Commentaires sur le Rapport 2021 du Conseil fédéral sur la politique de sécurité

digiVolution
prepare for the next

En bref

Le Rapport du Conseil fédéral sur la politique de sécurité (RAPOLSEC) du 14 avril 2021 est un progrès significatif[1] par rapport aux éditions précédentes et cela est à saluer. Chez *digi*Volution nous estimons cependant que **ce document essentiel pour notre pays peut et doit aller plus loin**. Nous l'avons analysé – sous l'angle de la mutation digitale – et suggérons des mesures et des approches nouvelles, à notre avis impératives.

En résumé, il s'agit de :

- Faire du RAPOLSEC une véritable stratégie dont les mesures soient **contraignantes** pour tous les acteurs concernés ; notre sécurité ne saurait passer après la facilité, le confort et les intérêts particuliers.
- Prendre en compte **tous les défis** susceptibles d'évoluer en dangers ou menaces (approche holistique) et développer les compétences et les capacités en matière de pensée complexe pour identifier et comprendre les mutations en cours, dont celle primordiale du digital (approche systémique).
- Établir des **stratégies en profondeur** (de l'État jusqu'à l'individu), en particulier pour la cybersécurité et la protection des infrastructures vitales[2] ; cela comprend l'imposition aux opérateurs de standards et de sanctions incitatives à la hauteur des risques subis par la société en cas de manquements ainsi que d'importants investissements dans la sécurité des infrastructures et dans la formation.
- Ajouter à nos objectifs stratégiques la **sauvegarde de la souveraineté digitale** et prendre, où cela est nécessaire et possible (pratiquement et financièrement), les mesures idoines en faisant en même temps de la Suisse un champion académique et industriel du digital.
- Rétablir le **principe de précaution**, promouvoir la **culture de l'anticipation** et établir une posture de « **disponibilité permanente et différentiée**» (par secteur) qui sortent la Suisse de son mode attentiste et réactif.
- Définir clairement les **intérêts stratégiques et vitaux de la Suisse**, ce qui doit être réalisé ou protégé dans un délai donné (y.c. les moyens pour mesurer continûment leur degré de réalisation).

[1] À l'exception de la qualité rédactionnelle juste passable de la traduction en langue française.

[2] Terme impératif parce qu'il signifie « mise en danger de la vie » et qu'il est ainsi plus précis et exclusif que le terme « critique » qui, sans qualificatif, dit tout et rien.

Index

Appréciation générale

La fondation *digi*Volution remercie pour l'opportunité de pouvoir apporter un commentaire au Rapport 2021 de politique de sécurité du Conseil fédéral (RAPOLSEC). Globalement, nous estimons que **ce document représente un progrès significatif par rapport aux précédentes éditions**, en particulier par l'énoncé de mesures pour répondre aux menaces et dangers. Nous estimons cependant que ce rapport **doit être complété et développé afin de mieux tenir compte de l'influence systémique de la mutation digitale**.

Nous avons formulé **six domaines de recommandations** que nous estimons impératifs pour empêcher que le fossé entre le « EST » et le « DOIT » ne devienne irréversible. **Ces recommandations ne sont cependant en aucun cas un appel à « moins de militaire conventionnel », ni non plus une quelconque mise en concurrence entre les domaines de la sécurité.** Les experts de *digi*Volution connaissent parfaitement la nature de l'ensemble des menaces qui pèsent sur la Suisse et ils sont conscients du fait que le temps pour mettre en place les moyens requis dépasse largement celui nécessaire pour que se développent les risques. Et tout porte à croire qu'un conflit majeur pourrait éclater dans un délai proche. **Il n'est donc pas question de seulement « faire mieux », mais surtout de « faire plus »**.

