Rénover la cybersécurité.

Auteur : Gérald Vernez

Les défis de la mutation digitale[1], en particulier les risques liés, augmentent sans cesse. L'ampleur de cette évolution pour la société réclame un changement de posture et d'instruments, une action en profondeur où chacun est conscient de ses responsabilités et en mesure de les assumer à son échelon. L'approche proposée dans cette courte contribution repose sur trois méthodes, holistique, systémique et en réseau et trois piliers, l'anticipation, la responsabilité et l'action. Il s'agit ainsi de mutualiser les capacités et de réellement rendre la cybersécurité accessible aux petites structures.

Même si on ferme les yeux, le temps est à l'orage

Consulter un dictionnaire au sujet du mot *«paix»* en dit long sur l'humanité: *«absence de guerre»*. En tout cas, depuis le 24 février, ceux qui avaient rêvé d'une Europe pacifiée après la chute du mur de Berlin ont été contraints de réviser leurs attentes. Oui, l'espèce humaine est incapable de penser en dehors du prisme de la compétition, de la conquête et de la destruction et il y aura toujours quelqu'un pour s'approprier ce que vous possédez ou pour essayer de vous dépasser.

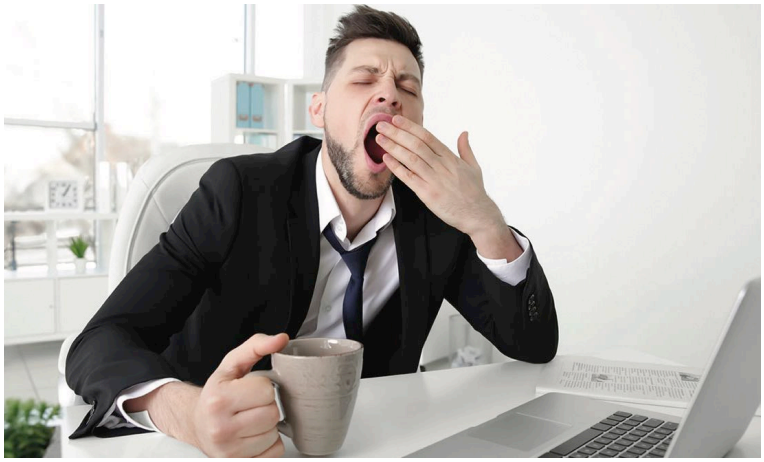
Le cyberespace ne fait pas exception et les délits contre ou au moyen de celui-ci, affranchis de la contrainte des formes classiques de la criminalité (distances, temps, risques, etc.) progressent rapidement et permettent des gains substantiels à leurs auteurs. En face des activistes, criminels, espions, saboteurs… acteurs agiles, collaboratifs et opportunistes, on trouve des dispositifs de sécurité souvent inexistants (au niveau des petites structures), inadaptés, inefficaces et compartimentés ou encore soumis à un contrôle démocratique et juridique étroit.

Ainsi, le score du match entre la société et la face obscure du cyber penche largement en faveur de cette dernière ainsi que des nations[2] qui ont par exemple inscrit le vol de propriété intellectuelle dans leur stratégie ou qui n'hésitent plus à y faire également la guerre. Tous ces acteurs ont fort bien compris que la digitalisation fait du monde une cible facile et un gigantesque self-service[3]. Malgré le coût des dommages[4] et les nombreux avis de tempête et la guerre en Ukraine, il faut malheureusement constater que nous n'avons pas encore réussi à cesser de faire semblant et de nous mentir.

Corriger la posture et élargir la focale

Lorsque les patrons de l'ANSSI en France[5] ou du NCSC en Suisse[6] informent certaines entités exposées aux cyberrisques, leur comportement indifférent et irresponsable – alors qu'ils sont assis sur des bombes – laisse songeur.

Récemment, un entrepreneur alerté à deux reprises pour sa vulnérabilité a ainsi répondu: *«je n'ai pas le temps pour ça»*. La troisième fois c'est lui qui appelait au secours…! Frustrant lorsque des incidents appartiennent à la catégorie apparemment plutôt nombreuse des *«aurait pu facilement être évité»*.



