

Maîtriser les défis de notre mutation numérique est impératif

Gérald Vernez, fondateur et directeur de la fondation digiVolution¹

Mutation numérique?

De simples commodités pour améliorer le travail, les technologies de l'information et de la communication (TIC) sont devenues le moteur et le cœur incontestés de la mutation numérique. Mutation? Comme en biologie, le changement toujours plus rapide et profond induit sur notre société est irréversible. Un dysfonctionnement majeur de cette dimension dont la société est totalement dépendante entraînerait des conséquences systémiques incalculables. Il est bien loin le temps où le numérique se résumait au PC de bureau et que l'informaticien était relégué dans les sous-sols de l'entreprise et de l'organigramme. La cybersécurité se résumait alors à quelques vagues considérants techniques et n'intéressait quasiment personne. Hautement dynamique, le cyberspace est cependant la résultante de nombreux domaines tels que représentés ci-dessous. Qui veut maîtriser sa «*sécurité au temps de la mutation numérique*» doit désormais disposer de connaissances de base de l'ensemble de ces paramètres et de leurs interactions.



Pour maîtriser cette complexité, **les décideurs** économiques, politiques et académiques doivent comprendre ces enjeux et, autant que possible, en anticiper les développements et les effets. N'attendons-nous pas d'eux, à tous les niveaux, qu'ils disposent de connaissances minimales en matière de droit ou de finances? **Il est grand temps qu'ils maîtrisent également les notions clés de leur environnement numérique et de leur capital immatériel.**

Un horizon qui doit inquiéter

Malgré ses importants moyens, la Suisse compte de multiples retards. Globalement, notre système politique fonctionne encore selon les structures et les schémas hérités de 1848. Notre ambition en tant que nation correspond-elle aux exigences de la mutation

¹ <https://digiolution.swiss/>

numérique? Tout indique le contraire alors que notre pays est l'un des plus menacés d'Europe, à parité avec l'Allemagne, au sujet de laquelle le BITKOM² estime les pertes subies en 2022 en raison des seules cyberattaques s'élevèrent à près de 3.8% de son PIB. Pour la Suisse qui selon Microsoft³ est pareillement touchée, cela signifie aussi de lourdes pertes. Proportionnellement, la Suisse perdrait ainsi près de 30 milliards de francs, six fois le budget de son armée? Cela doit bien entendu être pris avec des pincettes, mais d'ici 2028⁴, la facture mondiale de l'ensemble des besoins sécuritaires dans le cyberspace pourrait dépasser 10% du GDP. Supportable? La Suisse perçoit-elle cette urgence? Et dotte-t-elle sa chaîne de poursuite pénale en conséquence?

Penser en termes stratégiques

Les solutions techniques sont centrales, mais elles ne suffisent plus pour une société qui mute rapidement. Et c'est sans compter la multiplication des coups de boutoir de la fragmentation géopolitique. Chaque entité, de l'individu à l'État, doit comprendre la nature des défis de cette mutation et devenir un acteur de sa sécurité et de celle de la collectivité. Quel automobiliste roulerait sans freins? Cela reviendrait non seulement à se mettre soi-même en danger, mais aussi à imposer ses risques à autrui. Nombreux sont pourtant celles et ceux qui naviguent dans le cyberspace sans aucune sécurité...! Cela doit changer!

Le nouvel office fédéral pour la cybersécurité donne la direction générale et - selon ce que permettent ses moyens limités - peut assister des victimes lors de cyberattaques alors que les cantons sont le plus souvent démunis. **La sécurité et la résilience de la société dépendent donc de l'engagement de chacun, dans une approche de cybersécurité en profondeur qui commence par le principe de précaution et l'empowerment des décideurs.**

dVPedia

Pour concrétiser cette approche, *digiVolution* s'est donnée pour mission de réfléchir à de nouveaux modèles et de proposer des solutions concrètes. Ainsi a été créée la **suite dVPedia** [[lien](#)], un « *service⁵ d'information pour tous* », car la connaissance et la sécurité sont des biens communs auquel tout décideur⁶ doit pouvoir accéder facilement.

Rencontrer des difficultés avec le numérique ou subir des cyberattaques n'est pas honteux. C'est de ne pas y être préparé qui l'est !



² <https://www.bitkom.org/Presse/Presseinformation/Organisierte-Kriminalitaet-greift-verstaerkt-deutsche-Wirtschaft-an#>

³ <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022>

⁴ <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>

⁵ Sur abonnement (modique) pour en assurer la pérennité.

⁶ Rares sont les ceux qui y ont été préparés.