❶ Pour un rapport devenant une stratégie

Sur le fond, nous avons conscience que **ce rapport n'est pas un « livre blanc »** et qu'il représente un consensus entre de nombreux acteurs dont les intérêts sont multiples et souvent même contradictoires. C'est cependant **dans cette forme non contraignante que réside sa principale lacune**. Imposer un nombre de pages à un document aussi important pour l'avenir du Pays (comme cela nous a été rapporté), ne sert qu'à rendre inutilement générique son contenu ; à l'avenir, ce genre d'objectif rédactionnel doit être aboli, car cela ne saurait être une quelconque limite imposée à la conception de la sécurité de la Suisse. **La dégradation continue de la situation géopolitique exige au contraire que la Suisse se rassemble derrière un projet complet, fort et cohérent** qui ne fragmente pas systématiquement, comme c'est le cas aujourd'hui, les mesures en petites tranches diluées sur de nombreuses années.

Nos suggestions – Ce rapport, pièce fondatrice de la politique de sécurité de la Suisse, doit **devenir une véritable stratégie** afin d'établir un lien fort entre les différents instruments, leurs moyens et leur engagement. Une telle stratégie doit définir des directions, des projets et des moyens concrets et **servir de référence contraignante pour tous les acteurs concernés**. Nous suggérons de **réviser la structure des organes responsables de la conception et du pilotage de la politique de sécurité et d'en faire un pôle de compétence permanent** qui ne soit pas qu'un bureau chargé de coordonner périodiquement le RAPOLSEC et d'assurer la gestion des affaires politiques courantes. Dans le contexte de l'évolution de la nature des défis, un **examen de la notion de neutralité et de son applicabilité s'impose aussi, en particulier par rapport à la mutation digitale**.

❷ Pour une approche holistique et systémique

L'analyse du RAPOLSEC indique qu'une approche classique par secteurs (en silo) a prévalu dans son développement. Pourtant la complexification et la dynamisation du monde montrent qu'une telle structure de pensée est devenu inappropriée. Les rapports des précédentes décennies ne sauraient non plus être pris pour exemple dans une sorte de « on a toujours fait comme ça ». L'acronyme VICA est une réalité. Une recherche de l'occurrence des termes qui le composent (Volatile – Incertain – Complexe – Ambigu) ou de l'analyse de leurs conséquences, montre pourtant leur absence. **Ce rapport ne donne ainsi pas à la Suisse l'impulsion nécessaire pour sa sécurité et sa défense du futur**.

Bien que de nombreux termes soient mentionnés, ils ne sont pas approfondis et le texte comprend parfois des énoncés que nous estimons erronés. C'est particulièrement le cas au sujet des disputes technologiques entre Chinois et Occidentaux qui ne peuvent en aucun cas être qualifiées de « chicaneries » ; il s'agit là au contraire d'une course à la suprématie, d'une lutte dont l'issue déterminera les équilibres stratégiques de demain.

Nos suggestions – Le RAPOLSEC doit **prendre en compte tous les facteurs qui renforcent ou affaiblissent la sécurité de la Suisse**. Des domaines tels que l'urbanisation, les ressources minérales, l'énergie, l'eau, la démographie, l'immigration, la culture et les comportements sociaux, l'influence, la formation et la recherche et bien sûr l'évolution du climat ne doivent pas être simplement énoncés ; ils doivent être rigoureusement et systémiquement analysés. Au niveau stratégique, **la Suisse doit développer ses compétences et capacités en pensée complexe, notamment pour identifier et comprendre l'ensemble des mutations en cours**.

❸ Pour une cybersécurité intégrale

L'espace digital représente un changement de paradigme. Trois qualificatifs décrivent la position de la Suisse et de tous les États. Ils sont :

- **dépendants** d'acteurs systémiques privés et publics qui méprisent et menacent leur souveraineté, c'est-à-dire leur capacité à penser, à décider et à agir librement et de façon autonome ;
- **fragilisés** par une explosion des vulnérabilités ; celles-ci sont technologiques (tel que les produits arrivant sur le marché quasiment sans contrôle comme les objets connectés), logistiques (tels que les approvisionnements en ressources et composants clés) et humaines (en termes de pénurie de personnel qualifié ou de fossé intergénérationnel) ;
- **menacés** par un nombre croissant d'acteurs malveillants qui abusent des possibilités de l'espace digital à des fins géopolitiques, criminelles, de manipulation / désinformation ou de surveillance ; la course aux cyberarmements tourne à l'avantage des agresseurs qui n'hésitent pas à frapper les intérêts et services les plus vitaux (privés et publics, hôpitaux compris) et que le cadre politique, légal et éthique insuffisant ne freine pas ; ainsi, avant même d'entrer dans un conflit ouvert qui impacterait l'espace digital, l'estimation des dégâts (rapidement croissants) dépasse déjà largement 1% de notre PIB ; une récente étude allemande parle même de pertes économiques au-delà de 6.6% du PIB.

