Rapport d'orientation
stratégique 2022

Futurs numériques : incertitudes et *conséquences*

Messages-clés pour les organisations
et leurs directions du numérique
pour 2030-2035

Cigref

Rapport d'orientation stratégique 2022

Cigref
RÉUSSIR LE NUMÉRIQUE

Futurs numériques : incertitudes et *conséquences*

Messages-clés pour les organisations et leurs directions du numérique pour 2030-2035

Nota bene : la rédaction de ce document a été achevée en juillet 2022 et les éléments de contexte relatés sont directement liés à sa période de rédaction.

Avant-propos

En 2020, nous avions identifié cinq champs de transformation afin de qualifier et d'analyser les différentes tendances numériques qui vont façonner notre environnement économique, sécuritaire, social et sociétal, ou encore écologique, à l'horizon d'une quinzaine d'années.

En 2021, nous avons développé quatre scénarios prospectifs pour 2035 pour caractériser les futurs possibles et archétypaux qui pourraient structurer, au cours de la quatrième décennie de ce siècle, l'activité des Etats et des entreprises. Ces scénarios, très contrastés, ont vocation à encadrer ce que sera un futur plausible à cet horizon. Enfin, **cette année**, après une mise à jour des champs de transformation et un ajustement des scénarios, l'essentiel de nos travaux d'orientations stratégiques a consisté à évaluer les conséquences générales de nos analyses prospectives pour nos membres, et plus généralement pour les grands organismes, publics et privés, et leurs directions du numérique. **Nous avons extrait de ces travaux dix messages-clés pour nos lecteurs**. Ils synthétisent les recommandations du Cigref pour se préparer, dès à présent et au cours de cette décennie, à la situation que la conjugaison des évolutions géopolitiques, des mutations technologiques, des transitions énergétiques et des dégradations environnementales ne manquera pas de faire apparaître à l'horizon 2035.

Comme nous l'avions fait l'année dernière avec quatre nouvelles d'anticipation que leurs auteurs avaient écrites pour illustrer les scénarios prospectifs, nous avons demandé cette année à un artiste d'interpréter dans son univers graphique ce que lui inspiraient les cinq champs de transformation numérique et les quatre scénarios prospectifs. Je remercie Vincent Roland qui a mis son talent au service de notre rapport d'orientation stratégique 2022. Ses illustrations permettent de faire passer un souffle d'air frais sur ce travail parfois aride et, nous l'espérons, de stimuler la réflexion et la curiosité du lecteur.

Bien qu'il s'agisse de prospective, nous qualifions le document présenté ici de « rapport d'orientation stratégique », parce que c'est d'abord à lui que le Cigref se réfère pour déterminer, à fréquence annuelle, sa propre stratégie : en effet, en lançant en 2019 ce premier cycle prospectif et en publiant annuellement ses rapports d'orientation stratégique, le Cigref a poursuivi au moins trois objectifs :

- Le premier consiste à structurer l'activité de son Conseil d'administration en matière de sélection des thématiques développées dans le cadre des travaux d'intelligence collective qu'il organise et anime au profit de ses membres.
- Le deuxième est de fournir à ses membres un cadre méthodologique, enrichi d'une veille active, pour qu'ils puissent développer, au sein de leur organisation, leur propre réflexion prospective et une démarche d'orientation stratégique adaptée à leur secteur d'activité, à la culture de leur organisation ou encore à leur niveau de maturité dans ce domaine.
- Enfin, troisième objectif, et comme le notait déjà Bernard Duverneuil dans son avant-propos de l'édition précédente, la publication régulière de ce Rapport d'orientation stratégique permet d'inscrire le Cigref dans le paysage des cercles de réflexion où se développe une pensée originale et structurée sur les enjeux numériques et leur devenir.

En publiant cette **édition 2022** *de son* **Rapport d'orientation stratégique, le Cigref achève le premier cycle de trois ans de ses travaux prospectifs** *menés avec le soutien de* **Futuribles.**

Cette démarche d'orientation stratégique témoigne de la richesse des échanges qui font du Cigref un lieu précieux de débat et d'élaboration collective : elle repose d'abord sur l'engagement du Conseil d'administration à la piloter et l'entretenir dans la durée, en lui accordant les moyens nécessaires, au profit des membres du Cigref. Elle se nourrit ensuite de l'engagement et de la pertinence des travaux du Conseil d'orientation stratégique du Cigref, composé, à parité, de représentants de membres du Cigref, pour la plupart directeurs des systèmes d'information de grands groupes, et de personnalités qualifiées représentant, dans leur diversité, différentes sensibilités de l'écosystème numérique. Elle prend forme enfin grâce à l'implication remarquable de l'équipe des permanents du Cigref et de celle de notre partenaire Futuribles. Ce sont eux les artisans motivés, patients, attentifs et rigoureux de cette démarche, et je les en remercie.

Nous allons nécessairement poursuivre ces travaux qui cadencent désormais, sur un rythme annuel, l'activité du Cigref. Nous les poursuivrons avec une ambition renforcée suivant trois axes.

- Tout d'abord, nous souhaitons contribuer au développement de la culture de la prospective en entreprise, notamment dans les directions du numérique. La méthode de raisonnement prospectif offre aux dirigeants et aux décideurs une palette d'outils remarquables pour s'orienter dans un monde d'incertitude, et propose une alternative crédible et autonome au prêt-à-penser *mainstream* parfois proposé par de grands cabinets de conseil réputés « sachants » dans le domaine du numérique.
- Ensuite, nous souhaitons renforcer l'implication de nos adhérents au sein des ateliers prospectifs que nous animons au cours de l'année pour enrichir davantage encore la réflexion collective du Cigref. Le Rapport d'orientation stratégique du Cigref est un exercice d'intelligence collective à part entière qui se nourrit de l'expertise des adhérents du Cigref.
- Enfin, nous souhaiterions que ce rapport puisse devenir le support d'un dialogue fructueux avec les organisations professionnelles qui développent elles-mêmes une démarche prospective. Nous avons eu l'opportunité de partager la nôtre avec l'Institut de l'entreprise, dans le cadre de ses travaux intitulés « l'Entreprise Full-RSE à l'horizon 2030 ». Cette expérience s'est avérée particulièrement stimulante et riche d'enseignements. D'autres réflexions du même type sont actuellement conduites sur la sécurité numérique dans l'environnement du Campus cyber, dont le Cigref est partenaire. Nous sommes disposés à participer à des regards croisés de ce type sur d'autres thématiques.

Au nom du Conseil d'administration du Cigref et de toute l'équipe rédactrice, je vous souhaite une excellente lecture de ce nouveau Rapport d'orientation stratégique du Cigref. Vos remarques, vos suggestions, vos commentaires, amis lecteurs, seront les bienvenus car ils permettront d'améliorer et d'enrichir ses éditions ultérieures. Notre démarche prospective sort confortée de cette période de troubles successifs qui ont secoué l'ordre mondial au cours de ces dernières années, entre la crise sanitaire de la COVID-19, l'accélération du dérèglement climatique, la croissance de l'insécurité dans l'espace numérique, la guerre en Ukraine, ou encore le retour de l'inflation. Puisse-t-elle être un instrument au service du numérique durable, responsable et de confiance que nous voulons bâtir pour demain !

Jean-Claude Laroche
Président du Cigref

Executive Summary

Le Rapport d'Orientation Stratégique 2022 du Cigref s'inscrit dans la lignée des ROS 2020 et 2021. En ce sens, ce document est, simultanément, le prolongement des rapports précédents et une brique supplémentaire apportée à la réflexion stratégique du Cigref pour définir ses activités et son plan de travail. Aussi s'articule-t-il autour de trois parties complémentaires : les deux premières constituées respectivement de la veille prospective et d'une actualisation des scénarios pour les futurs numériques, puis une troisième présentant dix messages-clés à destination des organisations pour s'adapter aux futurs numériques.

La veille prospective et les scénarios ont été illustrés par des créations originales produites par M. Vincent Roland. Ces œuvres ont pour ambition de stimuler les imaginaires de nos lecteurs, pour se plonger dans les futurs numériques possibles proposés dans le ROS.

PARTIE 1.
VEILLE PROSPECTIVE

Cette première partie déroule une veille prospective sur les cinq grands champs de transformation du numérique identifiés dans le premier rapport d'orientation stratégique publié en octobre 2020. Ils permettent de concentrer la réflexion poursuivie ici sur cinq thématiques-clés couvrant largement les différentes facettes du numérique et identifiant leurs divers enjeux. Ces champs de veille ne sont pas exhaustifs mais ils proposent une réflexion transversale sur le numérique pour nourrir les travaux du Cigref, ainsi que pour renseigner ses membres sur les évolutions majeures auxquelles ils doivent se préparer. Chacun de ces champs thématiques a été actualisé en 2021 puis en 2022. Là encore, cette actualisation, loin d'être exhaustive, s'appuie néanmoins sur une veille rigoureuse ainsi que sur des entretiens avec les experts membres du Comité d'Orientation Stratégique. Elle cherche à rendre compte des préoccupations principales des membres du Cigref pour les 10-15 ans à venir. En voici les grandes lignes.

CHAMP 1. ENJEUX TECHNOLOGIQUES ET NOUVEAUX USAGES

Le déploiement de la technologie cloud au sein des organisations se poursuit progressivement, de même que celui des réseaux et infrastructures 5G à travers l'Europe, même si ce dernier demeure moins rapide qu'escompté. À l'inverse, les efforts de R&D sur l'informatique quantique se sont, eux, fortement renforcés, à tel point que les premières applications concrètes devraient arriver plus vite que prévu, dès 2030. En parallèle, l'UE cherche à réguler l'espace numérique notamment en proposant d'encadrer les usages de l'intelligence artificielle. Mais d'autres technologies potentiellement révolutionnaires, les NFT et les métavers par exemple, ont fait leur apparition (ou réapparition) et suscitent de nombreux questionnements, notamment en termes de législation. Enfin, cette hyper-technologisation croissante de la société, accélérée par la crise sanitaire, suscite de plus en plus de mouvements de résistance.

CHAMP 2. NUMÉRIQUE ET ENVIRONNEMENT

Face à l'urgence climatique encore mise en exergue dans les récentes publications du GIEC, la capacité des organisations à maîtriser leur empreinte environnementale devient primordiale. Les technologies sont consommatrices d'énergie et de ressources rares mais sont aussi porteuses de solutions pour piloter plus efficacement la transition écologique. Les organisations se préoccupent davantage de ces enjeux et les incluent dans leur politique RSE, sous l'égide d'initiatives européennes et du gouvernement français, en avance sur le sujet grâce à la promulgation de la loi REEN en novembre 2021. La notion de responsabilité numérique s'étend également aux enjeux d'accessibilité du numérique au sein de la société.

CHAMP 3. RISQUES CYBER ET ENJEUX GÉOPOLITIQUES

Alors que le nombre et l'intensité des cyberattaques affectant les organisations publiques comme privées ne décroît pas, ces dernières s'inquiètent de plus en plus de leur capacité à assurer ce risque. Par ailleurs, les enjeux géopolitiques liés au numérique ont particulièrement été étudiés dans ce rapport à l'aune du conflit entre l'Ukraine et la Russie : utilisation du cyberespace comme moyen de pression politique, risques sécuritaires sur les câbles sous-marins et compétition accélérée dans le domaine des satellites basse-orbite. Sont également évoqués le rôle du continent africain face aux enjeux numériques mondiaux et l'évolution de la Chine dans cet espace numérique.

CHAMP 4. FOURNISSEURS ET SERVICES NUMÉRIQUES

La position hégémonique des fournisseurs américains et chinois de services numériques (Google, Microsoft, Amazon...) s'est renforcée à la faveur de nombreuses acquisitions dont le montant a atteint de nouveaux records en 2021. Face à cela, l'Union européenne continue à structurer son corpus réglementaire, pour défendre l'indépendance de ses entreprises et applique les premières sanctions découlant du RGPD. De leur côté, certaines entreprises concluent des partenariats technologiques avec ces géants numériques ou, à l'inverse, renforcent leur politique open-source. Par ailleurs, les gouvernements chinois et américain cherchent à contrôler davantage leurs entreprises numériques, à la fois instruments dans la guerre commerciale qui les oppose, mais aussi sujets d'inquiétude du fait de leur puissance croissante.

CHAMP 5. NOUVELLES FORMES DE TRAVAIL ET ENGAGEMENT DES COLLABORATEURS

La pénurie de talents dans le domaine numérique est une tendance lourde. Elle profite à une catégorie de travailleurs qui exigent des salaires de plus en plus importants. Cette pénurie, conséquence d'un manque de formations adéquates, est particulièrement prégnante en France et en Allemagne. Cette situation a un impact sur les organisations, qui sont appelées à innover dans leurs méthodes de recrutement pour attirer davantage de candidats. D'un autre côté, elles doivent faire face à une nouvelle génération de travailleurs qui recherchent davantage de sens dans leur travail et un meilleur équilibre entre vie professionnelle et privée. La démocratisation du télétravail entraîne des conséquences durables sur la gestion du parc immobilier d'entreprise et fait le succès des espaces de coworking. D'autres tendances font également leur apparition pour repenser les formes de travail, telles que l'expérimentation de la semaine de quatre jours dans plusieurs pays et entreprises européennes.

PARTIE 2. ACTUALISATION DES SCÉNARIOS SUR LES FUTURS NUMÉRIQUES

Intimement liée à la veille prospective, la seconde partie de ce rapport propose quatre scénarios, établis en 2021, sur les futurs numériques à horizon 2030-2035. Ces scénarios ont été actualisés à la lumière des récents événements et nous apparaissent toujours robustes. Ils présentent quelques archétypes de trajectoires possibles pour l'Europe et le monde dans la décennie à venir, avec un focus sur les enjeux numériques. Ils ont été construits grâce aux éléments identifiés dans la veille, articulés de manière cohérente et vraisemblable suivant deux axes : l'évolution du leadership mondial et l'évolution du paysage numérique (jeux d'acteurs, régulations…) à horizon 2035. Bien sûr, d'autres configurations seraient envisageables. Mais les figures de l'avenir proposées ici permettent d'encadrer la réflexion sur les futurs grands enjeux des 10-15 prochaines années. Avant de présenter ces scénarios actualisés, cette partie propose aussi une synthèse des grandes incertitudes auxquelles les organisations sont aujourd'hui confrontées.

LES NOUVELLES INCERTITUDES À HORIZON 2035

La guerre déclenchée par la Russie en Ukraine en février 2022 est venue brutalement rebattre les cartes géopolitiques et géoéconomiques des dix prochaines années et interroge sur le futur de la Russie, la constitution de nouvelles alliances mondiales, les conséquences du conflit sur l'UE et les chaînes d'approvisionnement. À ces interrogations, s'ajoutent d'autres incertitudes à horizon 2030-2035 concernant le futur de la Chine, le rôle et le poids des États émergents et l'avenir des méga-projets numériques.

SCÉNARIO 1. MONDIALISATION RÉGULÉE PAR LES ÉQUILIBRES GÉOPOLITIQUES

Le premier scénario fait le pari d'un monde où la crise sanitaire, mais surtout la guerre qui a opposé la Russie et l'Ukraine, aura servi de déclic et de prise de conscience pour les États comme pour leur population de la nécessité de mettre en place de nouveaux outils internationaux de régulation. Les interdépendances économiques favoriseraient une logique de jeux d'influence et de soft power, au détriment d'un conflit armé.

Attention toutefois, le conflit en Ukraine a bien renforcé une logique de coopération internationale face à la Russie mais il est aussi révélateur de l'échec des institutions internationales et des puissances mondiales à réguler les conflits et à les endiguer.

SCÉNARIO 2. VERS UNE « EUROPE PUISSANCE » DANS UN MONDE RÉGIONALISÉ

Dans ce scénario, les échanges économiques et les systèmes de normes (sanitaires, juridiques, commerciales…) se restructurent à l'échelle de grandes plaques régionales. Cette régionalisation des rapports de force et des relations économiques résulte de profondes divergences entre États, révélées notamment par la guerre en Ukraine, mais aussi par les répercussions de long-terme de la crise sanitaire Covid-19 et les impacts disparates du réchauffement climatique sur les pays.

Aujourd'hui, cette régionalisation du monde apparaît renforcée du fait d'une gestion désynchronisée de la crise Covid au niveau international, et des réactions étatiques face à l'invasion russe en Ukraine entre soutien, neutralité et condamnation. Parallèlement, l'Europe investit dans des ressources stratégiques et consolide son appareil législatif pour préserver son indépendance.

