Comment créer une société plus cyber-résiliente ?

Par
Marie Kratz
ESSEC Business School

Suite à la révolution technologique, nous sommes désormais confrontés à un flux rapide et massif d'informations. La donnée a de plus une valeur marchande. Gérer cette quantité d'informations crée des problèmes de sélection par les individus, d'éthique, de sécurité et une hausse exponentielle des coûts humains et financiers de la cybercriminalité. Même si individus, compagnies, et politiques, prennent conscience de l'importance grandissante du risque cyber, comment prendre chacun sa part de responsabilité pour créer une société plus résiliente ?

Comprendre les risques cyber : un défi certain

Le manque de données statistiques fiables, les pertes sur des éléments intangibles difficiles à mesurer, les constants développements informatiques rendent la modélisation complexe. De fait, de par sa nature émergente, il est difficile d'appliquer au risque cyber les techniques traditionnelles d'analyse de risque. L'analyse d'un risque cyber dans une situation donnée met en jeu plusieurs facteurs : les motivations des cybercriminels, les caractéristiques des cibles, les motivations de l'utilisateur, les protocoles de sécurité, etc.

Le risque cyber est un **sujet multidisciplinaire,** du fait de sa complexité, sur lequel chercheurs en sciences humaines et sciences 'dures' devraient collaborer afin d'obtenir une image réaliste de ces risques et pouvoir ainsi établir des stratégies de protection des individus et de la société. En effet, il est fondamental de confronter et rapprocher des **approches qualitatives et quantitatives** *(1)*.

Le cyber, une affaire d'experts?

Le développement des nouvelles technologies nous concerne tous. Si les uns ont pour rôle d'expliquer, les autres doivent comprendre. Nous ne pouvons perdre **notre esprit critique** sous prétexte de complexité technologique. Comme souligné par Aurélie Jean *(2)*, nous devrions tous comprendre en quoi consiste un algorithme, ce qu'est une donnée, changer son attitude vis-à-vis des plateformes, développer l'art du doute, de la distanciation, face à une information qui s'est accélérée et qui joue souvent sur le sensationnel, l'excitation, plus que l'explication *(3)*. **Alors que l'explication est indissociable de la pensée !**

© Photo by Elijah O'Donnell on Unsplash

Cyber-résilience ou cyber-sécurité ? *(4)*

Le terme de « cyber résilience » est apparu récemment et prend de plus en plus d'importance. La cybersécurité est focalisée sur la sécurité seule, mais les organisations ont besoin d'une stratégie plus large qui inclut sa capacité à survivre à une attaque et la possibilité d'assurer une partie des risques inévitables.

Il existe une différence substantielle de sens entre les deux. Le terme de résilience fait référence au flottant, à l'élastique, au malléable, à ce qui est facile à renouveler et protecteur. **La cyber résilience qualifie la capacité d'une organisation à se rétablir et à continuer d'exercer son activité lorsqu'elle subit une cyber-attaque.**

Le futur de cette résilience sera dans la combinaison de mesures de sécurité, de redondances dans les systèmes informatiques et de couvertures assurantielles pour assurer la survie et le fonctionnement du système, mais aussi, en prévention, dans l'éducation et le développement du doute face à l'information.

Cyber et Ethique

Enfin, pour améliorer la cyber-sécurité *(5)* **,** il faut prendre conscience qu'on doit aller au-delà des solutions technologiques et des investissements, vers la **mise en place d'une législation** sur ce sujet, mais une législation suffisamment souple, proposant des **solutions intermédiaires et itératives**. Les pays les plus développés économiquement constituent toujours des cibles privilégiées, mais le renforcement de leur arsenal juridique augmente leur résilience. La RGPD est un pas dans ce sens.

(1). Living in a stochastic world and managing complex risks (disponible en ligne: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2668468). Voir aussi les deux articles de presse de M. Dacorogna, M.Kratz et P. Lecomte: "Managing risk is about raising society's resilience", The Business Times, Singapore, Dec. 2015; 'Changing times require new tools for risk management', Asia Insurance Review, Dec. 2016

(2). A. Jean. De l'autre côté de la Machine - Voyage d'une scientifique au pays des algorithmes. Éditions de l'Observatoire, 2019. Voir également L'émission 'Le virtuel, porte d'entrée sur le réel'

(3). 'Comprendre ce qu'expliquer veut dire', par le physicien V. Berger, dans 'La conversation scientifique' par Etienne Klein, France Culture

(4). M. Kratz. S'adapter au nouvel environnement des risques: peut-on assurer le risque cyber ? ESSEC Knowledge Avril 2019 et Reflets Magazine Juin 2019

(5). Voir aussi le numéro spécial (à l'occasion du FIC2020) de la revue de la Gendarmerie Nationale : 'L'humain au cœur de la cybersécurité'