La cybersécurité évolue rapidement. Initialement tâche verticale de cyberdéfenseurs opposés à des cyberagresseurs, c'est désormais **un phénomène transversal et hautement dynamique**, qu'une approche classique en silo et depuis le haut ne peut plus maîtriser. Les efforts de la Confédération de ces dernières années sont bien sûr à saluer, mais les changements sont lents et leur ampleur correspond de moins en moins aux **enjeux d'une dimension désormais systémique**. **Le fossé entre le « EST » et le « DOIT » se creuse de façon alarmante.**

Le RAPOLSEC (chapitre 4.2.5 : *Accroître la protection contre les cybermenaces*) énumère presque uniquement des mesures au niveau de la Confédération et en termes vagues tels que « *La protection contre les cybermenaces peut être renforcée* ». Pendant ce temps, l'Union Internationale des Télécommunications (UIT) classe la Suisse au 42ème rang des nations en matière de maturité face aux cyberrisques et l'obligation d'annoncer les cyberincidents pour les opérateurs d'infrastructures vitales (OIV) est attendue par le Parlement depuis 2017. Plus grave sont les résultats connus de longue date et désormais publics en matière d'approvisionnement électrique (télécharger le rapport de l'OFEN), l'infrastructure la plus immédiatement vitale ; ce domaine n'atteint pas la note de 1 sur une échelle de 0 à 4 ! **La confiance et l'autocontrôle ont atteint leurs limites**. En matière de santé ou de circulation routière, chacun est responsable et reçoit pour cela une sensibilisation. Sur la route il faut même un permis de conduire et la négligence ou les comportements inadéquats sont sanctionnés par des pénalités parfois lourdes. Mais rien de tout cela dans l'espace digital malgré le potentiel de conséquences graves !

Nos suggestions – En matière de cybersécurité, le périmètre ne doit plus être limité à l'État et aux OIV. Une « **cybersécurité en profondeur** » et des **principes clairs de responsabilité** doivent être instaurés, **jusqu'au niveau de l'individu**. Comme dans la protection de l'espace aérien, le principe de **sauvegarde de la souveraineté digitale** doit être déclaré, appliqué et réalisé dans les domaines où cela est nécessaire et possible, avec des moyens en suffisance. Il faut **imposer aux OIV un standard clair de cybersécurité**, le contrôler et, si besoin, **sanctionner les manquements aux normes à la hauteur des risques vitaux auxquels ils exposent la société**.

❹ Pour une politique d'anticipation et de précaution

L'histoire montre que la Suisse a été systématiquement prise de court par les conflits depuis la guerre franco-allemande de 1870-1871. Récemment, et malgré plusieurs avertissements, notre pays a de nouveau été pris en défaut. Cette fois, par la pandémie, où un récent rapport de l'AEP montre que l'approvisionnement économique du pays a connu de nombreux ratés. Des mesures ordonnées sur la base des enseignements de l'Exercice du réseau national de 2014 (ERNS) n'ont pas été mises en œuvre. On peut légitimement se demander quelle est l'utilité de l'*Organe de détection précoce des crises* de la Chancellerie fédérale, pourquoi la pandémie et le risque de conflit armé sont quasiment absents du rapport de prospective « Perspectives 2030 » de 2014 et pourquoi ce rapport n'a pas encore été mis à jour.