BIO

Gérald Vernez a étudié la géologie, la météorologie et la politique de sécurité. Après une première carrière d'ingénieur et de gestionnaire de risques dans l'industrie, il a rejoint l'état-major général de l'armée suisse en 1996. Il a préparé et entraîné l'état-major de crise de la Confédération pour le passage à l'an 2000 (Y2K), planifié l'organisation du commandement (Command & Control) de l'armée, puis développé le domaine des opérations d'information. Chef d'état-major de l'état-major de conduite de l'armée de 2009 à fin 2010 il a ensuite été directeur adjoint pour l'élaboration de la première stratégie nationale pour la protection de la Suisse contre les cyberrisques avant de devenir en 2013 Délégué du chef de l'armée pour la cyberdéfense puis, dès 2016, Délégué pour la cyberdéfense du Département fédéral de la Défense (DDPS). Depuis 2021 Gérald Vernez dirige la Fondation digiVolution (www.digivolution.swiss), une nouvelle force de réflexion et d'action stratégique.

En Suisse, les entreprises du secteur de l'électricité annonçaient même en 2021 une maturité moyenne de cybersécurité en dessous de 1[7] sur une échelle de 0 à 4. Si le 42ème rang[8] attribué à la Suisse par l'UIT dans son index global 2020 est certainement en partie immérité et dû à l'absence de réponse de la Suisse à son enquête, il apparaît que malgré ses talents de premier plan et ses importants moyens, à maints endroits notre pays peine encore à saisir les enjeux et a besoin d'un vigoureux changement de posture.

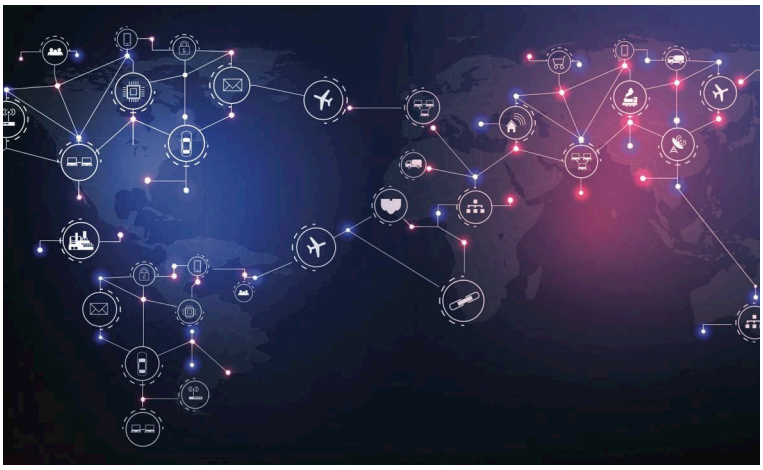
Depuis une quinzaine d'années, avec la cyberattaque contre l'Estonie (2007), celle subie par le secteur nucléaire iranien (Stuxnet, 2010), les révélations de Snowden (2013) ou encore les attaques contre les infrastructures électriques ukrainiennes (2015, 2016), la cybersécurité a considérablement gagné en importance.

Pour l'OTAN et l'Union Européenne un événement grave serait même susceptible de justifier le déclenchement des mécanismes ultimes de défense. Après la terre, la mer, le ciel, les domaines électromagnétique et informationnel et enfin l'espace exo-atmosphérique, les armées rivalisent désormais dans le cyberespace et les commandements cybernétiques se multiplient.

Un développement logique, mais entre toutes ces sphères d'opération, il y a un «*mais*» de taille. En effet, le cyber est la seule dimension présente au cœur de toutes les autres dès leur conception. Considérer donc le cyber sous le seul angle technique, des menaces et

des geeks est à l'évidence réducteur. Sa focale doit être considérablement élargir.

Il est simple de dire «*je veux une cyberdéfense*», mais de quoi dépend une telle capacité pour être installée et exploitée durablement? De personnel, de matériel, d'infrastructures, de textes de lois, de finances, etc. qui proviennent tous d'une chaîne complexe de capacités, compétences, procédures, etc.



Avec le COVID, la guerre en Ukraine, la dispute américano-chinoise sur les terres rares, les avertissements du ministre suisse de l'Économie quant aux prochaines pénuries d'électricité et les nombreux événements observés durant les 18 derniers mois[9], il est désormais clair que la liste des domaines à prendre en considération pour appréhender correctement et à temps la mutation digitale, ses défis et les mesures pour les maîtriser doit impérativement être élargie.