SCÉNARIO 3. UNE CHINE CONQUÉRANTE DANS UN MONDE BIPOLAIRE

Ce scénario illustre une trajectoire dans laquelle la Chine parvient à s'affirmer comme leader des échanges internationaux. Profitant d'un contexte de multiplication des crises, la Chine a su tirer parti de la guerre en Ukraine, en renforçant ses liens avec une Russie affaiblie. Cette montée en puissance accélérée de la Chine exacerbe les tensions avec les États-Unis. Ce bras de fer oblige de nombreux pays du monde à choisir leur camp. Divisée et fragilisée, l'Europe n'affirme pas sa « troisième voie ».

De fait, la scission internationale provoquée par la guerre Russie-Ukraine pourrait profiter à la Chine, en particulier si l'Europe peinait à structurer une défense commune.

SCÉNARIO 4. FAR WEST, COLONIES DIGITALES ET CARTELS NUMÉRIQUES

Ce dernier scénario propose une immersion dans un environnement dégradé, fragilisé par la crise sanitaire puis par le conflit entre la Russie et l'Ukraine qui a éclaté aux portes de l'Europe. Très fragilisés par leur endettement, de nombreux États ne sont plus en mesure d'y faire face. Les géants du numérique, relativement préservés par la crise économique et dotés d'immenses capitaux financiers, profitent alors de cette situation pour s'imposer comme partenaires privilégiés pour les pays et les entreprises en Europe, et étendent même leurs services pour remplir certaines fonctions régaliennes des États.

PARTIE 3. MESSAGES-CLÉS POUR LES ORGANISATIONS ET LEURS DIRECTIONS DU NUMÉRIQUE

Cette année encore, le Cigref a innové pour sa nouvelle édition du ROS, rapport qui s'inscrit dans un processus de réflexion continue, pour lier recherche prospective et actions concrètes. Ainsi, afin d'inscrire plus encore les travaux prospectifs ainsi réalisés au cœur des réflexions stratégiques des membres de l'association, des ateliers d'immersion leur ont été proposés pour chacun des scénarios. Ces ateliers, dont la méthodologie plus détaillée est présentée en annexe, ont permis, en sus des deux parties précédentes, de stabiliser dix messages-clés pour les directions du numérique des entreprises et organismes publics. Ces messages-clés ont pour ambition d'aider ces directions à se préparer aux transformations à venir. Les partager fait donc partie de la mission d'intérêt général que s'est fixée le Cigref dans le domaine numérique.

1. D'ici 2035, les directions du numérique des organisations ne devront plus simplement se préparer aux crises mais à leur enchaînement, voire à leur conjonction.

2. Dans ce contexte, les directions du numérique pourraient avoir à réinventer leur système de gestion des risques, dont leurs systèmes de protection face aux cyberattaques et aux risques hybrides, si les assurances traditionnelles ne sont plus en mesure de couvrir ces risques.

3. D'ici 2035, les organisations et leurs directions du numérique seront de plus en plus partie prenante des systèmes de sécurité des États en temps de crise.

4. D'ici 2035, les directions du numérique des organisations devront s'adapter à la régionalisation des normes, des réglementations et des chaînes de valeur. Cette régionalisation aura des impacts sur l'accessibilité des matières premières, le développement des infrastructures numériques et la gestion des bases de données.

5. D'ici 2035, les directions du numérique devront de plus en plus pondérer leurs choix d'investissements technologiques avec des critères tant environnementaux que de maîtrise des dépendances stratégiques.

6. L'arrivée de l'informatique quantique, plus rapidement que prévu, et celle des métavers font partie des grandes ruptures conceptuelles envisageables dans les 10 prochaines années que les directions du numérique peuvent anticiper et auxquelles elles doivent donc se préparer.

7. D'ici 2035, les directions du numérique devront gérer la pénurie de talents en Europe mais aussi dans les pays émergents.

8. D'ici 2035, les directions du numérique devront être des parties prenantes croissantes de l'engagement RSE des organisations, à la demande tant des collaborateurs que des clients et seront redevables devant les actionnaires et la direction générale.

9 D'ici 2035, les directions du numérique pourront être de plus en plus confrontées à des mouvements de résistance internes et sociétaux contre la tendance à l'hyper-technologisation.

10. D'ici 2035, la forte composante géopolitique et stratégique du numérique et sa contribution croissante à la performance économique de l'entreprise conduira à réévaluer le positionnement des directions du numérique au sein de la direction générale.

Note de contexte

De la même façon que nous nous y sommes prêtés dans les éditions précédentes, cette note de contexte introduit les travaux prospectifs du Cigref présentés dans ce rapport d'orientation stratégique 2022. Elle permet de dresser un panorama aussi factuel que possible de la situation générale dans laquelle ce rapport a été rédigé, en juillet 2022. Cette note de contexte s'avère d'autant plus nécessaire que cette situation a considérablement évolué depuis l'été 2021, le paysage géopolitique, politique, économique, social, sanitaire et environnemental s'étant transformé de manière inédite en France, en Europe et dans le monde.

Cette note de contexte, comme l'année précédente, se compose de deux parties principales, la première consacrée à une analyse synthétique de la situation géopolitique globale, la seconde plus spécifiquement consacrée aux différents enjeux numériques tels qu'ils se présentent à ce jour pour les membres de notre association. Il est bien entendu nécessaire d'entourer notre propos de quelques précautions d'usage, notamment sur le caractère non exhaustif de nos observations. Nous ne prétendons pas, en effet, à une description complète de la situation, mais nous souhaitons rappeler les principaux faits saillants qui structurent l'actualité en cette période où nous bouclons nos travaux prospectifs, avant de les sceller sur le marbre de l'imprimeur.

CONTEXTE GLOBAL

Si la crise sanitaire de la COVID-19, l'augmentation des effets visibles du changement climatique et la rivalité croissante entre les Etats-Unis et la Chine, pour ne prendre que ces trois facteurs géostratégiques, n'avaient suffi, la Russie a relégué toutes nos velléités naissantes à l'optimisme qui pouvait poindre au tout début de l'année 2022. Depuis le 24 février de cette année, le déclenchement par les forces russes, massées depuis des mois à la frontière entre les deux pays, d'une guerre de haute intensité contre l'Ukraine, a engendré de multiples conséquences de nature géopolitique et économique. Depuis maintenant cinq mois, ce conflit, qui se développe aux portes de l'Europe, aura agi comme un accélérateur des recompositions géopolitiques, et comme un frein brutal à la reprise économique qui s'annonçait en fin d'année dernière, après les effets récessifs de la crise sanitaire de la COVID-19.

Le conflit en Ukraine

C'est le fait majeur de ces douze derniers mois. La guerre de haute intensité, menée par la Russie de Vladimir Poutine contre l'Ukraine, semble devoir s'installer dans la durée. A la détermination russe de prendre le contrôle total des oblasts de Lougansk et de Donetsk à l'Est, et probablement du Sud de l'Ukraine afin d'établir un continuum territorial depuis le Donbass jusqu'à la Transnistrie occupée, s'oppose la résistance acharnée des forces ukrainiennes soutenue en matériels et équipements militaires, mais également en renseignement, par les nations occidentales, Etats-Unis en tête. Il semble que le nouvel horizon stratégique de la Russie consiste à couper l'Ukraine de tout accès à la Mer noire, en prenant notamment le port d'Odessa. Actuellement, **un peu plus de 20% du territoire de l'Ukraine échappe désormais au contrôle de Kiev**.

Ce conflit, s'il ne dégénère pas dans une déflagration généralisée peu probable à ce stade, trouvera un terme dans le cadre d'**un processus diplomatique et des négociations de paix entre l'Ukraine et la Russie**. La géographie étant têtue, tout autant que la culture russe en matière stratégique, des concessions paraissent inévitables, tant en termes territoriaux et de contrôle par la Russie de certaines zones comme la Crimée, que sur le statut de l'Ukraine vis-à-vis du monde occidental et plus particulièrement de l'OTAN. Dans la perspective de telles négociations de paix, la Russie semble s'engager dans une guerre d'usure afin de consolider ses positions et ses gains territoriaux, alors que l'Ukraine, confrontée à d'importantes pertes humaines, à des destructions massives de ses infrastructures et à des difficultés pour régénérer ses forces militaires, peine à contenir l'avancée russe.

Ce conflit marque un véritable tournant et modifie profondément le paysage géopolitique mondial. Pour la Russie la désillusion est immense, et l'histoire sera probablement sévère envers les responsables politiques de ce gâchis stratégique, mal préparé et mal engagé. L'Ukraine, malgré ses pertes territoriales, se sera définitivement détachée de son « grand frère » russe et de son modèle autoritaire et conservateur, pour se jeter d'abord dans les bras du libéralisme démocratique de l'Union européenne, qui lui a ouvert son processus d'adhésion, et probablement ensuite dans ceux du système de sécurité de l'OTAN.

À la faveur de ce conflit, l'Occident, après la sidération provoquée par ce retour brutal du tragique sur le continent européen, avec son cortège de milliers de morts et de millions de déplacés, a fait la démonstration d'une unité inédite. **L'Union européenne a adopté toute une série de sanctions à l'égard de la Russie et de sa classe dirigeante**, et tente de mutualiser les douloureuses conséquences énergétiques du conflit, alors que la question de l'acceptabilité des effets économiques du conflit sur les citoyens européens commence à se poser. L'OTAN, quant à elle, est sortie de son état de « mort cérébrale », selon l'expression sévère d'Emmanuel Macron en novembre 2021. Elle renforce ses capacités d'intervention à l'Est de l'Europe, et s'élargit à la Suède et à la Finlande, transformant de facto la mer Baltique en lac otanien, ce qui constitue un autre choc stratégique pour la Russie après des décennies de neutralité de ces deux nations scandinaves.

La communauté internationale, si ce concept conserve quelque pertinence, reste cependant profondément divisée face à l'agression caractérisée de la Russie envers l'Ukraine. Le 2 mars 2022, l'Assemblée générale des Nations unies adoptait, après deux jours de débats, une résolution qui « *exige que la Russie cesse immédiatement de recourir à la force contre l'Ukraine* », lors d'un vote approuvé massivement par 141 pays, sur les 193 membres que compte l'organisation. Cinq s'y sont opposés, dont évidemment la Russie et la Biélorussie, mais aussi la Corée du Nord, l'Erythrée et la Syrie. Et trente-cinq, dont la Chine, se sont abstenus. Au total, entre oppositions et abstention, les représentants de plus des deux tiers de la population mondiale n'ont pas soutenu cette résolution.

La situation en Chine

Derrière le rideau, le Chinois Xi-Jinping observe le théâtre géopolitique avec circonspection, et s'en tient pour le moment à l'écart. S'il est attentif à la situation, il maintient une prudente relation avec une Russie affaiblie qui recherche de manière urgente et vitale de nouvelles alliances stratégiques et commerciales.

Xi-Jinping est en effet confronté à plusieurs difficultés que le conflit en Ukraine n'aide pas à résoudre. La première difficulté tient aux **dysfonctionnements du modèle économique chinois** qu'il a mis en place à partir de 2013. Son intention était de recentrer l'économie chinoise sur son marché intérieur. La consommation chinoise n'ayant pas réellement décollé, c'est le secteur de l'immobilier qui a tenté de prendre le relais. Au cours du dernier trimestre de l'année 2021, la bulle immobilière chinoise a éclaté et le secteur a enregistré de nombreuses faillites. Le recentrage de la croissance chinoise sur son marché intérieur n'a pas bien fonctionné.

La deuxième difficulté pour Xi-Jinping, c'est la rigidité de **sa stratégie zéro COVID**, poursuivie de manière assez dogmatique. Cette stratégie, appliquée sans ménagement, notamment dans une ville comme Shanghai, se traduit par un ralentissement important de l'activité industrielle chinoise. On a constaté, au mois d'avril 2022, une baisse spectaculaire de 11% de la consommation sur un an.

La troisième difficulté est la conséquence des deux premières. Xi-Jinping est confronté à de **nombreuses dissensions politiques** qui se développent dans l'attente du congrès du parti communiste chinois qui doit se tenir au cours de l'automne prochain. La réélection probable de Xi-Jinping s'accompagne de tensions qui obèrent la capacité de la Chine à prendre les mesures nécessaires pour maintenir, voire restaurer, sa compétitivité et la croissance de son économie.

La quatrième difficulté pour Xi-Jinping est de nature démographique. Si le défi démographique auquel la Chine est confrontée est bien connu, et depuis longtemps, **le vieillissement de la population** est clairement plus rapide que prévu. La triple hausse du coût de la vie, du logement et de l'éducation des enfants, conjuguée à l'impact du COVID 19, sont de puissants freins à la natalité, malgré les assouplissements successifs de la politique de natalité ces dernières années, autorisant les couples à avoir deux enfants depuis 2016 puis trois depuis 2021. Les démographes estiment que la part de la population en âge de travailler pourrait être réduite de moitié entre 2021 et 2050.

Enfin, cinquième difficulté, **la situation internationale n'est pas favorable pour l'économie chinoise**, principalement en raison du choc énergétique amplifié par le conflit en Ukraine et les sanctions internationales à l'encontre de la Russie. Dans ce contexte, les exportations chinoises diminuent de façon significative. Ce ralentissement de l'économie chinoise est du reste très pénalisant pour l'économie européenne. Il provoque des ruptures sur les chaînes d'approvisionnement de certaines de nos industries, comme celle de l'automobile. Les effets ont été perceptibles dès le mois d'avril 2022. Malgré un rebond des exportations chinoises au mois de juin 2022, consécutif à la levée des restrictions sanitaires à Shanghai, celles-ci pourraient cependant entrer dans une période plus longue de stagnation en raison des menaces de récession aux Etats-Unis et en Europe. Les conséquences pour Xi-Jinping sont sévères. L'économie chinoise n'atteindra probablement pas le seuil de 5,5% de croissance prévu par le Gouvernement pour 2022, seuil en dessous duquel la stabilité sociale de l'Empire du milieu est considérée comme compromise.

De fait, il semble bien que, sous l'impulsion de Xi-Jinping, la Chine ait inversé ses objectifs prioritaires. Au plan intérieur, la Chine est passée de la primauté accordée à l'enrichissement de la population à celle donnée, de façon de plus en plus rigide, au contrôle politique et social de celle-ci. Au plan extérieur, la Chine affirme sa puissance géopolitique, diplomatique et militaire, quelles qu'en puissent être les conséquences sur ses relations économiques avec le monde occidental. L'exemple de Hong Kong, et de l'affaiblissement de sa place financière, est emblématique de cette évolution du pouvoir chinois, et fait craindre le pire pour Taïwan.

La situation aux Etats-Unis

Sur le devant de la scène internationale, l'Amérique de Joe Biden tente, depuis son arrivée au pouvoir en janvier 2021, un retour vers une version plus classique, et plus ouverte, de son leadership. La première puissance mondiale ne laisse pas cependant d'interroger quant à **sa capacité à maintenir, dans le temps long, ce leadership**. Certes, l'Amérique demeure, sans contestation, la première puissance militaire au monde, et son économie reste encore la première devant celle de la Chine. Mais les profondes fractures de son corps social exacerbent autant les conservatismes les plus débridés que les progressismes les plus excessifs.

Si leur **déclin relatif, tant culturel qu'économique, engagé depuis deux décennies au moins**, devient de plus en plus visible, les Etats-Unis semblent dans l'incapacité d'analyser ce phénomène et d'en tirer des conclusions de nature politique. Ainsi, la richesse produite par les États-Unis qui était 22 fois plus importante que celle produite par la Chine en 1960 ne l'est plus que d'1,3 fois à peine en 2020. Par ailleurs, depuis la chute de l'Union soviétique en 1991, les Etats-Unis ont vécu dans l'illusion d'être l'unique hyperpuissance dans un monde unipolaire, et disposant du pouvoir de façonner le reste du monde à leur image. Cette illusion s'est définitivement évanouie dans la débâcle de l'évacuation internationale d'Afghanistan, engagée le 15 août 2021 après la prise de Kaboul par les talibans.

À l'image du marin de Sénèque pour lequel il n'y a pas de vent favorable s'il ne sait où aller, l'Amérique donne le sentiment d'une nation dont la boussole de la raison et de la décence commune montrerait des signes de faiblesse. Son déclin relatif n'ayant pas encore été identifié et analysé comme tel, et sa société se lézardant de multiples fractures politiques, **le risque de changements brutaux de cap tous les quatre ans devient une éventualité inquiétante**. A l'heure actuelle, l'hypothèse de la reconquête en 2024 de la Maison-Blanche par un Donald Trump toujours plus décomplexé, ou, s'il n'est lui-même empêché par ses démêlés judiciaires, par l'un de ses proches alliés, apparaît, si ce n'est probable, à tout le moins plausible.