La liste des « pannes » d'anticipation est longue. Les quelques travaux réalisés n'ont pas de suivi systématique. Les expressions telles que « business continuity », « due diligence » ou encore « planification prévisionnelle » sont souvent utilisées, plus rarement appliquées. À l'évidence, la Suisse n'investit pas assez dans l'anticipation et le principe de précaution. La

notion de « supply chain security » est populaire dans les salons, mais que fait-on effectivement pour ne pas, à notre tour, être victimes des cyberattaques comme celles qui viennent de toucher les USA ? Nous constatons à tous les échelons et dans toutes les organisations – récemment même au NCSC – que l'accroissement impératif des ressources en personnel et en moyens financiers au profit de la cybersécurité est freiné, en contradiction avec les discours et les enjeux. En matière de TIC, on sait aussi que d'ici 2026 près de 20% du personnel spécialisé manquera. Les entreprises n'auront alors d'autre choix que de diminuer la qualité de leurs prestations, de renoncer à innover, de déléguer des tâches à l'étranger ou de nouer des alliances qui vont multiplier les dépendances, les risques d'espionnage ou encore d'appropriation par des concurrents.

Le domaine formation, recherche et innovation (FRI) n'est pour ainsi dire pas mentionné dans le RAPOLSEC. Le terme « formation » n'apparaît pas ; le terme « recherche » apparaît 3 fois et « innovation » une seule fois. La sécurité (cyber ou pas) ne se décrète pas et ne s'achète pas sur étagère. Sans efforts significatifs dans les domaine précités, la Suisse ne sera qu'une consommatrice de technologie avec un niveau sans cesse croissant de dépendances et donc de diminution de sa souveraineté.

Nos suggestions – Il faut **revaloriser l'expérience et ceux qui la détiennent** (et si on utilisait les compétences des seniors ?), **rétablir un principe de précaution fort** et **promouvoir une culture de l'anticipation** afin qu'en termes de sécurité nous échangions notre posture réactive contre une posture proactive. Il s'agit ensuite – sur les bases (encore) exceptionnelles dont nous disposons – de **faire de la Suisse un champion académique et industriel du digital** pour elle-même et à la conquête des marchés, à l'exemple d'Israël et de l'Estonie. Ces développements devront être précédés par un **inventaire global et une appréciation des mesures existantes d'anticipation et de prévention**.

❺ Pour un continuum de défense

A la chute du mur de Berlin, le monde occidental a célébré le triomphe de ses idées et l'absence d'alternatives à sa doctrine libérale. Certains intellectuels parlaient même « *de la fin de l'histoire* ». L'ennemi soviétique à genoux, la peur d'une guerre mondiale a cédé la place au mirage des dividendes de la paix. La Suisse a alors taillé dans ses budgets et même risqué de les diviser par deux avant d'imaginer combler son retard militaire en cas de crise par une doctrine de *montée en puissance.* Sollicité par le Parlement en 2009 qui s'inquiétait des conflits pouvant découler de la crise économique, le Conseil fédéral répondait : *« En cas de menace concrète nécessitant la montée en puissance de l'armée, seul le type de la menace permet de décider du genre, de la portée, des coûts et de la durée des mesures à prendre »*.

La doctrine de la Suisse en matière de sécurité est donc avant tout réactive, largement militaire, symétrique et principalement définie par les budgets. Que signifie « menace concrète » dans la réponse ci-dessus ? Dans quelle situation se trouve actuellement la Suisse et dans quel domaine ? De combien de temps dispose-t-elle pour être en mesure d'affronter une crise ? En Suisse, la situation sécuritaire est traditionnellement répartie en trois catégories : « normale », « particulière » et « extraordinaire » qui servent notamment à répartir les compétences entre Confédération, cantons et communes lors de crises. On trouve cette répartition p.ex. dans les « *Instructions de la Chancellerie fédérale sur les mesures organisationnelles à prendre dans l'administration fédérale pour maîtriser les situations particulières*

ou extraordinaires », dans la loi sur les services météorologiques, celle sur les pandémies ou encore sur l'armée. Nous estimons que cette catégorisation induit un puissant biais cognitif, préjudiciable à la mise en place à temps de moyens suffisants.

En cas d'attaque massive dans le cyberespace, combien de temps aurions-nous entre la situation normale et celles particulière et extraordinaire ? Trouverions-nous sur le marché du matériel et du personnel pour combler à temps les failles de nos systèmes ?

