation et de réglementation concernant l'usage des données personnelles.

Pour certains, l'informatique peut représenter une faille dans la sécurité des systèmes d'information dans la mesure où elle traite les informations de manière automatique. Aussi, la sécurité des systèmes d'information a souvent été regardée au travers d'un prisme se focalisant sur les artefacts, sur l'informatique et, sur les technologies. Ce livre se veut intemporel, pertinent au XIX^{e} siècle aussi bien qu'au XXI^{e}, il ambitionne de changer ce paradigme et de s'intéresser à la sécurité des systèmes d'information en considérant les individus comme des composants à part entière. En effet, ils sont susceptibles, tout comme un ordinateur ou n'importe quel artefact, de constituer une *menace intérieure* pour la sécurité du système d'information.

Introduction

L'informatique n'est plus ce qu'elle était en 1974, ni même en 2006. Les systèmes d'information dans les organisations sont largement supportés par des systèmes informatiques sous-jacents, dont la sécurité peut être rigoureusement assurée au travers de procédures, de fragments de code et d'infrastructures.

Alors qu'une carte perforée d'hier pouvait être dérobée pendant son trajet entre une perforatrice et une tabulatrice, une information d'aujourd'hui, dématérialisée, est soumise à d'innombrables menaces quant à sa sécurité. Les artefacts numériques sont partout, l'informatique est ubiquitaire (Nojima, 2005 ; Friedewald et Raabe, 2011), si bien que l'individu n'est plus un simple utilisateur du système d'information, mais un composant à part entière (Arduin *et al.*, 2015). La définition faite par Reix (2002) d'un système d'information intègre une composante numérique, certes, mais également une composante humaine. Se pose alors la question suivante : comment assurer la sécurité d'un système d'information en prenant en compte les individus en tant que composants au comportement parfois irrationnel ?

Ce livre s'intéresse plus particulièrement à la composante humaine du système d'information, notamment parce qu'elle constitue une *menace intérieure* pour sa sécurité. La sécurité doit en effet être assurée non seulement du point de vue des artefacts numériques, mais aussi et surtout d'un point de vue humain, social et managérial. Cela constitue la principale originalité de cet ouvrage qui fait évoluer le paradigme de la sécurité des systèmes d'information en insistant particulièrement sur la menace intérieure, celle qui se trouve à l'intérieur même de l'organisation, maîtrise ses processus, son pare-feu et sa politique de sécurité. Qu'elles soient intentionnelles ou

accidentelles, malicieuses ou non malicieuses, les menaces intérieures doivent être identifiées, connues et maîtrisées, ce que ce livre propose de faire.

Entre 2013 et 2015, plus de 100 banques de 30 pays ont été victimes de cyberattaques, avec des pertes estimées entre 300 millions et 1 milliard de dollars, d'après un rapport de la société de cybersécurité Kaspersky Lab (Kaspersky, 2015). La plupart du temps, les institutions concernées passent sous silence ou minimisent ces attaques. Les outils utilisés ne sont pourtant pas d'une grande complexité, mais l'opération d'infiltration, elle, l'est : les attaquants ont pris le temps de comprendre les procédures internes à l'organisation visée afin de cibler la composante humaine. Ce rapport se focalise sur le logiciel malveillant Carbanak, au travers duquel les attaquants ont procédé à une reconnaissance manuelle du réseau de la victime afin d'accéder à ses systèmes critiques et de comprendre son infrastructure pour y installer des logiciels d'accès à distance. Comment les attaquants ont-ils installé Carbanak dans l'organisation visée ? Quel point d'entrée dans le système ont-ils utilisé ?

Alors que 200 milliards de mails sont envoyés chaque jour dans le monde, en 2015, les attaquants ont utilisé la méthode du *spear phishing*[1]. Des mails personnalisés ont été envoyés à un nombre limité de cibles pertinemment choisies (voir figure I.1). Contrairement au *phishing*[2], le *spear phishing* intègre des techniques d'ingénierie sociale afin de mettre en confiance la cible et de la persuader du caractère véridique des informations qui lui parviennent. Ces techniques seront étudiées dans ce livre et le lecteur intéressé les retrouvera dans le chapitre 4.

Ainsi, c'est bien l'humain qui a constitué le point d'entrée dans le système utilisé par les attaques Carbanak énoncées ci-dessus. Une fois installé, Carbanak enregistre toutes les frappes au clavier et prend des captures d'écran toutes les vingt secondes. Ces informations permettent ensuite aux attaquants de mieux connaître leur victime et de mieux cibler leurs prochaines attaques.

1. « harponnage. »
2. « hameçonnage. »

```
Good Day!
I send you our contact details
 The amount of deposit 32 million rubles and 00 kopecks, for a period of 366
days,% year---end contribution term
 Sincerely, Sergey Kuznetsov;
+ 7 (953) 3413178
f205f @ mail.ru
```

Figure I.1. *Exemple de mail de harponnage Carbanak ayant fonctionné. Un fichier de configuration compressé au format .rar l'accompagnait (source : Kaspersky, 2015)*

Dans un système d'information, l'humain est – au même titre que l'ordinateur ou tout autre artefact numérique – un composant du système : il traite, stocke et diffuse des informations. Depuis l'informatisation massive des systèmes d'information dans la seconde moitié du XX^{e} siècle, une volonté forte de sécuriser les systèmes d'information a mis l'accent sur la sécurité des systèmes *informatiques* sous-jacents. Cette volonté a néanmoins mis de côté la composante humaine. L'humain peut ainsi constituer une menace, mais c'est continuer de négliger cette menace, en se focalisant sur le numérique, qui participe au succès des attaques. Des observations que nous avons pu mener sur le terrain, aussi bien que des investigations dans la littérature en la matière, nous ont conduits à nous focaliser sur la menace intérieure que constitue la composante humaine, c'est-à-dire les employés dans une organisation, pour la sécurité du système d'information.

Ce livre est composé de deux parties : la première présente le système d'information du point de vue de ses composants : des technologies (chapitre 1), qu'historiquement l'Homme a déployées à des fins précises telles que supporter l'échange et le traitement d'informations dans des systèmes organisés (armée, commerce, puis « organisations »), et des personnes (chapitre 2), qui sont autant de composants interprétants dont le comportement est parfois irrationnel au sein des systèmes organisés qu'ils composent. Ces composants du système d'information, technologies et personnes, sont autant de points d'entrée susceptibles de constituer une menace pour la sécurité du système d'information. Aussi, la seconde partie de ce livre focalise son attention sur la menace intérieure que peuvent constituer les personnes qui composent le système d'information. Une catégorisation de ces menaces intérieures est proposée (chapitre 3), puis le focus va se porter sur chacune d'elles. Les menaces intérieures non intentionnelles dans le chapitre 4, où des techniques de manipulation et d'ingénierie sociale amènent un employé,

composant du système, à faciliter malgré lui l'infiltration d'un attaquant. Les menaces intérieures intentionnelles et non malveillantes dans le chapitre 5, où un employé a intérêt à contourner la politique de sécurité des systèmes d'information pour faciliter son quotidien mais sans volonté de nuire. Enfin, les menaces intérieures intentionnelles et malveillantes dans le chapitre 6, où le contexte organisationnel et les processus cognitifs pouvant conduire un employé à vouloir nuire sont analysés, de même que la possibilité – ou non – de l'en dissuader. Une discussion sur les limites et les évolutions possibles des éléments présentés dans ce livre est finalement proposée en conclusion.