Cependant, face à la menace que la Russie fait peser sur la sécurité et la stabilité en Europe, et en soutien de ses alliés, l'Amérique conserve une capacité sans équivalent de mobilisation militaire. Les États-Unis renforcent partout en Europe leurs forces stationnées et déploient, au profit de l'Ukraine, des aides financières et des équipements militaires déterminants pour l'issue du conflit.

La situation en Europe

L'Europe, jusqu'à présent cantonnée dans un rôle de spectatrice de la scène internationale, sort quant-à-elle de sa torpeur stratégique et de ses illusions sur le pouvoir égalisateur de la mondialisation heureuse par le commerce et les échanges. L'Allemagne, notamment, doit admettre sa lourde erreur stratégique avec un Vladimir Poutine qui l'a enfermée dans une dépendance insupportable aux énergies fossiles russes. Alors que les importations en provenance de Russie représentaient, en 2021, environ 45% de la consommation de gaz naturel de l'Union européenne, la Commission propose un plan visant à s'affranchir de la dépendance au gaz russe d'ici 2027. Et au cœur de l'été 2022, les ministres de l'énergie des 27 Etats membres tentent avec la Commission de s'accorder sur un plan de réduction de la consommation d'énergie du continent européen. Les injonctions à la sobriété énergétique, tant pour les acteurs économiques que pour les particuliers, se font de plus en plus pressantes. Triste ironie de l'urgence de la crise énergétique que traverse le continent, le recours à des énergies plus polluantes que le gaz naturel russe, comme le charbon ou les hydrocarbures non conventionnels, est privilégié, notamment en Allemagne et dans une moindre mesure en France.

Cinq mois après le déclenchement de la guerre en Ukraine, et alors que la Commission et les gouvernements européens tentent de se préparer à un arrêt total des livraisons de gaz russe l'hiver prochain, l'onde de choc du conflit continue de se propager à l'ensemble de l'économie du continent. Dans ce **contexte de crise énergétique et de difficultés d'approvisionnement** que connaît l'Europe, son industrie enregistre une baisse sensible d'activité et son secteur des services entre progressivement en récession. Dans ses prévisions économiques de l'été 2022, la Commission européenne estime que la guerre en Ukraine place l'économie du continent sur une trajectoire de croissance plus faible et d'inflation plus élevée encore que ce qui était escompté au printemps dernier, principalement en raison de la hausse des prix de l'énergie et des matières premières alimentaires. Ces facteurs entretiennent les tensions inflationnistes mondiales, érodent le pouvoir d'achat des ménages et suscitent des réactions en matière de politique monétaire et de hausse des taux plus rapides que prévu.

La zone euro est elle-même confrontée au **risque d'une nouvelle crise des dettes publiques**. Le 21 juillet 2022, la Banque centrale européenne a amorcé une hausse de ses taux directeurs pour tenter, conformément à son mandat principal, de contenir l'inflation, tout en prévenant le risque de trajectoires d'emprunt divergentes de chacun des Etats membres. Cette hausse va, en effet, renchérir les taux auxquels les Etats peuvent emprunter, notamment la Grèce, l'Italie, l'Espagne, le Portugal et la France, dont les endettements sont très supérieurs à la moyenne de l'endettement de la zone euro. Cette situation va nécessairement limiter leurs marges de manœuvre pour, d'une part, amortir la baisse du pouvoir d'achat des ménages et les hausses du coût de l'énergie, et d'autre part financer les indispensables transitions qu'appelle, après plusieurs semaines de manifestations caniculaires en Europe, la lutte contre les effets du réchauffement climatique.

Le réchauffement climatique

Le réchauffement climatique, justement, alors que ses conséquences apparaissent jour après jour plus évidentes, place des populations entières et leur environnement naturel dans **des situations de stress caniculaire et hydrique majeur**, dont il est désormais admis, au moins dans le monde occidental, qu'il constitue le défi prioritaire auquel l'humanité est désormais confrontée. Nous aurons, dans les décennies qui viennent, à nous adapter à une situation climatique nouvelle moins favorable au vivant, et à limiter de manière drastique les émissions anthropiques de gaz à effet de serre pour éviter, autant que nous le pourrons, d'aggraver encore la situation.

Que dire du contexte climatique, au cœur de l'été 2022, alors que des feux de forêt inédits, provoqués par une sévère sécheresse et des températures records, ont mobilisé toutes les attentions ? Que dire du contexte climatique, au cœur de l'été 2022, alors que la plupart des Etats européens tentent de sécuriser leurs approvisionnements en gaz naturel et relancent ou intensifient le recours au charbon, en contradiction avec leurs engagements climatiques, pour s'affranchir de l'usage cynique par Vladimir Poutine de l'arme énergétique ? Que dire du contexte climatique, au cœur de l'été 2022, quand les courbes d'émissions de gaz à effet de serre semblent, notamment en Chine, désespérément orientées à la hausse ?

Pourtant, **des efforts concrets ont été réalisés en Europe**. Ainsi, de 1990 à 2020, les Etats membres de l'Union européenne ont réduit de 31% leurs émissions de gaz à effet de serre, au-delà des objectifs que nous nous étions fixés, en partie d'ailleurs en raison des effacements consécutifs à la crise sanitaire. En revanche, au rythme actuel et sans nouveaux dispositifs transitionnels, la réduction des émissions sera de 41% en 2030 par rapport à celles de 1990, bien en-deçà de l'objectif contraignant de 55% fixé par l'Union européenne.

Dans le même temps, **la Chine, premier émetteur mondial de gaz à effet de serre avec environ 27% des émissions, a accéléré en 2022 la mise en service de nouvelles centrales à charbon** pour éviter, selon les autorités chinoises, des pénuries d'électricité. La production d'électricité du pays le plus peuplé de la planète repose encore à 56% sur le charbon, dont on sait le caractère particulièrement nocif pour le climat.

Les limites planétaires et écologiques semblent sonner la fin du dogme, en vigueur sans doute depuis la fin du XVIIIème siècle, et certainement depuis la fin de la Seconde Guerre mondiale, de l'alliance entre croissance économique et progrès social. Alors que les Etats devront continuer à rembourser leurs dettes, à financer la protection sociale et à investir dans la transition écologique, ils sont incités, pour les plus avancés d'entre eux, à explorer de nouvelles voies conciliant prospérité et sobriété, à engager de nouvelles dynamiques de progrès, respectueuses de l'environnement et acceptables par les populations.

CONTEXTE NUMÉRIQUE

Pénurie des compétences

La pénurie croissante de compétences numériques, la difficulté à les recruter et à les fidéliser, la tension extrême sur certaines compétences clés, et la **mondialisation de la guerre des talents**, constituent un champ de préoccupation majeur pour l'ensemble de la filière du numérique. Il y a quelques mois, le dirigeant d'une entreprise de services numériques renonçait à relocaliser en France certaines de ses activités implantées en Inde, en raison des tensions en Europe sur les emplois qualifiés dans la filière numérique, alors même que ces activités ne bénéficient plus aujourd'hui en Inde d'avantage compétitif significatif et pâtissent de cet éloignement géographique.

Dans ce contexte, le **manque de mixité dans les métiers techniques du numérique** et la désaffection des femmes pour ces métiers dits « numérisants » renforce ce phénomène de pénurie. Les femmes ne représentent que 15 % à peine des effectifs des compétences techniques, tant dans l'industrie du numérique que dans les directions des systèmes d'information. Et la situation devrait se détériorer dans les années à venir. En effet, dans l'enseignement supérieur, les femmes représentent tout juste 10% des étudiants des filières de formation aux métiers techniques du numérique. Ce fait démographique est, hélas, têtu. Toutes choses égales par ailleurs, sans action significative, ces chiffres se retrouveront donc inéluctablement dans l'économie à l'horizon d'une quinzaine d'années.

La France et l'Europe ne peuvent se satisfaire, ni du manque d'intérêt de 50 % de la population pour ces métiers d'avenir, ni de ce déterminisme sociétal qui éloigne les filles d'un secteur d'activité si nécessaire à la croissance de l'économie et à la prospérité de notre continent. Il est anormal que les femmes soient si faiblement engagées dans ces métiers indispensables, tant pour répondre aux principaux défis, notamment environnementaux et climatiques, auxquels l'humanité est confrontée, que pour construire et organiser nos futurs numériques. Nous n'avons ni droit moral ni intérêt à laisser cette situation se dégrader encore et encore, au-delà du raisonnable.

Sécurité numérique

La situation sécuritaire dans l'espace numérique est une préoccupation majeure pour toutes les organisations, publiques et privées, qui voient leur surface d'exposition croître de façon quasi-exponentielle, et qui sont confrontées à **une cybercriminalité qui s'est professionnalisée, mondialisée et industrialisée** au cours de ces dernières années. Les principales puissances numériques elles-mêmes, à commencer par les Etats-Unis, la Chine et la Russie, sont au bord du cyber-affrontement, et le conflit en Ukraine a renforcé cette dynamique délétère. La menace est elle-même polymorphe et souvent difficile à cerner, entre activités criminelles, activités d'espionnage et opération de lutte informatique offensive avec des armes logiques. Les acteurs de cette cybermenace agissent bien souvent dans une forme de porosité avec des officines étatiques ou paraétatiques, notamment en Russie, en Iran ou en Corée du Nord, pour ne citer que les plus évidentes.

À ce rythme, si la France et l'Europe ne prennent pas rapidement la mesure du **défi sécuritaire auquel nous sommes collectivement confrontés**, et n'adoptent pas des mesures vigoureuses permettant de changer les paradigmes de la sécurité dans l'espace numérique, nos États, notre économie, nos concitoyens, le fonctionnement même de nos démocraties pourraient être confrontés au chaos numérique à l'horizon de la prochaine décennie. L'espace numérique pourrait devenir un espace de non droit où seuls quelques *happy few* disposeraient des moyens pour y mener leurs activités au sein de *compounds* numériques extrêmement sécurisés. Cette sombre perspective n'est hélas pas qu'une simple hypothèse ou une vue de l'esprit, mais un scénario plausible qui prolonge le caractère exponentiel de la croissance des cybermenaces observée au cours de ces dernières années. La première des obligations des États, en matière de souveraineté numérique, concept vague utilisé ces derniers temps à tout bout de champ, devrait consister à assurer la sécurité des biens et des personnes dans l'espace numérique et la sécurité des activités légales qui s'y déploient, au même titre que dans l'espace physique.

La Commission européenne a annoncé en mars 2022 **une initiative législative, le *Cyber Resilience Act*, pour effacer la singularité de l'industrie du numérique**, seule industrie en Europe à n'être soumise à aucune norme de sécurité contraignante ni à aucune règle prudentielle pour la fabrication de ses produits et services. Pour répondre aux besoins du marché européen et protéger les utilisateurs contre les produits et services non sécurisés, cette initiative vise à fixer des exigences de cybersécurité auxquelles les fabricants et les vendeurs de ces produits et services devront se conformer.

Sobriété numérique

Le numérique représenterait aujourd'hui plus de 4 % des émissions de gaz à effet de serre dans le monde, en forte augmentation au cours des prochaines années, probablement 6 à 8% vers 2025. En premier ordre de grandeur, et pour simplifier, **l'empreinte environnementale du numérique est constituée à 70% par le *hardware* et les infrastructures physiques**, essentiellement pour leur fabrication, à 20% par le fonctionnement des centres de données et du cloud, et à 10% par les usages eux-mêmes.

L'essentiel de l'empreinte environnementale du numérique provenant de la fabrication et de la distribution des équipements informatiques, il n'y a pas d'autre choix pour obtenir un impact significatif sur cette empreinte environnementale que d'**augmenter la durée de vie des équipements et de lutter contre l'obsolescence matérielle**. Pour que l'impact de ce genre de mesure soit significatif, la durée de vie des smartphones, par exemple, qui est de 3 ou 4 ans en moyenne doit passer à 6 ou 8 ans, et celle des ordinateurs passer de 5 ou 6 ans à plus de 10 ans. Par ailleurs, les équipements numériques doivent être conçus pour garantir un recyclage efficace permettant que les équipements d'aujourd'hui constituent la matière première de fabrication des équipements de demain. Enfin, et c'est le plus important, il est indispensable que les fournisseurs de logiciels ne provoquent pas artificiellement l'obsolescence des équipements informatiques, ordinateurs, serveurs et smartphones.

Il est par ailleurs nécessaire d'**améliorer l'efficacité énergétique des *data centers***, sans effets collatéraux sur l'écosystème naturel environnant, et d'éco-concevoir l'ensemble des piles logicielles qui sont déployées dans ces data centers, une telle mesure permettant des gains énergétiques de 30% environ. Enfin, il serait légitime d'imposer aux opérateurs de data centers de fournir une information claire, et à la maille de chaque data center, sur l'intensité carbone de l'énergie primaire qui alimente le réseau électrique auquel chacun d'eux est raccordé, hors stratégies de compensation des émissions de gaz à effet de serre.

Les utilisateurs professionnels de solutions et services numériques ne peuvent, à leur échelle, qu'agir sur une part mineure de l'empreinte environnementale du numérique. L'impact de ces usages doit être mis, par ailleurs, en regard des externalités positives que revêt le numérique en tant qu'**outil d'aide, d'évaluation et de maîtrise de l'empreinte environnementale de l'ensemble des activités de l'entreprise**.

Dans ce contexte, il sera sans doute nécessaire de penser de nouvelles régulations pour contraindre les fabricants d'équipements informatiques et les fournisseurs de services numériques à des exigences de maîtrise de leur empreinte, comme c'est déjà le cas pour d'autres industries, notamment l'industrie automobile. Par ailleurs, dans un contexte de conflit d'usage de la production électrique, il sera sans doute nécessaire de concevoir des arbitrages en fonction de critères d'utilité sociale des services numériques futurs, tels que les métavers.

Maîtrise des dépendances numériques

Dans un rapport publié au début du mois de juillet 2022, la Banque des règlements internationaux, qui se définit elle-même comme la banque des banques centrales, s'inquiète de la dépendance croissante des institutions financières vis-à-vis des fournisseurs de services cloud. La BRI explique que le recours excessif aux services cloud des *hyperscalers*, essentiellement américains et demain chinois, pourrait exacerber les risques opérationnels et générer des vulnérabilités systémiques dans le cas où ces fournisseurs de services feraient face à des dysfonctionnements. Ce diagnostic alarmé, que la BRI pose de manière évidente pour le secteur financier, est également pertinent pour la plupart des autres secteurs d'activité, et pour les Etats eux-mêmes.

Dès lors qu'il s'agit de services critiques, de leurs applications cœur de métier ou de leurs données les plus sensibles, ces stratégies de mouvement vers le cloud renforcent les vulnérabilités des organisations publiques ou privées européennes qui utilisent les services de ces *hyperscalers*. En effet, elles peuvent d'abord faire l'objet d'accès légaux à leurs données les plus sensibles, sans qu'elles n'en soient informées, que permettent plusieurs législations, américaines ou chinoises, à portée extraterritoriale, par exemple pour effectuer du renseignement d'intérêt économique. Elles sont susceptibles, ensuite, de subir un bannissement brutal des services de ces *hyperscalers* si une crise géopolitique survient inopinément entre l'Europe et les Etats-Unis. Elles sont enfin à la merci de modifications substantielles des modèles d'affaires de leurs fournisseurs de services cloud, et d'une captation illégitime de la valeur qu'elles créent sur leur marché, dès lors que leur niveau de dépendance rend extrêmement difficile toute stratégie de sortie.

L'Europe tente depuis plusieurs années de combler ses retards dans l'industrie du cloud, avec des résultats mitigés à ce stade. Elle s'est également engagée dans une stratégie de régulation des principaux *hyperscalers*, notamment américains. A ce titre, l'entrée prochaine en vigueur du *Digital Markets Act*, en principe au premier trimestre de l'année 2023, devrait permettre de détendre les dépendances de l'Europe et de son économie vis-à-vis des fournisseurs de services cloud qui seront qualifiés de *Gatekeepers* au titre de ce règlement.

CONCLUSION

Cette note de contexte est plus longue et dense que nous ne l'avions envisagée initialement, en raison des événements qui ont à nouveau bouleversé, comme le fit en 2020 la crise du SARS-CoV-2, notre horizon stratégique. Confrontés à des temps incertains, les décideurs ont besoin, plus que jamais, d'instruments de navigation, de cartes et de repères. Il est en effet indispensable de connaître sa position initiale, et c'est l'ambition de cette note de contexte, pour tracer sa route et s'orienter vers la direction choisie.