Depuis le début des années 2000, de nombreux signaux montrent que les conflictualités évoluent. Deux officiers chinois l'ont formalisé en 1999 déjà dans leur livre « Unrestricted Warfare ». Cette contribution majeure est malheureusement restée largement inconnue en Occident. Elle décrit une doctrine sous le seuil de la guerre, s'attaquant à toutes les composantes de la société pour vaincre l'adversaire stratégiquement et établir une suprématie permanente. Ces principes sont déjà appliqués par certains États (Chine[3] et Russie en tête) et dépassent de loin les visions militaires conventionnelles, dans lesquelles les **effets de multiplication, d'amplification et d'accélération de et par l'espace digital ne sont pas compris**.

La rapide et profonde mutation de notre société cyber-bio-physique alimentée par l'extraordinaire progression technologique des 20 dernières années a considérablement développé le champ des possibles et nous nous trouvons désormais dans un état de conflit permanent, nommé prosaïquement et naïvement de « compétition » par ceux qui relativisent la situation réelle. Dans l'immédiat, pour la Suisse, tout se passe sous le seuil de la guerre, souvent hors du champ militaire et également dans un cadre immatériel. Difficiles à attribuer, ces agressions apparaissent comme inoffensives, car elles se cachent dans une certaine normalité. Pourtant il s'agit bien d'une forme de conflit.

Nos suggestions – Abandonner la notion à la mode de « conflit hybride » – d'origine américaine, non définie dans notre corpus doctrinal ni traduite dans nos moyens matériels – qui n'apporte pas de plus-value ; l'étude des conflits montre que tous comportent cette caractéristique et que les belligérants font déjà usage de tous les moyens et des armes du moment pour atteindre leurs objectifs. **Renoncer à la classification *normale*, *particulière* et *extraordinaire* et mettre en place une culture et une posture « de disponibilité permanente et différentiée »** par secteur qui sorte la Suisse du mode attentiste et réactif synonyme de surprise et donc de défaite. **Mettre en place une « défense en profondeur » du pays et de ses infrastructures vitales** (anticipation – détection – protection – adaptation – résilience – défense – restitution d'un état normal – amélioration continue) **où les aspects digitaux sont intégrés de manière transversale**.

❻ Pour la protection des infrastructures vitales

Il y a peu d'années encore, le grand public considérait l'informatique comme quelque chose d'optionnel, un « gadget de plus », une « machine à écrire améliorée », « réservée aux geeks ». Beaucoup regardaient « Star Trek », « 2001, l'Odyssée de l'espace », « Terminator »

[3] La Chine est un *compétiteur* stratégique qui ne partage pas les valeurs universelles que se sont données les nations après la Seconde Guerre mondiale. Ce danger majeur n'est pas abordé dans le RAPOLSEC.

ou « Minority Report » comme des idées irréalistes ou des dystopies. « Cela n'arrivera jamais ! ». Entre-temps, de nombreuses technologies apparues dans ces fictions font désormais partie de notre quotidien et de nombreux développements annoncés par des visionnaires de l'industrie comme Ray Kurzweil ou Bill Gates se matérialisent aussi. L'espace digital est désormais au cœur de la société. Nous vivons une **mutation**, en d'autres termes, **une situation dont nous sommes intrinsèquement et irréversiblement dépendants et dont le défaut entraînerait un effondrement de la société**.

Sans TIC et sans électricité, de nombreux services vitaux (santé, énergie, finance, transports, eau, alimentation, etc.) seraient instantanément indisponibles. La complexité de notre société est telle et ses interdépendances si nombreuses, que nous ne savons pas comment ni combien de temps il nous faudrait pour « rallumer le moteur ». Après quelques jours d'indisponibilité, les dégâts sur la vie et le tissu économique prendraient une tournure sévère, puis dramatique et vraisemblablement irréversible après quelques semaines. Quid des pillages et violences que cela entraînera ? Les images de nos commerces lors du semi-confinement en 2020 ne sont qu'un avant-goût de la panique – amplifiées par les médias sociaux tant qu'ils fonctionnent – et des conséquences qui pourraient suivre. Mais en 2020, le *pronostic vital* de la Suisse n'était pas engagé. L'arrêt des infrastructures et services vitaux aurait une toute autre signification. Et pour les immobiliser, point besoin de « boots on the ground » de la part d'un ennemi aéroterrestre ; mais il viendra plus tard. Il est donc impératif d'agir fermement avant que les dégâts ne soient plus supportables.

