Les enjeux de la cybersécurité

David Bensoussan

L'auteur est professeur de sciences à l'Université du Québec

Selon le futuriste Alvin Toffler, l'ordre économique aura été déterminé par trois phases successives : la première, celle de l'agriculture, s'est étalée sur plusieurs milliers d'années et a mis fin à l'alimentation par la cueillette ; la seconde est la vague industrielle qui s'est étendue sur trois siècles et est en voie d'être supplantée par une 3e vague : celle du savoir.

Le terme vague convient bien à cette troisième phase, car elle est accompagnée de numérisation et envahit de plus en plus rapidement notre environnement et bouleverse notre mode de vie.

Le premier ordinateur construit par John Von Neuman était capable d'effectuer 15 000 opérations par seconde. Nos ordinateurs portatifs peuvent exécuter plusieurs milliards d'opérations par seconde[1].

Dans le futur, la puissance de calcul sera infiniment plus grande avec les ordinateurs quantiques qui sont actuellement en développement. Qui plus est, l'intelligence artificielle va permettre d'augmenter la capacité de calcul et d'analyse à des niveaux de sophistication qui relèvent de la science-fiction.

---

[1] L'invention du transistor en 1953 a préfiguré les circuits intégrés de très haute vitesse. Selon la loi empirique de Moore, la capacité d'un circuit intégré à semiconducteur - aussi appelé puce électronique - se mesure à la densité des composants qu'il contient et double tous les 18 mois. Elle est caractérisée par sa finesse de gravure en nanomètres (nm). Ainsi, une finesse de gravure de 5 nm (soit la dimension de 50 atomes) permet d'intégrer 200 millions de transistors par millimètre carré. En 1971, le premier microprocesseur d'Intel (modèle 4004) intégrait 2300 transistors; un demi-siècle plus tard, celui d'Apple (M1 Max) en intégrait plus de 50 milliards.

La dépendance du numérique et les dangers qui lui sont associés.

Le monde moderne est transformé par des nouvelles réalités technologiques envahissantes dans les domaines de la production manufacturière, des télécommunications, des loisirs et de la défense. Notre économie est pour ainsi dire virtualisée.

Or, toute nouveauté introduit des améliorations, mais aussi des risques. Car les données personnelles, commerciales et publiques s'accumulent dans des serveurs qui sont susceptibles de subir des attaques logicielles malveillantes. C'est le cas aujourd'hui et il faut s'attendre à ce que les attaques informatiques augmentent substantiellement. L'Internet des objets qui va faire communiquer ensemble un grand nombre de senseurs domiciliaires risque d'augmenter sérieusement les risques d'intrusions hostiles.

Nul doute que les institutions responsables de la défense de l'État et du citoyen doivent se prévaloir de mesures préventives pour arrêter, interrompre, dégrader, tromper et détruire les intrusions et attaques informatiques. Il leur incombe de protéger tant les installations vitales tout comme l'approvisionnement en eau et en électricité que la vie privée des citoyens.

Logiciels malveillants et rançongiciels

Les services de sécurité commencèrent à s'intéresser à la cybersécurité dans les années 80. Ce domaine commença à être considéré comme une arme dans les années 90 avant de devenir une nécessité dans les années 2000. Au cours de la décennie suivante, la cybersécurité fut de plus en plus employée dans les domaines civils et non plus exclusivement militaires.

Les premiers logiciels malveillants cherchaient à geler les opérations d'un ordinateur ; par la suite, ils menacèrent de publier des informations personnelles ou même des informations sensibles des compagnies et des gouvernements.

À titre d'exemple, la Russie est connue pour ses attaques cybernétiques contre l'Estonie en 2007, la Géorgie en 2008 ainsi que d'autres visant le réseau d'alimentation électrique de l'Ukraine en 2017, ou encore les réseaux sociaux aux États-Unis dans le but d'interférer avec les élections américaines et ternir l'image de la candidate à la présidence Hilary Clinton. La Corée du Nord a lancé des attaques cybernétiques contre la Corée du Sud et les États-Unis. L'Iran fit de même contre la compagnie pétrolière saoudienne Aramco.