Que retiendrons nous de cette année 2022, dans 10 ou 15 ans, lorsque nous aurons atteint l'horizon de ce travail prospectif ? Qu'avons-nous retenu de la période 2008-2012, à part la crise financière des subprimes, la crise de la dette grecque, l'accident de la centrale nucléaire japonaise de Fukushima, les printemps arabes avec notamment la chute de Kadhafi et l'intervention militaire en Libye sous égide de l'ONU ? Et qu'avons-nous appris de ces événements ? Sans doute beaucoup plus, collectivement, que nous ne sommes en mesure de nous en rendre compte individuellement. Ramasser les événements récents, les passer au tamis, retenir ceux qui semblent porteurs de sens et d'enseignements pour le futur, et, avec ces fragments, tracer le cadre dans lequel s'inscrit la réflexion prospective, c'est à cet exercice que tente de se livrer cette note de contexte.

Je laisse le sage Sénèque prendre à nouveau le fil du propos pour le conclure. « Le plus grand obstacle à la vie est l'attente, qui espère demain et néglige aujourd'hui ». Notre exigence, en effet, consiste à comprendre aujourd'hui pour se préparer à demain. Nous espérons que, d'une certaine manière, ce nouveau rapport d'orientation stratégique puisse y contribuer.

Henri d'Agrain
Délégué général du Cigref

Sommaire

p.02 Avant-propos
p.06 *Executive Summary*
p.12 Note de contexte
p.102 Conseil d'Orientation Stratégique du Cigref
p.104 Remerciements
p.104 Équipe de publication
p.106 Annexe

01

Veille prospective 5 champs de transformation

Enjeux technologiques et nouveaux usages
p.28

Numérique et environnement
p.38

Risques cyber et enjeux géopolitiques
p.46

Fournisseurs et services numériques
p.58

Nouvelles formes de travail et engagement des collaborateurs
p.66

02

Actualisation des scénarios pour les futurs numériques

De nouvelles incertitudes ont émergé à horizon 2035
p.76

Mondialisation régulée par les équilibres géopolitiques
p.78

Vers une Europe puissance dans un monde régionalisé
p.82

Une Chine conquérante dans un monde bipolaire
p.86

Far West, colonies digitales et cartels numériques
p.90

03

Messages clés pour les organisations : naviguer dans un monde d'incertitudes

Enjeux technologiques et nouveaux usages
p.28

Numérique et environnement
p.38

Risques cyber et enjeux géopolitiques
p.46

Fournisseurs et services numériques
p.58

Nouvelles formes de travail et engagement des collaborateurs
p.66

01 Veille prospective

Cette partie propose une actualisation des champs de transformation identifiés dans le Rapport d'orientation stratégique (ROS) 2020, et mis à jour une première fois dans le ROS 2021. Ces champs de transformation recouvrent les domaines du numérique dans lesquels des évolutions majeures sont à l'œuvre et où le jeu d'acteurs, mouvant, exige du Cigref et de ses organisations membres une attention particulière. Au nombre de cinq, ces thématiques ont été sélectionnées grâce à l'approche PESTEL (acronyme pour Politique, Économique, Social, Technologique, Environnemental, Légal ou réglementaire), qui permet de conduire une analyse systémique sur un sujet donné.

En matière de technologies et de leurs usages, mais aussi de leurs régulations, l'exercice prospective est délicat. Le temps de la technologie n'est ni linéaire, ni cyclique, ce qui oblige à prendre en compte plusieurs dimensions dans l'analyse des évolutions et donc dans la veille opérée. Il s'agit, en outre, de discriminer entre effets de mode, effets d'annonce et transformations réelles. En parallèle, les jeux d'acteurs fluctuent et se recomposent sur la scène internationale au rythme d'enjeux géopolitiques et économiques. À cela, s'ajoutent pressions environnementales croissantes et poids des opinions publiques, qui, toutes, jouent un rôle sur le futur des sujets évoqués ici. Pour parvenir à conduire cette veille prospective complexe et multidimensionnelle, le ROS a proposé d'analyser de manière distincte pour chaque champ les tendances lourdes, peu susceptibles d'évoluer à horizon 2030-2035, les émergences ou signaux faibles et les incertitudes majeures, grandes questions posées pour l'avenir. Cette grille de lecture sert de fil rouge aux recherches conduites depuis lors.

L'actualisation de ces champs est donc l'occasion de réévaluer les analyses conduites précédemment et d'identifier les nouveaux phénomènes à prendre en compte par le Cigref et ses organisations membres. Sans ambition exhaustive, cette veille continue a pour vocation de nourrir les réflexions stratégiques des organisations membres du Cigref. Elle a aussi permis d'alimenter les scénarios prospectifs présentés dans la seconde partie de ce rapport.

Cette partie a été illustrée par des œuvres originales de M. Vincent Roland.

CHAMP

01

Enjeux technologiques et nouveaux usages

Veille prospective

Dans ce premier champ, qui porte spécifiquement sur le développement des nouvelles technologies et sur leurs usages potentiels, la grille d'analyse prospective choisie a déjà permis de confirmer, en 2021, un certain nombre des premiers constats établis en 2020. Encore aujourd'hui, ces derniers se vérifient alors que nous procédons à l'actualisation de ce champ pour l'édition de 2022. Comme démontré depuis deux ans, le numérique continue d'être un facteur de résilience majeur, tout au long de la crise sanitaire. Certaines technologies, comme le cloud, se révèlent tout à fait centrales et stratégiques pour les organisations et continuent donc d'être développées. La tendance est lourde puisqu'en 2022, 41% des entreprises européennes ont adopté la technologie cloud, contre seulement 19% en 2016 (source : Eurostat).

ENJEUX TECHNOLOGIQUES ET NOUVEAUX USAGES

De la même manière, **les réseaux et infrastructures 5G**, présentés en 2020 comme des technologies matures, poursuivent leur déploiement en Europe. Les anciennes technologies disparaissent progressivement pour laisser place à la 5G. Le redressement judiciaire de la start-up toulousaine Sigfox en 2021, spécialisée dans les réseaux bas débit et basse consommation, est particulièrement révélateur de ce phénomène puisque l'entreprise a, entre autres, lourdement pâti de son retard dans l'adoption de nouvelles infrastructures. De fait, les applications industrielles de la 5G restent très variables en fonction des pays. En Allemagne, ou au Japon par exemple, les avancées se font bien plus rapidement qu'en France et ce malgré la récente annonce franco-allemande d'un investissement à hauteur de 17,7 millions d'euros (source : Min. Économie) dans quatre projets de 5G industrielle, et la promesse faite en mars 2022 par le gouvernement français de créer un campus fablab à destination des industriels pour tester de nouvelles applications. Selon le rapport du député Hebert sur la « 5G industrielle » délivré en 2022, de telles différences entre pays s'expliquent d'abord par les décisions politiques nationales. Alors que les gouvernements allemand et japonais ont rapidement attribué certaines fréquences 5G aux entreprises, le gouvernement français, lui, les a restreintes aux seuls opérateurs télécom. La Chine, quant à elle, compte déjà 1,43 million de stations de base 5G, soit 60% du total mondial à la fin 2021 (source : Min. Industrie et TIC, Chine). Ces évolutions variables auront des conséquences sur la compétitivité des entreprises tant en termes de diversification de leurs services qu'en termes d'amélioration de leurs flux logistiques, par exemple. Elles sont aussi fortement liées aux jeux d'acteurs économiques et politiques, comme en témoigne le bannissement de Huawei aux États-Unis. Ces enjeux de dépendance et de souveraineté sont plus largement détaillés dans le champ 4. Par ailleurs, le développement inégal de la 5G aux échelles nationales pourrait aussi accentuer les problématiques de fracture numérique. Jusque-là liées à des enjeux d'accessibilité à internet (zones blanches), la fracture pourrait maintenant aussi être conditionnée par des enjeux de débit. En France là encore, si le nombre de sites ouverts par les grands opérateurs augmente progressivement, la cartographie nationale en date de septembre 2021 révèle déjà les zones qui pourraient être concernées par ces problématiques.

En parallèle de ces évolutions tendancielles, deux domaines, au moins, connaissent une nette accélération alors qu'ils relevaient, il y a un an encore, de l'ordre de signaux faibles voire d'incertitudes. L'informatique quantique a ainsi bénéficié d'investissements continus apportés par les industriels (notamment IBM) et les États (par exemple la Chine) en raison des enjeux stratégiques qu'elle représente. **La capacité de puissance de l'informatique quantique** a donc connu un bond sans précédent début 2022, ouvrant la voie à de possibles révolutions du calcul, de la cryptologie, ou encore de l'optimisation des flux. Alors que le ROS 2020 s'interrogeait sur l'apparition de premières applications tâtonnantes d'ici 2030, leur réalisation semble désormais certaine dans les cinq prochaines années. Le marché du quantum devrait représenter 9 milliards de dollars dès 2030 (contre 260 millions en 2020), ce qui devrait avoir un impact sur la recherche bien sûr mais surtout sur l'évolution des rapports de force sur la scène internationale (Source : Statista Digital Economy Compass, 2021).

ENJEUX TECHNOLOGIQUES ET NOUVEAUX USAGES

En effet, l'avènement du quantique provoquera une profonde révolution des usages du numérique et des politiques de cybersécurité, à laquelle gouvernements comme entreprises doivent d'ores et déjà se préparer. Déjà le National Institute of Standards and Technology (NIST) aux États-Unis et l'Autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) en France préconisent d'adopter au plus vite une approche hybride permettant de conserver la cryptographie traditionnelle existante mais d'y intégrer une couche additionnelle de cryptographie résistante au quantique.

Le deuxième domaine à prendre indéniablement de l'ampleur est celui de la **régulation des technologies, des usages et des acteurs du numérique**. Véritable incertitude en 2020, le positionnement des juges et des régulateurs sur ces questions semble se préciser très nettement, en Europe, mais aussi aux États-Unis et en Chine. Il s'agit aussi bien d'encadrer les usages de certaines technologies à risque, que de limiter la puissance des plus grosses entreprises sur la question de la collecte et de l'utilisation des données personnelles, notamment (voir, sur ce sujet, le champ 4).

Sur certains sujets, **les régulations relèvent encore de la *soft law***, c'est-à-dire d'une liste de bonnes pratiques sans dimension contraignante. D'autres sont en cours d'élaboration. Ainsi, par exemple, le Digital Service Act européen est toujours en phase de négociation. S'il était adopté, il obligerait les grandes plateformes à mieux réguler leurs contenus et permettrait de diminuer leur capacité d'ingérence dans les démocraties. Ce texte s'inscrirait alors dans la lignée de la loi contre le séparatisme adoptée en France en août 2021 qui punit toute diffusion d'informations relatives à la vie privée, familiale ou professionnelle si ces dernières mettent en danger la vie d'autrui.

De même, la Commission européenne **fait de la régulation de l'intelligence artificielle** un axe central de ses réflexions, avec pour ambition, là encore, de restreindre le champ d'expérimentation des industriels et de protéger les individus contre les biais potentiels des algorithmes. Le développement de l'IA soulève, en effet, toujours autant de questions morales et éthiques. Les machines sont de plus en plus amenées à échanger entre elles dans un circuit fermé où la place de l'humain devient anecdotique : certaines grandes entreprises utilisent déjà des robots pour passer leurs commandes auprès d'autres entreprises, commandes elles-mêmes prises en charge par des robots. Plus frappant encore, d'ici quelques années, les données traitées par les intelligences artificielles pourraient être exclusivement des données de synthèse, générées automatiquement par d'autres IA pour alimenter la recherche et le développement d'applications avec des conséquences bien réelles sur les individus (source : Accenture). Ces évolutions exigent, bien évidemment, de réfléchir aux cas d'usages et à leur acceptabilité.

veille prospective

D'autres technologies posent aussi de véritables questions législatives **encore irrésolues comme la blockchain**. Étant par définition immuable, elle est, en effet, contraire au RGPD européen qui comporte un droit à l'oubli. Par ailleurs, elle permet le développement de **crypto-monnaies alternatives** qui menacent, pour certaines, la stabilité des systèmes financiers traditionnels. C'est, en tout cas, l'opinion défendue par les économistes Nicolas Dufrêne et Jean-Michel Servet dans une tribune en date de décembre 2021 (source : Le Monde).

Ces régulations - ou tentatives de régulations - des technologies et de leurs usages relèvent sans conteste d'**une prise de conscience croissante par les États**, et en particulier les États membres de l'UE, de l'importance de réguler les pratiques des entreprises privées dans le champ numérique, en raison des enjeux stratégiques, politiques comme économiques, associés. Le rôle joué par de nombreux lanceurs d'alerte, en particulier Frances Haugen contre Facebook depuis l'automne 2021, est non négligeable. Ces individus permettent d'accélérer et de structurer les réactions des institutions publiques face à la toute-puissance des plateformes du numérique qui cherchent, elles, à court-circuiter les instances juridiques en développant des socles de normes, moins contraignantes, plutôt qu'en appuyant la production de textes de lois.

Ces évolutions doivent être suivies de près. Elles recomposeront indéniablement les forces en présence d'ici 2030-2035. Elles positionnent, en effet, **l'Union européenne à l'épicentre de la production de normes et de règles** pour orchestrer les pratiques sur son marché intérieur, par ailleurs très attractif pour les entreprises étrangères. Elles l'érigent aussi en modèle potentiel pour d'autres autorités nationales et ce pour les années à venir. Dans le même temps, **ces régulations interrogent sur le champ d'action laissé libre aux entreprises européennes** elles-mêmes. Si ces dernières souhaitent s'inscrire dans la compétition mondiale pour l'innovation technologique, certaines d'entre elles s'inquiètent des règlements limitant leurs capacités d'expérimentation. Ces règlements pourraient, en effet, être un frein à leur succès dans un environnement toujours largement dérégulé à l'échelle internationale. L'équilibre doit donc encore être trouvé. Il semblerait, toutefois, que l'Union européenne soit effectivement en train de « sortir de sa naïveté », sous l'impulsion de Thierry Breton, Commissaire européen au marché intérieur depuis 2019. En témoignent ses prises de positions plus fortes et moins conciliantes dans le conflit sino-américain. En témoignent aussi ses ambitions affichées en matière numérique, présentées en mars 2021 dans sa « boussole » à horizon 2030 et qui s'articulent autour de quatre points principaux : 1) augmenter significativement les compétences numériques et la qualification numérique des citoyens comme des professionnels, 2) assurer des infrastructures numériques sûres, performantes et durables et bénéficier de capacités de production de semi-conducteurs mais aussi s'affirmer dans le domaine du quantique, 3) soutenir la transformation numérique des entreprises, et 4) numériser la totalité des services publics. Reste à savoir **dans quelle mesure les investissements nécessaires** à la réalisation de ces ambitions pourront effectivement être mis en œuvre, alors même que les États ressortent considérablement endettés de la crise sanitaire…

Enfin, quelques éléments nouveaux ont émergé en 2021-2022 dans ce champ.

Parmi ceux-ci (et sans prétention d'exhaustivité), nous retenons **l'engouement pour les NFT**, acronyme pour *non-fungible tokens*. Les NFT existent depuis 2014 mais ils ont connu un succès récent qui témoigne, pour certains, d'une transformation majeure des modes d'investissement, en particulier dans le domaine de l'art. Ces jetons non-fongibles sont des données cryptographiées qui représentent un objet, souvent numérique, et en assurent l'authenticité, l'unicité et donc la valeur. Ils permettent de vendre et de collectionner des créations numériques, y compris si elles sont complètement virtuelles (une paire de baskets dans un jeu vidéo, par exemple). Les NFT échappent à toute forme de régulation et pourraient donc être à l'origine d'une bulle financière. Ce système, qui repose sur la blockchain, a aussi un coût environnemental conséquent, souvent rappelé par ses détracteurs.

Autre point majeur, **les biotechnologies**, peu évoquées dans les précédents rapports, ont connu des avancées récentes, qui témoignent de l'intérêt qu'elles suscitent et de leur potentiel géostratégique dans un contexte de tensions croissantes sur les ressources et les matières premières. Ainsi, par exemple, le stockage de données sur l'ADN, éventualité théorique dans les années 60, connaît aujourd'hui de premières applications concrètes. En novembre 2021, Stéphane Lemaire et Pierre Crozet ont fait rentrer deux capsules métalliques, contenant chacune 100 milliards de copies de la Déclaration des droits de l'homme et du citoyen de 1789, et de la Déclaration des droits de la femme et de la citoyenne de 1791, conservées sous forme d'ADN, aux archives nationales, prouvant ainsi la faisabilité de cette technique. Le stockage ADN des données pourrait permettre de répondre à deux enjeux au moins : l'augmentation exponentielle du volume de données d'une part et le poids croissant des coûts énergétiques associés pour les stocker d'autre part. Les États-Unis et la Chine investissent donc massivement dans des programmes de recherche. De son côté, l'Europe dispose du programme Oligoarchive, financé à hauteur de 3 milliards d'euros pour un usage limité, pour le moment, à l'archivage. Toujours dans le domaine des biotechnologies, la recharge d'une puce ARM par des algues grâce à la photosynthèse est une autre avancée récente potentiellement révolutionnaire. Ces recherches, encore expérimentales, pourraient toutefois induire de nouveaux usages et comportements dans le stockage de la donnée et l'alimentation énergétique des composants électroniques.