Nos suggestions – En plus des mesures suggérées au chiffre 3 (imposer aux OIV un standard clair de cybersécurité, de le contrôler et de sanctionner les manquements à la hauteur des risques vitaux qu'ils font subir à la société), il s'agit de **procéder à une réévaluation des moyens et rôles de l'État ainsi que ceux des OIC dans la défense de ces dernières** qui sont désormais dépassées en termes de compétences et de moyens. **Des investissements clés de l'État doivent être consentis dans le but d'assurer la sécurité et la souveraineté de la Suisse**.

Conclusion

Le RAPOLSEC 2021 est une avancée indéniable par rapport aux précédents. Il comporte cependant d'importantes lacunes et **son caractère de « rapport » ne permet pas d'imposer des mesures concrètes.**

S'agissant du chiffre 3.3, les *objectifs* « […] *constituent des priorités de la politique de sécurité pour ces prochaines années.* », cet énoncé ne définit ni niveau d'ambition ni délai de réalisation. Ces *objectifs* ne définissent pas et ne distribuent pas les rôles nécessaires à leur réalisation. Tout cela s'apparente *in fine* à un « tigre sans dents ».

Globalement, ce rapport montre une **incompréhension des conséquences de la mutation digitale et de son impact transversal et systémique dans tous les domaines de la société**. Le rapport se limite à l'approche régalienne de la politique de sécurité, « top – down » avec ses acteurs historiques et **ne saisit pas la nécessité d'inscrire la sécurité de la Suisse dans la profondeur**. Certaines notions, mises en évidence par une occurrence faible de termes clés (notamment dans le domaine des FRI – Formation, Recherche, Innovation), trahissent un **manque conceptuel de notre politique de sécurité**.

La détection précoce est un objectif clé, mais à la lecture de l'objectif 7 « *renforcer la résilience et la sécurité d'approvisionnement en cas de crises internationales* » on ne réussit pas

à se départir de l'impression que **l'anticipation n'est pas comprise. Les mesures prises « en cas de crise » surviendront toujours trop tard.** Avec l'hyperconnexion et les dépendances qui en découlent, le risque est par ailleurs significatif que les crises deviennent toujours plus des « multicrises » (multidimensionnelles). Les structures de conduite y sont-elles adaptées ? Qu'a-t-on appris du COVID ?

Il ne sera certes pas possible d'éviter toutes les situations de surprise, l'emballement général auquel nous assistons ne faisant que renforcer leur probabilité d'occurrence. Mais il n'est plus admissible que nous soyons, comme dans le cas du COVID, pris de cours dans des domaines pourtant identifiés et pour lesquelles des mesures ont été ordonnées, mais qui restent non réalisées et non contrôlées.

Le terme « futur » n'apparaît qu'à trois reprises dans le document. Cela est cohérent avec le titre de « rapport » du RAPOLSEC, mais cela démontre combien il serait **impératif de donner à ce document une vue vers l'avant** et pour cela de **connaître les intérêts vitaux de la Suisse**.

