Les cyberrisques

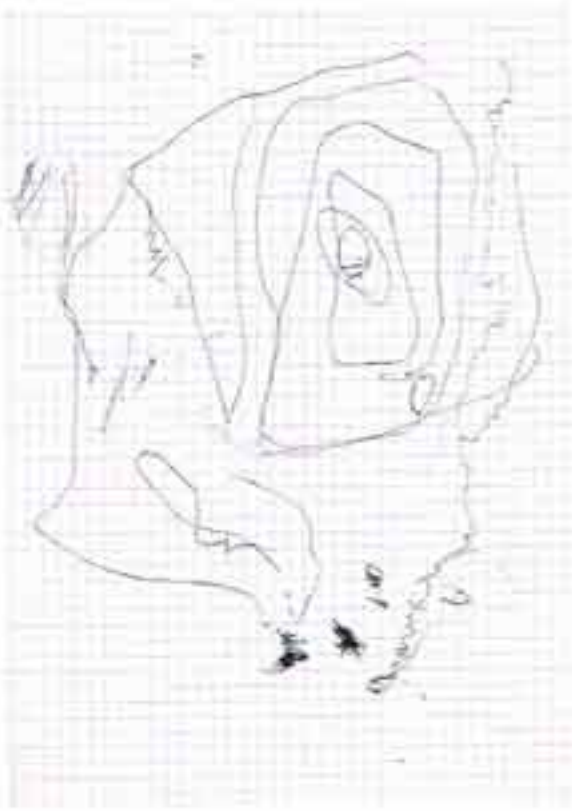
Réalités
et
perspectives

Prof. Solange Ghernaouti

Membre de l'Académie Suisse des Sciences Techniques (SATW)

Directrice du Swiss Cybersecurity Advisory & Research Group

Université de Lausanne



ISBN 978-2-9700878-0-9

2013

Les cyberrisques

Réalités
et
perspectives

Prof. Solange Ghernaouti

15 questions clés pour comprendre rapidement les principaux risques liés aux technologies de l'information et à Internet et les défis de la cybersécurité pour les individus, les organisations et l'Etat. Ce livre offre un panorama objectif et synthétique d'un sujet complexe pour ne pas rester démuni face à la réalité des cybermenaces et de leurs impacts sur notre société.

Prof. Solange Ghernaouti est membre de l'Académie Suisse des Sciences Techniques (SATW), directrice du *Swiss Cybersecurity Advisory & Research Group* de l'Université de Lausanne et experte internationale en cybersécurité.

ISBN 978-2-9700878-0-9

2013

Table des matières

Les cyberrisques

Réalités et perspectives

Sommaire

Le 3 janvier 1983 Time Magazine consacrait sa couverture à l'ordinateur sous le titre « *Machine of the year ; The Computer Moves In*" en spécifiant : "Un monde émerge, résultant d'un bouleversement technologique qui introduit l'ordinateur auprès de tout un chacun". Ainsi, après avoir consacré pendant plus de cinquante ans sa couverture "L'Homme de l'année" à un humain, Time Magazine a choisi pour L'Homme de l'année, non pas un homme, mais l'Ordinateur, marquant de cette manière le fait que l'ordinateur est devenu en quelques décennies l'ordonnateur du changement global de notre époque[1].

Aujourd'hui, l'informatique et les télécommunications sont devenues omniprésentes et des vecteurs incontournables de toutes nos activités. Avec l'Internet, notre société est entrée dans l'ère informationnelle, où tout est information numérique, tout est traitement informatique.
L'information numérique est capable de représenter tous nos différents systèmes de communication, paroles, sons, musique, images, vidéo, chiffres, dessins, tableaux, ... le binaire est devenu la nouvelle symbolique universelle, commune à tous les ordinateurs. La conversion de l'information en binaire, son traitement informatique

---

[1] Source : R. Berger ; S. Ghernaouti « Technocivilisation, pour une philosophie du numérique » ; PPUR 2010.

et sa communication via des réseaux, ne sont pas seulement affaire de technique ou de technologies. Cela entraîne des effets économiques, sociaux et culturels considérables et change structurellement notre façon d'agir, que cela soit aux niveaux collectif ou individuel, au niveau national ou international. Un nouveau monde se crée « le cyber », un nouveau territoire se développe « le cyberespace ».