ENJEUX TECHNOLOGIQUES ET NOUVEAUX USAGES

Enfin, l'annonce par Mark Zuckerberg du lancement du **métavers, son grand projet de réalité virtuelle**, interpelle. Si ce projet reste encore de l'ordre de l'hypothétique, les investissements qu'il recouvre, les jeux d'alliance qu'il a déjà ouverts (citons, entre autres, le partenariat signé entre Facebook et Carrefour en France) et les conséquences qu'il pourrait avoir sur l'économie, l'organisation sociale et la vie quotidienne même des individus obligent à s'y intéresser. Quel impact pourrait avoir le métavers sur les foyers, les entreprises, et les démocraties ? Un tel univers pose autant de questions éthiques (notamment sur la protection des données personnelles ou la lutte contre le cyber-harcèlement) que de questions de souveraineté pour les organisations et les gouvernements européens. S'il semble évident que de nombreux acteurs, outre Meta, cherchent à investir le champ de la réalité virtuelle, notamment pour améliorer le travail et la collaboration à distance (Microsoft, Zoom) ou proposer de nouveaux services (Epic Games), la question de la régulation et du contrôle de ces technologies et de leurs usages associés reste toujours entière.

Ces interrogations sont d'autant plus prégnantes qu'au même moment, et à l'opposé de ces tendances à l'hyper-technologisation, les **mouvements de résistance au numérique**, ou plus globalement aux nouvelles technologies, se sont densifiés au cours des derniers mois. Présentée comme une incertitude majeure dans le ROS 2020, cette défiance semble s'être accentuée tout au long de la pandémie, et ce à plusieurs titres. Les arguments qui l'alimentent sont en effet pluriels. Le développement et les ventes de nouvelles technologies apparaissent, pour de nombreux individus et associations, contradictoires avec la prise de conscience de l'aggravation de la crise environnementale, de plus en plus évidente à mesure que les sinistres s'enchaînent partout sur le globe. À cela s'ajoutent les enjeux d'exclusion des personnes les moins aisées, y compris dans le champ du travail, alors qu'une part croissante des activités du quotidien se numérise. Corrélés à ce phénomène, les risques pour la santé mentale liés à la sur-utilisation et à la sur-exposition au numérique sont de plus en plus avérés, en particulier chez les plus jeunes. Enfin, à une échelle plus large, le rejet, par une partie de la population, des technologies ARN-m utilisées dans les vaccins contre le Sars-Cov2 témoigne, à tout le moins, d'un durcissement des opposants à la course technologique mais aussi d'un durcissement des politiques gouvernementales vis-à-vis de ces opposants. Dans les années à venir, ces tensions pourraient donc s'aggraver, voire être au cœur d'une ligne de fracture croissante entre différentes communautés à plusieurs vitesses, au sein même des pays développés. Dans ce contexte, il n'est pas sûr que la « culture de la transparence » que souhaite promouvoir le gouvernement français en accélérant, par exemple, sa stratégie d'open source, soit suffisante pour rétablir une réelle « confiance démocratique ».

Point de vue

MÉTAVERSE

« Depuis qu'en octobre 2021 Mark Zuckerberg décida de changer le nom de la société Facebook en « Meta », en référence au métaverse qu'il souhaite bâtir, le mot a acquis une grande popularité. Pourtant le terme, inventé en 1992 par Neal Stephenson dans le roman Snow Crash, est relativement ancien et le principe d'une telle simulation, décrite en 1964 dans l'ouvrage « Simlacron 3 » de Daniel Galouye, l'est plus encore. Les premières tentatives d'univers virtuels sont elles aussi datées. Second Life, où l'on peut se promener à loisir, et se présenter aux autres au moyen d'avatars, à savoir d'êtres numériques que l'on compose, que l'on coiffe et que l'on habille à son goût, date de 2003, ce qui fera bientôt vingt ans. De fait, il existe déjà de multiples applications industrielles des réalités virtuelles (VR – Virtual Realities en anglais) qui permettent le développement de métavers proprement immersifs. Citons par exemple le domaine des jeux vidéo ; citons aussi ce que l'on appelle les « jeux sérieux » (*serious games* en anglais) avec de nombreuses utilisations dans le secteur du marketing ou de la formation. Enfin, les simulations sont déjà essentielles dans le domaine militaire, où elles concourent à la formation des opérateurs ».

Par Jean-Gabriel GANASCIA
Professeur Sorbonne Université

Le regain d'intérêt actuel n'est donc pas lié à la nouveauté du concept mais aux progrès techniques qui permettraient de le systématiser. Le perfectionnement actuel des technologies qui sous-tendent les réalités virtuelles laisse en effet désormais espérer la réalisation de tels univers dans lesquels nous serions en mesure de nous projeter à loisir. Au plan technique, les VR font ainsi appel à trois notions complémentaires : 1) la **reproduction** numérique d'un monde semblable, à certains égards, au nôtre, 2) **l'immersion** dans cet univers par stimulation de tous nos sens, en particulier de la vision, de l'audition, du toucher et de la kinesthésie (sensation du mouvement), et enfin 3) la **navigation**, à savoir la capacité à se mouvoir à l'intérieur de cet univers. Aujourd'hui, la puissance des ordinateurs permet de reproduire, avec une fidélité croissante, le monde extérieur sous différents angles à l'aide de modèles numériques tri-dimensionnels. Les casques comme l'Oculus permettent de plonger dans ces univers et de s'y mouvoir. De même, il existe des dispositifs qui procurent des sensations kinesthésiques très troublantes et aident à se déplacer dans ces univers. On imagine aisément les nouvelles applications commerciales qui pourraient en être faites, par exemple en créant des boutiques ou des agences bancaires en ligne.

Mais ce regain d'intérêt soudain tient aussi à l'inquiétude d'être exclu du seul métaverse attractif : celui de Mark Zuckerberg. Car ce dernier ne souhaite pas seulement proposer un univers virtuel de plus, il a pour ambition d'agréger et de fusionner les différents métaverses dans un métaverse unique où tous pourraient échanger, comme nous le faisons déjà sur le web. Déjà, de nombreuses sociétés (par exemple Sony, Lego, Nike, HSBC, JPMorgan, Pfizer, Coca-Cola, etc.) investissent dans ce grand métaverse pour y équiper des terrains avec de multiples applications.

Face à cela, une première question se pose : allons-nous substituer au web un nouvel espace d'échange tri-dimensionnel qui sera le Métaverse ? Et, dans le cas où ce serait techniquement possible, cela serait-il souhaitable au plan industriel et politique ? En effet, non seulement beaucoup des métaverses actuels sont confidentiels et leurs promoteurs souhaitent leur conserver ce caractère privé, mais de plus, le coût écologique de la fusion de tous ces métaverses, avec la génération systématique d'univers de synthèse tri-dimensionnels, risquerait d'être prohibitif.

En parallèle, le projet de Mark Zuckerberg suppose qu'une société privée, en l'occurrence Meta, régisse l'intégralité de ce métaverse unique, ce qui lui donnerait un pouvoir exorbitant, puisque sans contrôle. Là où la gouvernance du web s'était mise en place progressivement, avec de nombreux acteurs comme l'ICANN, l'IGF, l'ISOC, l'IETF, le W3C etc..., nous aurions alors un seul administrateur qui pourrait imposer ses propres règles sur un mode autoritaire, ce qui est difficile à imaginer lorsque l'on voit déjà les difficultés qui se posent avec les politiques de régulation des contenus par les plateformes ou les problématiques de cyber-harcèlement.

Enfin, et pour conclure, rappelons que dans les œuvres de science-fiction où il a été introduit, le métaverse se présente plutôt comme une utopie négative où l'on est amené à douter de son existence d'être autonome puisque, lorsque nous nous y transportons en esprit, nous en venons à craindre d'être nous-mêmes les jouets de malins génies plus puissants que nous dans un grand métaverse cosmique que nous ignorerions. Dès lors, il apparaît étonnant qu'on nous propose comme futur désirable une dystopie qui fait plus écho à un cauchemar qu'à un rêve idyllique...

CHAMP

20

Numérique *et* environnement

Une prospective

La **capacité réelle du numérique à jouer un rôle dans la lutte contre le réchauffement climatique** continue d'interroger à mesure que les pressions sur nos écosystèmes s'accroissent. Les ROS précédents mettaient déjà en lumière les tensions existantes entre l'optimisation des usages et de la consommation d'énergie que permettent certaines nouvelles technologies et les impacts délétères de ces mêmes outils. De plus en plus, la **dichotomie entre les promesses** d'acteurs privés promouvant des technologies révolutionnaires **et la réalité d'un monde aux ressources limitées** devient évidente. Face à ce constat, il apparaît clair que la division entre virtuel et réel n'existe plus.

NUMÉRIQUE ET ENVIRONNEMENT

Ainsi, à l'heure où nous rédigeons ce nouveau rapport, un certain nombre de tendances déjà identifiées restent tout aussi pertinentes. **L'équation entre avancées techniques et pilotage de la transition écologique** est encore irrésolue. Certes, de l'espoir réside dans **le développement**, par exemple, **d'intelligences artificielles qui, combinées à la puissance de l'informatique quantique**, seraient capables d'optimiser les flux de production, les transports, de détecter des pollutions avant qu'elles ne s'étendent, voire de développer de nouvelles technologies capables de diminuer notre empreinte carbone. Sur la seule problématique des émissions de CO_2, la valeur ajoutée des technologies apparaît clairement dans les études conduites par Accenture sur la numérisation dans les domaines du bâtiment, de la mobilité et du « manufacturing » (source : Accenture). La mise en place de nouveaux outils de pilotage créerait ainsi un potentiel d'économie de CO_2 de 6 à 7 fois supérieur à l'empreinte négative. De même, des modélisations parviennent de mieux en mieux à prédire la recrudescence de phénomènes météorologiques extrêmes ou les effets du réchauffement climatique sur des zones très précises afin d'améliorer, par exemple, les politiques d'urbanisme. Déjà pendant la crise sanitaire Covid-19 (qui semble résulter, pour partie, des effets pervers des dégradations environnementales), **les technologies d'information, de prédiction et de communication ont prouvé leur utilité dans le suivi et la gestion de la pandémie**. À des échelles plus individuelles, **les outils numériques peuvent aussi être de véritables vecteurs pédagogiques** pour aider les citoyens à mieux orienter leurs choix de consommation et, plus globalement, à adapter leurs modes de vie aux enjeux environnementaux. Le consortium NumAlim travaille ainsi à la mise en place d'une application à destination des individus pour améliorer leurs pratiques de consommation.

Mais dans le même temps, l'**essor des crypto-monnaies et des NFT** (voir champ 1), **l'avènement imminent de l'informatique quantique, les investissements massifs dans la réalité virtuelle et la question de la sobriété de l'IA** elle-même, toujours hautement consommatrice en données, inquiètent par les dépenses énergétiques effrénées que ces technologies induisent. Jusqu'à présent, les organismes publics comme privés évoluaient dans un brouillard relatif, en l'absence de référentiels partagés pour évaluer les bénéfices-risques à la mise en œuvre de telle ou telle stratégie de développement technologique. À l'échelle européenne, la Corporate Sustainability Reporting Directive (directive CSRD) pourrait changer cette situation en apportant de premiers indicateurs communs pour évaluer le coût environnemental du SI d'entreprise. Elle obligera, en effet, les entreprises à fournir des informations relatives aux problématiques de durabilité, de changement climatique et à évaluer l'impact de leur activité sur l'environnement et la société en général. Ces critères communs seront établis par l'EFRAG (European Financial Reporting Advisory Group). D'autres travaux méthodologiques sont en cours sur ces sujets, notamment à l'échelle de l'Union européenne (EU Green Digital Coalition).

NUMÉRIQUE ET ENVIRONNEMENT

Ainsi, les lignes bougent car **la prise de conscience au sein des organisations et des populations s'accentue**, particulièrement en Europe. Dans ce champ, comme dans le précédent, l'Union européenne subit son retard en matière de production, de contrôle et de développement de matériaux stratégiques. La pandémie et ses répercussions a bien entendu ravivé les débats autour de l'accès et de la maîtrise non seulement des énergies mais aussi de certains métaux critiques, voire de l'eau. En effet, si la problématique énergétique est largement connue, celle concernant les réserves de métaux commence réellement à interroger. **D'ici 2030, l'utilisation de certains métaux sera multipliée par trente** pour produire les équipements qui permettront de générer de l'électricité verte. Or, ce sont ces mêmes métaux qui serviront aussi à alimenter la fabrication d'outils numériques (voir l'étude Ademe 2022 sur le sujet). De la même manière, **la disponibilité et le coût de l'eau** dans les années à venir devient une source d'inquiétude majeure. La dimension écosystémique de la production et de l'utilisation du numérique avait déjà été largement décrite par la littérature. Mais aujourd'hui se concrétise **l'ère des grands dilemmes**, dans laquelle les États et les entreprises auront à **faire des choix pour équilibrer transition écologique et évolutions technologiques**. Le développement de l'Internet des Objets est particulièrement illustratif sur ce point. La diminution du coût des capteurs du fait de leur généralisation pourrait participer à une multiplication massive des objets connectés dans les années à venir. Mais dans le même temps, la crise des semi-conducteurs qui dure depuis l'été 2021 révèle à quel point les problématiques d'approvisionnements en ressources critiques peuvent fortement ralentir les dynamiques de production et de mise sur le marché de nouveaux outils. Des solutions pour mettre fin à l'obsolescence programmée des terminaux et pour favoriser l'économie circulaire (par exemple pour réutiliser les serveurs de stockage de données) pourront être de plus en plus développées dans ce cadre.

Le retard pris par l'UE a ceci de positif qu'il l'encourage néanmoins à légiférer pour garantir son autonomie stratégique et la conduit à prendre à bras le corps la question environnementale. À Bruxelles, trois directions générales se préoccupent aujourd'hui de ces enjeux, y compris la DG Connect. En 2020, la Commission européenne jetait les bases de sa stratégie industrielle y incluant une analyse, poursuivie depuis lors, sur ses dépendances stratégiques (source : Commission européenne).

En parallèle, une minorité d'États, la France en tête, font déjà office de leader dans ce domaine. **Le Sénat français a ainsi adopté le 15 novembre 2021 la loi REEN** pour Réduire l'Empreinte Environnementale du Numérique. Cette loi encourage à accélérer la promotion de l'économie circulaire. De fait, sur ces questions, **la France est en avance mais isolée**. L'Arcep a ouvert des discussions avec ses homologues européens mais pour le moment sans succès. L'affermissement d'une doctrine européenne sur ces enjeux reste donc essentiel.

Notons, par ailleurs, que dans ce champ aussi, l'**équilibre entre maîtrise des externalités négatives et compétitivité des organisations européennes sur la scène internationale** restera à trouver. Certains secteurs sont particulièrement vulnérables, le secteur touristique notamment qui pourra connaître, en conséquence de la crise sanitaire et d'une perception croissante des enjeux environnementaux, une seconde vague de disruption technologique. Pour autant, **les organisations elles-mêmes tendent à se préoccuper de manière croissante de ces enjeux**. Si, pour certaines, cette appétence relève de sensibilités personnelles au sein des équipes, voire d'une stratégie engagée mise en place à l'échelle du groupe, elles sont aussi de plus en plus nombreuses à devoir rendre des comptes auprès de leurs investisseurs en matière de politique RSE, comme évoqué dès 2020. Ainsi, **la notion de sobriété numérique** prend de l'envergure dans les stratégies internes des organisations et recoupe des enjeux plus larges que la seule question environnementale.

De fait, la notion de responsabilité numérique ne s'arrête pas à cette seule question. Elle prend en compte, de plus en plus, des enjeux sociétaux. Les politiques de numérique responsable au sein des organisations englobent ainsi souvent les problématiques d'accessibilité, pour les clients comme pour les collaborateurs âgés ou en situation de handicap. Les problématiques d'accessibilité revêtent elles-mêmes plusieurs volets : l'accès à une connexion internet performante, l'illectronisme d'une partie de la population et la capacité financière à posséder son propre appareil connecté à internet. Selon l'INSEE, 17% de la population française a encore des difficultés d'accès au numérique en 2022, soit parce qu'elle ne dispose pas d'un accès à internet soit parce qu'elle ne sait pas utiliser les outils numériques.