En 2020, le clerc iranien Rahim Mahdavipour déclara dans un sermon télévisé que l'Iran avait lancé deux attaques cybernétiques contre Israël menées contre les installations de désalinisation de l'eau de mer et le réseau de distribution électrique. Ces deux attaques furent déjouées.

Le logiciel malveillant Stuxnet développé par la NSA américaine et l'unité 8200 israélienne fit désynchroniser les centrifugeuses atomiques iraniennes de leur vitesse de rotation nominale. Cette action frappa l'imagination. Elle fit réaliser qu'il était possible de s'attaquer à des installations physiques au moyen de virus logiciels.

Les rançongiciels (*Ransomware*) exigent une rançon en échange de la non-divulgation de renseignements sensibles. Le rançongiciel Conti (originaire de l'Europe de l'Est) a menacé de geler les services gouvernementaux en Irlande et s'est attaqué à la banque centrale d'Indonésie. L'on soupçonne que des dizaines de millions de dollars ont été ainsi extorqués ; des hôpitaux britanniques, irlandais et français, tout comme le système d'oléoduc américain *Colonial Pipeline* ont fait l'objet de rançongiciels.

Il faut également faire état du logiciel espion israélien Pegasus de la compagnie israélienne NSO destiné à infiltrer les téléphones intelligents et qui est utilisé sous licence par de nombreux gouvernements.

Problèmes d'éthique

Tant les citoyens que les industries et les administrations constituent des cibles de cyberattaques : vol de données, intrusions, escroqueries et malveillances de tous genres.

Comment protéger les données d'une banque sans avoir accès à des informations individuelles ? Comment limiter l'accès aux données médicales alors qu'elles sont vitales pour effectuer des traitements d'urgence ? Comment chercher à identifier un terroriste sans ratisser la base de données du citoyen?

Comment protéger la vie privée ?

Comment se protéger sans se mettre dans la peau de l'attaquant en vue de développer des mesures préventives ? Tôt ou tard, il faudra rentrer dans le système de l'adversaire et retrouver l'origine d'un virus informatique.

Les instances responsables de la sécurité devront être accompagnées de comités d'éthique qui définiront les activités cybernétiques permissibles et éviter les abus potentiels du pouvoir étendu des intrusions cybernétiques.

Comment réduire les risques d'attaques cybernétiques ?

L'importance de la cybersécurité a été reconnue par de nombreux pays. Ainsi, le président Poutine déclara en 2014 que chaque pays tente d'utiliser sa position dominante dans l'espace informationnel mondial pour atteindre des objectifs non seulement économiques, mais aussi politico-militaires. Le congrès annuel *Cyber week* en Israël réunit des milliers de participants de plus de 80 pays. Le fait que des cyber gendarmes aient participé au défilé traditionnel du 14 juillet vient souligner l'importance que la France porte à ce domaine.

Cette conscientisation des capacités et des dangers de la cybernétique devrait se faire dans les milieux scolaires, universitaires et industriels. Gérer ses mots de passe dans un coffre-fort numérique, éviter de tomber dans des pièges d'hameçonnage en évitant de pénétrer dans des sites suspects, sécuriser ses réseaux Wi-Fi sont autant de façons d'apprendre à connaître les risques et de mieux les contrer.

Le devoir de l'État est de recourir à des dispositifs contre le brigandage et la délinquance informatique et offrir des services destinés aux petites et moyennes entreprises. À titre d'exemple, le *Centre canadien pour la cybersécurité* offre des conseils de base aux individus, aux entreprises et aux institutions.

Une attention particulière devrait être apportée au harcèlement des jeunes et des vieillards qu'il faudra sensibiliser aux dangers de l'Internet et du *Dark net*. Ce dernier permet de naviguer de façon anonyme dans la toile.

L'environnement numérique est devenu le lieu géométrique des enjeux sociétaux, économiques, militaires et civilisationnels.

En matière de cybersécurité, il importe de ne pas rester sur la défensive et prévoir des attaques.