L'informatique communicante bouleverse entre autres, nos habitudes, nos modes de penser, de communiquer, de nous divertir, d'apprendre, de travailler, de créer de la valeur et de la partager ou encore de faire la guerre. Le formidable potentiel d'Internet et des technologies du numérique pour contribuer au développement personnel et économique est également au service des malveillants. Qu'ils soient délinquants, criminels, terroristes, mercenaires ou acteurs étatiques, certains savent exploiter les capacités offertes par le « cyber » pour nuire, déstabiliser, influencer, contrôler, espionner, voler, s'enrichir au dépend d'autrui ou prendre du pouvoir, selon des motivations et circonstances qui leurs sont propres.

Fait de société, désormais le numérique fait partie de notre quotidien et touche tous les domaines privé, professionnel, civil et militaire, toutes les organisations, petites et grandes, privées et publiques, le numérique concerne tout le monde, jeunes et moins jeunes, et toutes les activités licites et illicites. Par ailleurs, les malveillants et organisations criminelles sont de plus en plus performants grâce aux technologies de l'information, les escrocs ont une imagination sans limite, de nouvelles formes de guerres y compris de guerre économique se déroulent dans le cyberespace. Ne pas appréhender cette réalité c'est s'exposer inutilement à une perte de compétitivité économique, de stabilité, de souveraineté nationale et de crédibilité sur le plan international. De plus, c'est laisser l'opportunité de favoriser la prise de contrôle de nos infrastructures, y compris celles vitales à notre pays par des acteurs à priori déloyaux, c'est accepter de contribuer à la montée en puissance de la

criminalité qu'elle soit organisée ou non, c'est en faire porter le coût sur la société et c'est laisser prendre un retard préjudiciable aux force de justice et de police. Cela reviendrait à ne plus être en mesure de pouvoir protéger correctement la population, nos biens matériels et immatériels, notre héritage digital et les valeurs démocratiques de notre société.

Ainsi, les individus, les organisations et l'Etat sont confrontés à des cybermenaces, jusqu'alors inconnues. L'usage extensif des technologies de l'information et de la communication génère de nouveaux risques. Le cyberespace est fragile, sujet aux pannes et dysfonctionnement et la cybercriminalité fait à présent partie de l'actualité. Encore trop souvent méconnues et males appréhendées, les cybermenaces peuvent générer de la peur. On ne sait pas forcément prédire quand, ni comment elles vont se concrétiser, quels en seront les effets dominos et les incidents en cascade qui en découleront, qui en sont les auteurs ou les commanditaires. Ces derniers peuvent se trouver dans un certain pays, viser éventuellement un pays tiers et faire transiter les cyberattaques par des pays ou infrastructures différentes.

Evaluer les scénarios de risques possibles, leurs impacts directs et indirects pour mettre en place des mesures de protection, de détection et de correction est un exercice complexe et difficile. Dans le domaine « cyber », gérer l'incertain et le probable, anticiper les risques majeurs, mettre en place des mesures de résilience, de gestion de crise et de continuité, être proactif, prévenir, protéger et réagir sont des nécessités pour les organisations et l'Etat. Au niveau du pays, cela s'inscrit dans une approche globale de la gestion des risques et de la sécurité, dans une logique de continuum de cybersécurité et de cyberdéfense. Cela se traduit par une stratégie de la cybersécurité et des mesures opérationnelles performantes. Chaque acteur de la chaîne numérique, qu'il soit producteur ou consommateur, a un rôle à jouer en matière de cybersécurité. Une culture du numérique et de la cybersécurité, une compréhension des

risques et l'application de mesures simples, efficaces et efficientes doivent exister et être adoptées par chaque internaute.

C'est pour ne pas céder à la peur et rester démunis face aux cybermenaces que ce petit fascicule offre un panorama global des risques cybernétiques et la manière dont ils s'expriment notamment via la cybercriminalité, envers les personnes, les entreprises et la nation. Articulée autour de grandes questions, la problématique des cyberrisques est exposée de manière synthétique et pragmatique et complétée par une approche prospective concernant les principales évolutions technologiques. Les défis importants que la Suisse doit relever dans le domaine cybernétique sont identifiés et des éléments de maîtrise des risques sont proposés.

Prof. S. Ghernaouti, Avril 2013