Si de telles évolutions plus holistiques concernent encore une minorité d'organisations, il y a fort à parier que ces dernières s'assurent un temps d'avance sur leurs concurrentes dans les années à venir, en termes d'image, d'attractivité et de rentabilité.

Ainsi dans ce champ comme dans le précédent, **la question sociale se fait de plus en plus prégnante**. L'acceptabilité des technologies repose, on l'a vu, de manière croissante sur la conscience écologique des individus qui, pour certains, atteignent une forme de maturité dans le domaine. À cela s'ajoute un enjeu déjà évoqué en 2020 et en 2021 autour de la question de la surveillance des personnes à des fins écologiques mais qui pourrait accroître très fortement la tension au sein des démocraties. Les technologies, et ce qu'elles ouvrent comme possibles en termes de suivi et de contrôle, obligent à redéfinir collectivement les notions de liberté et de responsabilité individuelle. Sans débat cohérent organisé avec les populations, les tensions sociales déjà observées et décryptées à l'aune de la crise sanitaire risquent de s'accroître très fortement.

veille prospective

Point de vue

DU CARBONE À L'ÉNERGIE, PAS D'ISSUE SANS SOBRIÉTÉ

« Les rapports scientifiques se multiplient et confirment que le réchauffement climatique est à la fois plus rapide et plus prononcé que ce que les études antérieures prévoyaient. Il en est de même pour la détérioration de la biosphère et le dépassement des limites planétaires ».

Par Hugues FERREBOEUF
Chef de projet à The Shift Project

Dans ces conditions, il est indispensable que le numérique, comme tout autre secteur, modifie ses modes de production et, sans doute, ses logiques économiques sous-jacentes, pour contribuer à ralentir puis éviter la dégradation de nos écosystèmes. Le législateur en a pris acte en France à travers la loi pour la réduction de l'empreinte environnementale du numérique adoptée en novembre 2021 et tant les directions numériques des entreprises utilisatrices que leurs fournisseurs ont maintenant, à tout le moins, identifié cet enjeu, voire initié une démarche visant à contribuer à cet objectif. En Europe, des travaux préparatoires à une future réglementation sont en cours, en aval des conclusions du Conseil Européen de décembre 2020.

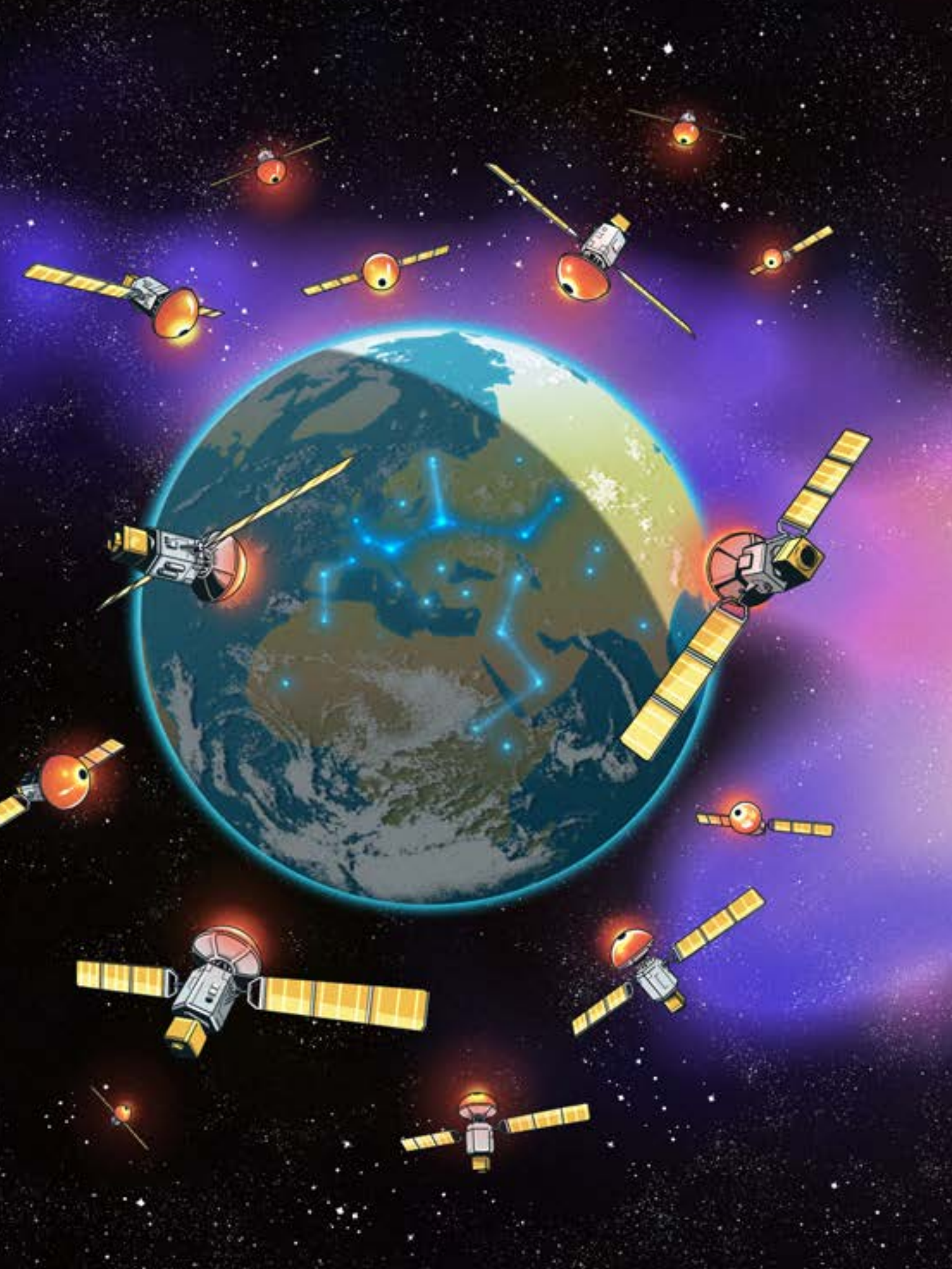
Pourtant les évènements géopolitiques récents ont brutalement mis en lumière ce que l'Agence Internationale de l'Energie avait indiqué depuis quelques années : faute d'anticipation suffisante, la transition vers une économie post-carbone va devoir se faire sous condition de ressources énergétiques et minérales limitées, notamment dans la décennie à venir. Pour réduire nos émissions il ne suffira pas de décarboner (partiellement d'ailleurs) l'énergie que nous consommons ; il faudra également réduire notre consommation d'énergie et, sans doute, de matière.

La sobriété énergétique va donc être non seulement un choix vertueux mais aussi une nécessité, sur le plan économique comme sur celui de la résilience opérationnelle.

Pour le secteur numérique dont la consommation d'électricité augmente d'environ un tiers tous les cinq ans dans le monde, le challenge est considérable et il ne pourra le remporter sans introduire un principe de sobriété (numérique cette fois) dans son fonctionnement, tant au niveau de l'offre que de la demande.

Pour les entreprises utilisatrices, il s'agira non seulement d'optimiser les systèmes d'information et les plateformes de services mais aussi de cadrer au plus juste ses expressions de besoins, ce qui peut représenter un véritable changement de paradigme.

Pour les fournisseurs de produits et de services numériques, cela induira des transformations profondes, allant jusqu'à des changements majeurs de leurs modèles d'affaires voire de leurs raisons d'être. Une situation porteuse de risques pour nombre d'acteurs dominants mais aussi d'opportunités pour des entreprises, françaises ou européennes, qui auront su l'anticiper pour en faire un avantage concurrentiel.



CHAMP 03

Risques cyber et enjeux géopolitiques

veille prospective

Dans le contexte de tensions internationales où nous écrivons ces lignes, l'imbrication entre enjeux cyber et géopolitiques est de plus en plus perceptible. Surveiller ces deux enjeux dans le cadre d'une même veille prospective revêt tout son sens pour répondre aux objectifs stratégiques et sécuritaires des organisations membres du Cigref.

La sécurité numérique inquiète chaque année davantage les organisations membres du Cigref. Les ROS précédents avaient noté l'**augmentation continue du nombre et de l'intensité des cyberattaques.** Cette tendance structurelle s'est renforcée en 2022. Le rapport d'Orange Cyberdefense publié en 2021 note une augmentation de 13% des cyberattaques en 2021 par rapport à 2020. Les petites et moyennes entreprises demeurent les principales victimes de ces vagues de cyberattaques par rapport aux grandes entreprises, qui ont, elles, investi massivement dans leur cybersécurité.

RISQUES CYBER ET ENJEUX GÉOPOLITIQUES

Comme nous l'avions noté en 2020 et 2021, cette augmentation des cyberattaques est due à une **industrialisation croissante des groupes de cybercriminels et à la structuration du *dark web*,** les hackers proposant leur service contre rémunération sur des plateformes spécialisées. Les marchés du *dark web* auraient généré un nouveau record de revenus en 2021, rapportant un total de 2,1 milliards de dollars en crypto-monnaies (source : Chainanalysis, Crypto Crime Report). Environ 300 millions de dollars de ce total ont été générés par les boutiques de fraude, qui ont servi d'intermédiaires pour la vente de logins, de cartes de crédit et de kits d'exploitation volés, entre autres. Le constat des derniers ROS, selon lequel les groupes de cyberattaquants seraient très structurés et organisés entre eux, serait tout de même à nuancer. **Les groupes de cyberattaquants constituent de plus en plus des nébuleuses difficilement identifiables**, malgré l'industrialisation de leur processus. Cette évolution est directement liée à la capacité des groupes de cybercriminels de réutiliser ou d'acheter les produits d'autres groupes actifs. Ainsi, le code du logiciel malveillant du groupe Egregor, arrêté en 2021 grâce à l'action conjointe de plusieurs polices nationales en Europe, a démontré des liens de parenté avec celui d'un autre groupe maintenant éteint, le groupe Maze. La réutilisation de ces outils d'attaques est une manière de préserver les ressources financières et humaines des groupes de cybercriminels. Le caractère nébuleux de ces groupes rend plus difficile l'identification des responsables pour une organisation, identification parfois nécessaire pour mener à bien une action en justice.

Par ailleurs, l'évolution de l'organisation de ces groupes cybercriminels n'est pas le seul point à nuancer par rapport aux éditions précédentes du ROS. En 2020, nous observions que les deux motivations principales des cybercriminels étaient d'ordre financier ou politique. La motivation principale des cyberattaques actuelles reste effectivement financière, le risque d'attaques d'ampleur et très destructrices demeure donc faible. Cependant, les organisations membres du Cigref s'inquiètent de plus en plus **des attaques de type cheval de troie pouvant infecter leur système d'information via des logiciels en apparence légitimes, mais qui contiendraient une fonctionnalité malveillante**. Guillaume Poupard, l'ancien Directeur Général de l'ANSSI, alertait sur les potentiels effets en cascade de ces campagnes actuelles de cyberattaques. Ces dernières viseraient alors à prépositionner des logiciels malveillants activables à distance sur plusieurs organismes, dans une optique de déstabilisation globale, à la fois politique et économique. Cependant, il est difficile de savoir jusqu'où cette escalade cyber pourrait aller. Cette notion de destruction dans le domaine cyber, à appréhender sous le prisme d'une analyse géopolitique, exige d'être intégrée dans les scénarios de gestion de crise et de continuité d'activités des organisations. Les organisations des secteurs critiques comme l'énergie ou les télécommunications ont davantage de risques d'être visées par ce type d'attaque.

RISQUES CYBER ET ENJEUX GÉOPOLITIQUES

Cette augmentation des cyberattaques a fait émerger en 2022 un nouveau sujet, celui de l'assurance, peu traité dans les ROS précédents. Face à cette recrudescence des cyberattaques, les organisations cherchent à s'assurer. Cependant, les assureurs sont réticents à prendre en charge ce risque émergent. Ils refusent de le faire ou augmentent les niveaux de primes à des tarifs prohibitifs. Selon une étude de l'Association pour le management des risques et des assurances de l'entreprise (Amrae), parue en mai, le montant des indemnisations versées en France entre 2019 et 2020 a été multiplié par près de trois, passant de 73 à 217 millions €. L'insuffisance des mesures de sécurisation du SI prises par les organisations empêche, encore aujourd'hui, les assureurs de proposer des offres intéressantes. Avant la mise en conformité exigée par les assurances, huit dossiers sur dix ne sont ainsi pas éligibles à une assurance cyber. Pour faire face à cette **difficulté des assurances à prendre en charge le risque cyber**, les organisations tendent à placer de plus en plus la résilience au cœur de leurs projets SI. Ce changement dans les critères de décision pourrait avoir un réel impact sur les futures DSI.

Certains sujets émergents en 2020 sont maintenant de vraies tendances structurelles. Nous observions ainsi la **fragmentation du cyberespace**. Ce phénomène pourrait s'accélérer au regard du conflit en Ukraine. En 2019, la Russie adoptait une loi sur la mise en place d'un internet souverain, baptisé Runet. Depuis cette adoption, ce réseau coupé de l'internet mondial a été testé et il est rapidement déployable, ce qui pourrait permettre à la Russie de couper rapidement internet en cas d'urgence. Cet internet souverain vient s'ajouter à ceux de la Chine, de la Corée du Nord et de l'Iran.

Le conflit en Ukraine a également d'autres conséquences sur le cyberespace. **L'utilisation du cyberespace comme moyen de pression politique** peut être maintenant considéré comme une tendance lourde à prendre en compte par les organisations. L'action malveillante d'acteurs étatiques répond à d'autres objectifs que celles des groupes spécialisés dans le ransomware, ce qui demande aux organisations d'agir différemment face à ce risque. En 2021, a été constatée une augmentation des attaques d'espionnage, parfois mises en place depuis plusieurs années. L'augmentation des entreprises privées spécialisées dans ce type d'espionnage est le signe d'une industrialisation de la pratique, au même titre que les attaques de type ransomware. La société israélienne NSO, à l'origine de l'affaire Pégasus qui a éclaté à l'été 2021, a vendu pendant plusieurs années un logiciel de piratage de smartphone à plusieurs États dont le Maroc, le Mexique ou encore l'Arabie Saoudite, ce qui a permis à ces États d'espionner des dirigeants politiques, des opposants politiques et des journalistes. Fin 2021, Meta fermait 1500 comptes connectés à sept sociétés spécialisées dans l'espionnage numérique (source : Le Temps). Le gouvernement chinois utilise particulièrement ce type d'attaque dans le cadre de la compétition économique et industrielle mondiale. Les entreprises sont donc des cibles de choix pour ce type d'attaques, plus difficilement détectables.

Enfin, **le cyber rentre de plus en plus dans le champ des opérations militaires et devient une arme étatique supplémentaire dans le cadre de conflits armés ou en remplacement d'armes physiques**. Cette hybridation des conflits trouve, là encore, son illustration dans la guerre actuelle entre l'Ukraine et la Russie. Même si depuis l'invasion de l'Ukraine par la Russie, enclenchée le 24 février 2022, le cyberespace est moins investi que prévu, témoignant, pour le moment, de la difficulté de conduire des attaques simultanément dans les domaines physique et virtuel, les États appellent leurs entreprises à la prudence. Les Etats-Unis affirment, par exemple, détenir des renseignements sur la volonté de la Russie de cibler le pays avec des attaques informatiques (Source : Le Monde, mars 2022). Cependant, le conflit entre l'Ukraine et la Russie n'est pas un phénomène nouveau. Depuis 2014, les deux pays sont en opposition ouverte, et la Russie a déjà mené plusieurs cyberattaques à l'encontre de l'Ukraine, notamment contre ses infrastructures électriques en 2015 ou plus récemment en janvier et février 2022 contre plusieurs sites gouvernementaux. Même si elles sont encore limitées, ces cyberattaques ont accompagné dès février les offensives terrestres à la frontière ukrainienne pour déstabiliser le gouvernement. Le président russe Vladimir Poutine a par ailleurs rappelé qu'il n'hésiterait pas à répondre aux sanctions européennes par des attaques asymétriques. L'ANSSI a donc, elle aussi, recommandé aux entreprises françaises de renforcer leurs moyens de cybersécurité. Cette volonté de déstabilisation d'un État passe également par une guerre informationnelle, c'est-à-dire par la publication de fausses informations en ligne, dans une logique de cognitive warfare, dont l'objectif est de « déstabiliser les esprits ». La guerre menée sur les réseaux sociaux entre l'Ukraine et la Russie est de fait virulente, même si l'Ukraine semble, à date, avoir pris le dessus en matière de communication et de propagande positive, la Russie privilégiant, pour le moment, une approche par la censure. Cette potentialité croissante d'ingérence étrangère au sein de la vie politique et publique des pays pourrait avoir de fortes répercussions lors d'un contexte électoral, ce qui pose la question du futur de nos démocraties numérisées.