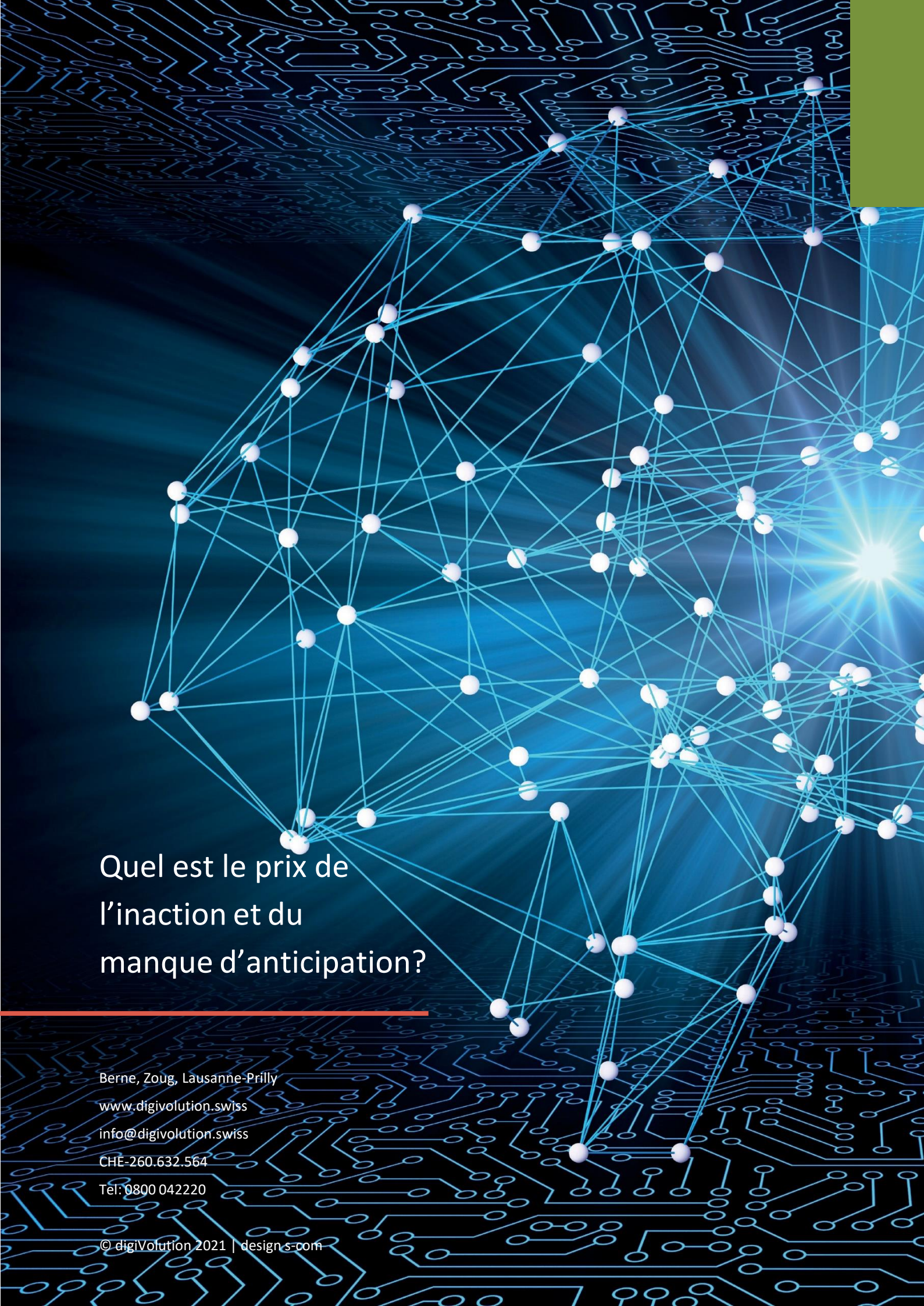
Portrait de la fondation *digi*Volution

« *Sens et sécurité dans une société cyber-bio-physique en mutation* »

Fondée en 2020, *digi*Volution s'est donnée pour mission d'être un **observatoire** de l'espace numérique au service des **décideurs** politiques, économiques et académiques, auxquels elle propose analyses, conseils et formations et de contribuer au **dialogue** public et politique en Suisse en matière de sens et de sécurité de la société digitale.

*digi*Volution veut aider la société suisse à comprendre et à maîtriser les défis multiples et dynamiques de la digitalisation afin qu'elle prenne à temps les bonnes décisions au profit de sa sécurité et de sa prospérité.

*digi*Volution est composée d'experts indépendants et neutres. Leur critique se veut constructive. Leur méthode est holistique, systémique et en réseau et ils considèrent comme clé l'expérience et l'anticipation. Ils pensent dans une perspective stratégique et du temps long. Ils positionnent leur action à la convergence des différences, des générations et des espaces cybernétique, biologique et physique.



Quel est le prix de l'inaction et du manque d'anticipation?

Berne, Zoug, Lausanne-Prilly

www.digivolution.swiss

info@digivolution.swiss

CHE-260.632.564

Tel: 0800 042220