Le kaléidoscope de la mutation digitale et trois recommandations clés

Les constats qui précèdent (pas de pause chez les malveillants, besoin d'un changement de posture chez les défenseurs et élargir la focale) ont présidé à la création de la fondation *digi*Volution[10] en 2020. Fondée par les membres de l'ancien groupe d'experts qui a forgé la cyberdéfense suisse, cette nouvelle institution à but non lucratif[11] inscrit son action stratégique dans une vision d'idéal et de neutralité au service des décideurs à tous les niveaux. Ainsi est né un observatoire chargé de cartographier tous les éléments de «*l'équation digitale*» de notre monde VUCA[12] et de comprendre

Cartographie © digiVolution

la nature et les interactions complexes de l'ensemble des «*tuiles*» de la figure ci-après, dans une approche holistique, systémique et en réseau.

La méthode de digiVolution se voit aussi dans les petites phrases qui jalonnent son message: «*prepare for the next*», «*quel est le prix de l'inaction et du manque d'anticipation*» ou encore «*notre ambition: des effets sur le terrain. Et vite !*». Derrière ces énoncés se cachent trois recommandations très claires:

- **Anticipation** – Ne pas être prêt à temps alors que toutes les données sont disponibles n'est pas une attitude acceptable; c'est tout simplement de la négligence et en droit suisse[13], c'est d'ordre pénal.
- **Responsabilité** – Dans un monde interdépendant, les risques qu'une entité accepte peuvent entraîner des conséquences pour d'autres; ainsi, une entreprise qui ne se protège pas s'expose à la faillite et à mettre ses employés au chômage.
- **Action** – Les plans et stratégies sont bien entendu nécessaires, mais il s'agit d'abord de mettre en œuvre des mesures de cyberhygiène – simples, disponibles auprès des autorités et des prestataires spécialisés et applicables de suite – et ainsi de créer sans délai des effets mesurables pour la sécurité de tous.

Conclusion

Les États et les grandes entreprises disposent généralement de moyens conséquents pour maîtriser les défis de la mutation digitale, mais ce n'est pas le cas des microentreprises (moins de 10 employés, 90% des entreprises et 25% des emplois en Suisse) et des individus.

Ces catégories ne disposent que rarement du temps, de l'argent et des compétences pour, en plus de tout le reste, s'occuper aussi de cette dimension.

C'est donc aux solutions d'aller à leur rencontre et de leur offrir, vite et à un coût négligeable, l'*empowerment* dont ils ont un urgent besoin. Les «*je n'ai pas le temps pour ça*» doivent disparaître.

Veillons cependant à ce que cela ne se fasse pas via la plateformisation à outrance promue par les géants technologiques et ainsi, de manière irréversible, au détriment des questions cruciales de souveraineté, de l'individu à l'État. ■

1 Ce terme signifie une modification en profondeur et irréversible, comme en biologie lorsque des poissons sont sortis des premiers océans il y a des milliards d'années et changé leurs branchies en poumons pour vivre grâce aux différents gaz qui composent l'atmosphère.
2 https://www.csis.org/analysis/put-chinas-intellectual-property-theft-larger-context
3 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
4 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr
5 https://www.lemagit.fr/actualites/252503454/Anssi-trop-dorganisations-ignorent-les-alertes-qui-leurs-sont-adressees
6 https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/schwachstelle-exchange-server-5.html
7 https://pubdb.bfe.admin.ch/fr/publication/download/10524
8 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
9 digiVolution a constamment assuré un suivi de situation et son analyse. Ces travaux sont disponibles sous https://www.digivolution.swiss/dv-blog/
10 La Fondation (institution sans but lucratif) est un observatoire de l'espace digital au service des décideurs politiques, économiques et académiques, auxquels elle propose analyses, conseils et formations. Elle contribue au dialogue public et politique en Suisse sur le sens et la sécurité de la société digitale.
11 Qui on l'espère fera des émules dans de nombreux pays.
12 https://hbr.org/2014/01/what-vuca-really-means-for-you
13 https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en