Cette diversification des menaces et des cyberattaques **augmente le besoin en compétences cyber au sein des organisations**. En 2020, nous rapportions ce besoin croissant qui constitue aujourd'hui une vraie source de préoccupations pour les organisations françaises. En 2021, 45% des entreprises indiquaient qu'elles peinaient à pourvoir les postes ouverts dans cette discipline. 5000 postes sont actuellement à pourvoir dans ce domaine dans l'Hexagone (source : PwC).

Face à ces différentes tendances lourdes et émergentes qui se sont renforcées ces dernières années, **la capacité à faire advenir un droit international du cyberespace demeure une incertitude majeure**. L'Union européenne donne le ton sur le plan réglementaire et la présidence française de l'Union en 2022 permet de mettre le numérique dans les principaux objectifs de l'Europe. Le numérique est l'une des trois priorités de la présidence française, entre régulation des contenus, rééquilibrage des marchés et investissement dans les acteurs européens. Cependant, l'aspect sécuritaire reste peu abordé et les investissements manquent pour parvenir à formuler une politique concertée de sécurité numérique, au-delà de la directive NIS 2, qui impose des règles communes de cybersécurité aux organisations de l'Union européenne. Adoptée en 2022, celle-ci ne se transcrira dans le droit des États membres qu'en 2024. Les organisations devront donc patienter et mener d'ici là des efforts de protection de leur SI de manière individuelle. Le manque de culture cyber dans la société civile peut aussi expliquer cette faible prise en compte de la sécurité numérique dans les politiques publiques. Cependant, le conflit ukrainien ayant entraîné une forte médiatisation sur l'utilisation de l'arme cyber dans le champ politique, cela pourrait favoriser une prise de conscience collective autour des risques cyber. Mais, le chemin à parcourir reste encore long et les entreprises ont un rôle important à jouer via les actions de sensibilisation menées en interne et les formations prodiguées aux collaborateurs.

Par rapport aux deux rapports précédents, de nouvelles incertitudes sont apparues. La perspective d'une **coupure de l'internet mondial résultant d'actions malveillantes sur les infrastructures sous-marines et satellitaires** doit être envisagée pour que les entreprises s'y préparent et intègrent cette hypothèse dans leurs scénarios de résilience. Le contrôle des câbles sous-marins européens destinés à acheminer les télécommunications du continent répond à un enjeu d'indépendance qui se renforce, du fait des attaques étrangères perpétrées sur ce type d'infrastructures. Par exemple, des câbles situés à proximité de la Norvège ont été endommagés lors d'une attaque attribuée à la Russie en fin d'année 2021 (source : Institut norvégien de recherche marine). Pour se défendre face à ce type d'attaques, la France investit dorénavant dans des drones sous-marins. Le développement de satellites basse-orbites destinés à la transmission des télécommunications pourrait aussi apporter une alternative à ces infrastructures terrestres. Cependant, leur utilisation reste encore anecdotique aujourd'hui, car 99% du trafic internet passe par les câbles. Les leaders du marché satellitaire sont Amazon avec son projet Kuiper et Tesla avec Starlink. Les deux entreprises misent sur des satellites situés à 550 kilomètres de la Terre pour apporter Internet là où la 5G et la fibre optique n'arriveront pas. Néanmoins, par rapport aux technologies terrestres, ces infrastructures n'offrent pas le même débit ni la même latence et sont souvent plus chères pour le consommateur. Au-delà de la couverture des territoires sans internet, les satellites répondent aux besoins particuliers de clients professionnels (marine, défense, plateformes pétrolières offshore, etc.) et aux besoins futurs de l'Internet des objets. Ces infrastructures commencent également à subir des attaques malveillantes. Ainsi, l'entreprise américaine Viasat, qui opère depuis avril 2021 le satellite Ka-Sat, a annoncé le 28 février 2022 avoir subi une panne partielle qui pourrait être le fruit d'une cyberattaque. Lors de cette panne, une dizaine de milliers d'internautes ont été privés de connexion.

RISQUES CYBER ET ENJEUX GÉOPOLITIQUES

Le rôle joué par le continent africain dans les enjeux du numérique mondial est également un élément d'incertitude croissant peu exploré dans les précédents ROS. Le continent africain a longtemps été considéré comme une terre promise pour les acteurs du numérique, à la fois comme vivier de talents et comme espace d'opportunités. Aujourd'hui, les enjeux sont surtout infrastructurels, on le constate à travers les investissements des principaux acteurs internationaux Les câbles sous-marins construits par Google et Amazon autour du continent africain constituent en effet des équipements d'infrastructure dont le continent dépendra pendant des années. D'un autre côté, Huawei se développe fortement en Afrique australe et entre en concurrence avec Orange. Un partage des rôles s'effectue entre ces deux acteurs sur les infrastructures 5G et sur l'IA. Cette logique de partage des territoires devrait perdurer encore plusieurs années. S'ils souhaitent exister dans l'Afrique numérique, les acteurs européens doivent donc d'abord se concentrer sur les infrastructures. Ainsi, Orange est l'acteur européen le mieux implanté sur le continent, l'opérateur télécom est présent actuellement dans 18 pays. Cependant, la Chine investit massivement sur le continent et est le premier investisseur devant les États-Unis, la France et la Turquie depuis 10 ans, selon un rapport de Swiss-African Business. L'an dernier, les investissements directs chinois sur le continent africain représentaient, selon le directeur du Centre d'études chinoises de l'Université de Dar es-Salaam, 50 milliards de dollars, soit cent fois plus qu'en 2000.

Plus globalement, **l'évolution de la présence chinoise et du rôle de la Chine dans le cyberespace après la crise sanitaire est une source d'interrogations** pour de nombreuses entreprises du secteur. La Chine recule-t-elle sur la scène numérique ? Un rapport annuel de la Chambre de commerce de l'Union européenne en Chine s'interroge sur les signaux qui laisseraient croire que le pays tend à se replier sur lui-même. Le rapport se demande si la Chine, en voulant réduire sa dépendance vis-à-vis du reste du monde, ne serait pas en train de tourner la page des politiques de réformes et d'ouverture initiées il y a quarante ans. Un des indices particulièrement mis en avant par ce rapport est celui du nombre d'habitants étrangers à Shanghai, la capitale économique du pays, qui a baissé de 28% en 10 ans. La fermeture des frontières lors de la crise sanitaire n'a fait qu'accentuer cette évolution. Cependant, les conclusions de ce rapport sont à nuancer. La Chine dispose en effet d'un plan à moyen terme défini en 2015, le plan Made in China 2025, construit en deux volets complémentaires. Le premier volet consiste à privilégier la dimension intérieure pour parvenir à une forme d'autosuffisance. Le second volet, qui arriverait dans un second temps, concerne le renouvellement de la tactique d'investissement à l'étranger pour acquérir de nouvelles technologies stratégiques, et le déploiement international des entreprises chinoises, en se concentrant notamment sur les pays concernés par la « Ceinture économique de la Route de la Soie ». La Chine pourrait donc ne pas avoir véritablement l'intention de se replier de manière définitive mais subissant encore les répercussions de la crise sanitaire, freiner, pour un temps seulement, ses ambitions à long terme. L'évolution de la Chine sur la scène internationale devra donc être étudiée par les entreprises en interne dans le cadre de travaux stratégiques et de prospective, que ce soit en termes de menaces ou d'opportunités.

Pour conclure, trois *wild cards* avaient été détaillées dans le ROS 2020. Deux d'entre elles ont vu leur probabilité d'avènement se renforcer.

La *wild card* concernant le **risque de l'exploitation d'une faille de sécurité majeure et systémique dans un système ou une application massivement utilisée** s'est renforcée au regard de la crise advenue suite à la découverte, en décembre 2021, de vulnérabilités dans Apache Log4J. Log4J est une bibliothèque de journalisation commercialisée par Apache et utilisée par des millions d'applications Java, présentes dans les systèmes d'information de nombreuses entreprises à travers le monde. Ces vulnérabilités ont donc entraîné une crise, qui met en exergue l'absence de normes de qualité sur les logiciels proposés dans les entreprises et plus largement l'absence de certification CE pour les consommateurs. Même si ces vulnérabilités n'ont pas fait l'objet d'exploitation critique par des hackers, elles ont nécessité la mobilisation des équipes de sécurité des entreprises lors de nombreuses semaines. Cet exemple n'est que la partie émergée de l'iceberg car, en 2021, l'ANSSI a publié, à travers le CERT-FR, 991 avis et 22 alertes concernant des vulnérabilités dans les produits suivis par l'agence (source : ANSSI).

RISQUES CYBER ET ENJEUX GÉOPOLITIQUES

La deuxième *wild card* dont la probabilité d'avènement s'est renforcée en 2022 concerne l'**effondrement du système financier suite à une cyberattaque de grande ampleur**. Dans son rapport sur l'évaluation des risques du système financier, publié le 28 juin 2021, la Banque de France consacre toute une partie sur les risques liés aux attaques informatiques. La crise sanitaire a accéléré l'exposition du secteur financier au risque cyber à travers un basculement massif et rapide des activités financières vers le télétravail et la prestation de services à distance, note l'institution. La banque centrale de Nouvelle-Zélande a d'ailleurs été victime d'une cyberattaque en janvier 2021. Heureusement, cette attaque n'a pas eu de conséquences importantes car elle a été rapidement détectée et contrôlée. Cependant, des données sensibles ont été volées. Ce risque devenant majeur pour les États, une simulation de cyberattaque sur le système financier a été organisée entre 10 pays, dont les États-Unis, l'Angleterre, l'Allemagne et l'Italie, entre le 9 et le 19 décembre 2021 dans les locaux du ministère des finances israélien. La France n'a pas participé à cette initiative.

En revanche, aucun événement durant l'année passée ne nous a permis de consolider la troisième *wild card* proposée dans les rapports précédents : l'éventualité de l'effondrement du *Great Firewall* chinois.

Point de vue

L'EUROPE

« Deux faits internationaux majeurs de ce début de XXIe siècle – la mondialisation des échanges et du terrorisme – ont été permis par la dissémination sans précédent des technologies numériques. Dans l'actuelle décennie, la combinaison de plusieurs crises systémiques (environnementale, pandémique, instabilité financière), ajoutée au retour de la guerre conventionnelle en Europe, place le Vieux Continent dans une position ô combien sensible. L'enjeu principal réside dans la capacité de celui-ci à naviguer à l'ère des accélérations technologiques, écologiques et géopolitiques que nous traversons ».

Par Julien NOCETTI
Chercheur associé à GEODE et à l'Institut français des relations internationales, professeur à l'Académie militaire de Saint-Cyr

En matière numérique, l'ardeur de certains décideurs européens à atteindre une « souveraineté » voire une « autonomie stratégique » se double bien souvent d'une rhétorique du retard, celle-ci servant à justifier l'incapacité de l'Europe à se départir d'une forme de sujétion technologique vis-à-vis des États-Unis et de la Chine.

Or, la souveraineté numérique est, elle aussi, un sujet évolutif. Il y a dix ans, les débats se résumaient souvent à répondre à la question « qui contrôle Internet ? ». Ce à quoi l'on assiste aujourd'hui est à la fois une complexification et une extension du champ numérique traditionnel (l'infrastructure Internet, le Web) et il faut par conséquent élargir notre focale en y incluant les technologies critiques (intelligence artificielle, 5G, quantique), l'approvisionnement en composants critiques, la maîtrise d'algorithmes sensibles, etc. Cette extension se poursuivra jusqu'à la prochaine décennie, avec des implications dont les contours restent difficiles à tracer.

Dans un contexte de « brutalisation numérique » de la vie internationale, l'UE s'est jusqu'à présent distinguée par sa qualité de superpuissance réglementaire, plus connue sous l'expression d'« effet de Bruxelles ». Cette préférence pour agir par la norme sur la scène internationale ne constitue pas une donnée inédite de la politique de l'UE. Ses succès en matière de protection des données personnelles et ses ambitions réitérées dans les sphères du commerce électronique ou de l'IA s'inscrivent dans cette logique. Toutefois, maintenir une influence normative suppose de préserver voire d'accroître ses capacités, ce que les États-Unis, et surtout la Chine, font déjà.

Une autre originalité du modèle numérique européen sera testée d'ici à la prochaine décennie – l'esquisse d'une « troisième voie » – entre les modèles californien et chinois, soit entre une vision dérégulée du numérique conduisant à un dévoiement du capitalisme et une approche basée sur un techno-étatisme décomplexé en matière de surveillance de masse. Cette voie intermédiaire aux contours insuffisamment précis met essentiellement l'accent sur la défense de valeurs européennes. En d'autres termes, l'Europe devrait, par rapport à l'« économie de l'attention » et à la « notation sociale » , proposer une autre voie fondée sur le respect des libertés fondamentales.

On peut toutefois critiquer l'approche même de l'UE : l'accord sur la spécificité de l'Europe en matière d'éthique et son exploitation diplomatique ne serait qu'un paravent à l'absence de véritable consensus entre États membres sur la politique industrielle, d'investissement et de formation à conduire. Exemplifiée par l'IA, la troisième voie numérique européenne peine à se dessiner face aux États-Unis et à la Chine qui promeuvent une conception techniciste du politique et qui voient dans l'IA le moyen de défendre leurs intérêts géopolitiques tout en contenant les tentations insurrectionnelles qui traversent leurs sociétés.

Déterminer si l'UE doit fonder sa stratégie numérique sur la seule morale deviendra une ligne de faille dans les rapports de puissances de ses États membres. Dans le même temps, le contexte de guerre politique menée contre l'UE par la Russie incite à un « retour des valeurs » , y compris dans le champ numérique, ce qui accélèrera les logiques de régionalisation technologique.

CHAMP

04

Fournisseurs *et services* numériques

prospective

Comme anticipé dans les ROS 2020 et 2021, la dépendance des entreprises européennes à leurs fournisseurs de services numériques ne s'est pas résorbée en 2022 malgré les évolutions réglementaires mises en œuvre au niveau de l'UE. L'oligopole dont jouissent les géants du numérique est cependant attaqué aux États-Unis et en Chine. La possibilité d'un effondrement de ces géants demeure lointaine mais nous avons particulièrement exploré cette hypothèse pour ce nouveau rapport.

FOURNISSEURS ET SERVICES NUMÉRIQUES

Les services numériques sont toujours entre les mains d'un faible nombre d'acteurs. **Cette situation oligopolistique se renforce, à la faveur de l'acquisition d'un grand nombre de petites entreprises par les géants du numérique**. Ainsi, en 2021, selon les données de Dealabs, Google a acheté 120 entreprises, Microsoft en a acquis 56, et Amazon 29. La valeur totale de ces fusions-acquisitions a atteint un nouveau record. Pour Google, elle est de 22 milliards de dollars, un record historique. Microsoft atteint les 25,7 milliards de dollars, un chiffre qui comprend les 19 milliards consacrés au rachat de la solution vocale intelligente Nuance. L'acquisition d'Activision Blizzard par Microsoft pour 70 milliards de dollars en janvier 2022 vient battre largement le record du rachat de LinkedIn en 2016 pour 26 milliards de dollars. Ce rachat risque de placer la firme de jeu vidéo de Microsoft dans une position dominante au sein de l'industrie vidéoludique. Cependant, toutes ces acquisitions aux montants faramineux éclipsent souvent le rachat de très nombreuses petites entreprises par ces géants du numérique, le problème étant que derrière ces petites acquisitions qui passent inaperçues car elles ne font pas l'objet d'enquêtes de la part de l'Autorité de la concurrence américaine, ce sont souvent des équipes d'ingénieurs et des brevets qui tombent entre leurs mains. Par ailleurs, l'autre enjeu de cette pratique de rachats concerne les acquisitions « tueuses ». Ainsi, entre 2015 et 2017, 60% des produits et services des entreprises rachetées par les GAFAM ont cessé d'être proposés à la vente sous leur nom d'origine (source : Maddyness). L'objectif de ces acquisitions tueuses est d'empêcher l'émergence de services concurrents et disruptifs sur le marché. Grâce à leur capacité d'achat, ces géants maintiennent ainsi leur domination sur le marché des services numériques. De plus, les clients de ces entreprises rachetées se trouvent dans une position de faiblesse au moment de la négociation de leurs contrats. Les fournisseurs peuvent alors leur imposer des clauses contractuelles en leur défaveur ou leur imposer des tarifs prohibitifs.

En effet, **les relations contractuelles entre clients et fournisseurs sont de plus en plus tendues**. En 2020, nous observions déjà que les clauses contractuelles favorisaient les fournisseurs. Depuis, les coûts de conversion dans le cloud ont rendu les entreprises dépendantes de ces acteurs dominants. Aujourd'hui, nous pouvons considérer que 40% de la charge de travail a été migrée dans le cloud (source : CIO online). Cette migration dans le cloud est surtout perçue par le prisme de la réduction des coûts. Ainsi, les opportunités de développement liées à cette migration ne sont pas envisagées. La réallocation des budgets vers la modernisation du SI n'a pas encore eu lieu, car les projets sont focalisés sur les infrastructures de migration. Les entreprises courent donc le risque de laisser s'ancrer, voire s'aggraver, les relations de dépendance aux gros fournisseurs étrangers qui proposent de nouveaux services à valeur ajoutée. Certaines entreprises utilisent déjà la notion de « *cloud stickiness* » pour évaluer leur degré de dépendance à un acteur du fait du déploiement de leur solution cloud. La résilience des entreprises par rapport à leurs fournisseurs doit donc être renforcée, notamment sur la maîtrise de leur dépendance. En 2021, l'invalidation du Privacy Shield mettait les entreprises dans une posture difficile à tenir sur le long terme, empêchant le transfert de données vers les Etats-Unis. En 2022, elles commencent à en expérimenter les conséquences. Ainsi, la CNIL a notifié aux entreprises qu'elles ne devaient plus utiliser les services de Google Analytics car l'utilisation de ce service entrainait le transfert de données vers les États-Unis.

FOURNISSEURS ET SERVICES NUMÉRIQUES

Par ailleurs, **la position hégémonique des géants du numérique est aussi maintenue grâce à leur forte capacité de lobbying**. Par exemple, l'association Gaia-X, dont l'objectif est de concevoir une infrastructure et un cadre d'architecture pour la circulation maîtrisée et sécurisée des données, compte comme adhérents les géants du numérique. Et pourtant, n'ayant pas leur siège social international en Europe, ils savent qu'ils n'auront pas accès au board de l'association Gaia-X. Ce projet européen est aujourd'hui en ordre de marche avec plusieurs publications à son actif, dont le document « *labelling Gaia-X criteria* » en avril 2022 qui vise à qualifier les offres de services au sein de Gaia-X en 3 niveaux. Cette publication répond aux besoins de confiance et de sécurité des producteurs de données et des utilisateurs de services numériques. Le niveau 1, appelé label 1, assure la transparence et le niveau de sécurité niveau 1 du schéma de certification de l'ENISA. Le label 3 demande l'immunité aux lois extraterritoriales des pays ne faisant pas partie de l'Union européenne, un niveau de sécurité cyber de niveau 3 et la maîtrise de la dépendance aux grands fournisseurs. Par ailleurs, la phase opérationnelle des travaux pour la constitution d'espaces de données se poursuit et s'accélère. Malgré la presse négative faite autour de Gaia-X, ce projet constitue aujourd'hui la seule opportunité pour répondre aux besoins des utilisateurs et des producteurs de données pour stocker, partager et valoriser leurs données grâce à des outils d'IA, de calcul et d'analyse dans un espace sécurisé et de confiance. En parallèle de ce projet, les entreprises et organisations publiques sont en quête de solutions de cloud de confiance pour réduire leur exposition aux risques géopolitiques, juridiques, et aux activités d'ingérence et de renseignement d'intérêt économique. En effet, elles s'accordent à dire qu'entre 15 et 35% de leurs données (source: étude auprès du groupe de travail « Cloud de confiance » du Cigref), avec une grande variabilité en fonction de leur secteur d'activité, ne peuvent pas migrer sur le cloud public. D'où leur besoin d'un cloud de confiance. Pour répondre à ce besoin, l'Europe lance des appels à projets avec European Cloud Alliance pour développer un cloud de confiance. L'idée de l'Europe est d'allier les opérateurs de cloud pour représenter une part plus importante de l'offre cloud en Europe. Des commandes publiques permettront de faire monter le niveau de l'offre si l'Europe s'y engage, comme le gouvernement américain l'avait fait avec AWS.

Pourtant, plusieurs solutions plus immédiates s'offrent aux entreprises pour réduire leur dépendance. Nous observions en 2020 que **les entreprises tentaient de réduire l'empreinte numérique des grands fournisseurs dans leur système d'information en recourant à des alternatives open-source**. Cette croissance de l'utilisation de l'open-source a perduré, notamment grâce à une amélioration de l'image de ces logiciels au sein des entreprises. Selon une enquête menée par Red Hat et publiée en début d'année 2022, 79% des responsables IT européens interrogés ont une perception plus positive de l'open source qu'un an auparavant. Cette perception positive de l'open source est cependant à nuancer, car les entreprises préfèrent toujours les grands fournisseurs de logiciels, surtout car ils facilitent la gestion des risques.

Pour réduire les dépendances et proposer des offres européennes de cloud, **une nouvelle pratique d'hybridation consiste à conclure des partenariats entre grandes entreprises françaises et géants du numérique**, chacun apportant une brique technologique. Pour ne pas être soumis aux lois extraterritoriales américaines, des partenariats locaux ont ainsi été conclus entre Microsoft, Capgemini et Orange d'un côté, et Google et Thales de l'autre (sources : Les Échos, mai 2021, Le Monde, octobre 2021). Il peut apparaître étonnant de continuer à lier des partenariats avec ces acteurs américains malgré une large prise de conscience des problématiques de dépendance à des acteurs oligopolistiques. Ces solutions apparaissent néanmoins comme des transitions vers des solutions purement européennes. Pour que ces partenariats soient profitables aux acteurs français, il faudra être vigilant au risque de vassalisation vis à vis des partenaires américains et veiller à la transmission des compétences auprès des équipes locales. Ces nouvelles offres hybrides sont aussi le signe de l'émergence de nouveaux modèles d'affaires, car elles modifient la relation entre client et fournisseur qui devient à la fois commerciale et partenariale. Cette évolution accroît encore les dépendances entre les deux acteurs. D'un autre côté, certaines offres purement françaises émergent pour répondre à des besoins particuliers, comme l'alliance entre Dassault Systèmes et Atos pour proposer une plateforme de cloud souverain de conception 3D.

La souveraineté numérique va au-delà de la proposition d'un cloud souverain européen. Ce sujet était au cœur de la campagne présidentielle 2022. Lors du « *pitch* » des candidats, un événement organisé par la plateforme programmatique « Convergences numériques 2022 », tous les candidats ont avancé des propositions pour accroître la souveraineté numérique de la France. Ce sujet est avant tout financier : **il faut augmenter les budgets pour accroître la souveraineté numérique au niveau français et européen**. L'*European Chips Act* propose un plan d'investissement de 50 milliards d'euros pour que l'Europe devienne leader dans la production mondiale de semi-conducteurs. L'Europe a une capacité financière limitée mais elle peut aussi compter sur les investissements étrangers. Par exemple, selon un rapport de Business France, la France n'a pas cessé d'être attractive pour les investisseurs en 2020, malgré la situation sanitaire. Ainsi, les investissements étrangers ont connu un recul de seulement 17%, contre 33% au niveau mondial. Le défi de l'Europe concerne donc la réindustrialisation, c'est-à-dire la capacité à déployer des usines dont le coût de production absorbe les coûts logistiques liés à la mondialisation des flux commerciaux.

veille prospective

En parallèle de ces évolutions, certaines tendances émergentes notées dès 2020 apparaissent renforcées et deviennent aujourd'hui des tendances structurelles de l'évolution des fournisseurs de services numériques. **La plateformisation de l'économie est une tendance qui se confirme année après année**. Le succès de ces plateformes repose sur leur capacité à diversifier leurs activités et à retenir leurs utilisateurs. Le succès de cette stratégie de plateformisation entraîne son déploiement vers de plus en plus de secteurs d'activités. Dans le rapport de 2021, nous notions que certains secteurs d'activité étaient en phase de recomposition vers une généralisation de la plateformisation, notamment dans les secteurs B2B. La santé a été un des premiers secteurs à entamer cette transition. Cette tendance se développe et englobe aujourd'hui d'autres secteurs comme le tourisme, avec la plateforme Alentour qui promeut le tourisme local, et l'agroalimentaire, avec la plateforme NumAlim. Cette évolution tend à effacer progressivement la frontière entre fournisseurs et clients. De plus en plus d'entreprises évoluent vers la proposition de services numériques, plutôt que de technologies. Pour accompagner cette transformation, les budgets augmentent en interne des entreprises pour le développement logiciel.

En 2020, nous observions également dans notre rapport **la volonté de la France et de l'Union Européenne de taxer davantage les GAFAM**. En 2021, l'Union Européenne est parvenue à appliquer davantage ses règlements, notamment le RGPD. La CNIL a sanctionné Google et Meta à hauteur de plusieurs millions d'euros pour non-conformité sur la collecte des cookies car ces deux entreprises ne permettent pas à l'utilisateur de supprimer la collecte de ces cookies sur leurs sites. Par ailleurs, l'amende infligée à Google en 2017 par la Commission européenne pour pratiques anticoncurrentielles à hauteur de 2,4 milliards d'euros a été confirmée en 2021 par le tribunal de l'UE, rejetant le recours de Google. L'entreprise américaine a encore la possibilité de contester cette décision devant la Cour de justice de l'UE, mais si l'Union Européenne parvient à imposer des sanctions aux GAFAM, c'est une bonne nouvelle pour les entreprises qui pourront se tourner vers le législateur pour lutter contre les conséquences de leur dépendance. Dans ce même sens, le *Digital Market Act* a fait l'objet d'un accord entre le Conseil et le Parlement européen en mars 2022, sa mise en œuvre aura donc lieu prochainement. Ce règlement, sur lequel travaille la Commission européenne depuis 2020, structure un cadre législatif pour réguler les pratiques des plateformes et services numériques et éviter les pratiques déloyales. L'ambition de la Commission est de réguler la concurrence sur les marchés numériques à travers un règlement qui cible les comportements économiques des entreprises à caractère systémique, de nature par exemple à enfermer leurs utilisateurs.

Ce durcissement réglementaire s'accompagne d'un développement de nouvelles instances pour faire face aux défis actuels et à venir en matière numérique. Ainsi, l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) en France est le nouvel organe régulateur dont l'objectif est notamment la lutte contre le piratage, la protection des mineurs, la lutte contre la désinformation et la haine en ligne, depuis l'adoption de la loi du 25 octobre relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique. Pour le moment, l'Arcom n'a pas encore pris de mesures pour lutter contre les contenus haineux en ligne.

Avec cette structuration et cette harmonisation croissantes des régulations, renaît donc une des principales incertitudes notées en 2020 qui questionnait **l'éventualité d'un démantèlement des grands acteurs du numérique par la voie réglementaire**. Les dernières prises de position de l'Autorité de la concurrence américaine vont dans ce sens. Inquiète de leur montée en puissance, la *Federal Trade Commission (FTC)* tente, en effet, de briser le monopole des grands acteurs du numérique par l'application des lois anti-trust. Jusqu'à présent les plaintes déposées à l'encontre de ces géants n'avaient pas reçu de réponses favorables de la part de la justice américaine, c'est maintenant chose faite. En janvier, une plainte déposée par la FTC a reçu un avis favorable de la justice fédérale. La procédure pourrait aller jusqu'au démantèlement de Meta, si l'entreprise de Mark Zuckerberg ne parvient pas à démontrer que son rachat de nombreux réseaux sociaux, comme WhatsApp et Instagram, ne relève pas de pratiques anticoncurrentielles et d'abus de position dominante.

FOURNISSEURS ET SERVICES NUMÉRIQUES

Le gouvernement américain n'est pas le seul à vouloir contrôler ses géants. **La Chine tente également de freiner l'ascension de ses méga-entreprises du numérique**. Depuis 2020, le gouvernement chinois impose ainsi de nouvelles lois aux entreprises chinoises pour éviter leur développement autonome à l'international, loin des intérêts du Parti communiste. La reprise en main de l'acteur chinois du e-commerce Alibaba a servi d'exemple. En novembre 2020, le Parti communiste chinois annulait l'introduction en bourse d'Ant Group, une filiale d'Alibaba dédiée aux services financiers. Cette introduction en bourse devait être une des plus importantes pour une entreprise chinoise. Dans ce cadre de tensions entre la société chinoise et son gouvernement, le créateur d'Alibaba, Jack Ma, disparaissait après avoir critiqué les banques publiques, pour réapparaître cinq mois plus tard. L'entreprise a été condamnée à 2,3 milliards d'euros pour abus de position dominante. Cette reprise en main du gouvernement chinois sert à contraindre les acteurs du numérique à servir les ambitions étatiques. Plus récemment, dans le cadre de la faille Log4Shell découverte par Alibaba, le gouvernement a sanctionné l'entreprise pour avoir prévenu en premier la société Apache avant le gouvernement chinois. En effet, l'exploitation d'une telle faille aurait pu être utile à l'espionnage mené par les organes gouvernementaux du pays.

Toutefois, malgré cette reprise en main des acteurs américains et chinois, la perspective d'un effondrement de ces géants du numérique demeure encore lointaine. Mais, si en 2020, le ROS faisait état de la faible probabilité de l'effondrement du système de spéculation économique permettant l'investissement financier essentiel à la croissance des géants du numérique, un nouvel événement advenu en 2022 est venu réinterroger cette probabilité. La chute du cours en bourse de Meta début février 2022 à hauteur de 26%, la plus forte baisse mensuelle du Nasdaq depuis deux ans, révèle, en effet, **l'instabilité financière de ces entreprises, soumises aux cours de la bourse et aux spéculations**. Cette baisse est due à une perte de 4 millions d'utilisateurs quotidiens de l'ex-Facebook, une première pour l'application dont le nombre d'utilisateurs ne faisait que croître depuis son lancement. Meta n'est pas la seule entreprise à avoir vu son cours en bourse baisser. Les géants du numérique ont perdu 800 milliards de dollars de capitalisation depuis le début de l'année 2022 (source : Siècle Digital).

L'ensemble de ces évolutions réglementaires et financières sont donc cruciales à suivre dans les mois et années à venir, en ce qu'elles pourraient, à terme, recomposer les rapports de force entre fournisseurs et clients de services numériques.

CHAMP

05

Nouvelles formes de travail et engagement des collaborateurs

prospecti

Sous l'impulsion donnée par la crise sanitaire, accélératrice de tendances préexistantes, **les collectifs de travail et le rapport au travail lui-même** continuent d'évoluer en profondeur dans les pays développés, et ce à plusieurs titres.

NOUVELLES FORMES DE TRAVAIL ET ENGAGEMENT DES COLLABORATEURS

D'un côté se dessine de plus en plus nettement **une catégorie de travailleurs sortis gagnants de la numérisation croissante des services, des usages et des pratiques de travail elles-mêmes**. Professionnels qualifiés, ils sont détenteurs de compétences très demandées, en particulier technologiques. Principaux bénéficiaires de la pénurie de talents qui frappe l'Europe, ils prétendent à des salaires de plus en plus élevés, qui pèsent inévitablement sur les stratégies de rentabilité des entreprises. Dans les métiers de la cybersécurité, de la donnée, du cloud, de l'intelligence artificielle et plus largement de la plateformisation des services, les savoir-faire manquent cruellement au sein de l'Union européenne. Par ailleurs, les exigences des employeurs se complexifient : les postes à pourvoir nécessitent, en effet, une plus grande diversité de compétences, notamment pour les postes en lien avec les fournisseurs de solutions technologiques, à la croisée des questions numériques, juridiques et géopolitiques. Sans adaptation, cette situation de pénurie des talents pourrait s'aggraver en France, déjà dans une situation critique, notamment au regard de l'abandon progressif de l'apprentissage des mathématiques chez les plus jeunes.

Par un effet mécanique inévitable, **le prix de ces compétences spécifiques croît et se corrèle à l'inflation économique** qui touche le secteur de l'énergie et des ressources critiques. Cette situation est amplifiée par **l'internationalisation du marché du numérique**. Les grandes entreprises débauchent directement les meilleurs talents à l'étranger tandis que, simultanément, les viviers d'employés situés dans les pays émergents diminuent, à mesure que ces professionnels prennent conscience de leurs leviers de négociation et réhaussent à leur tour leurs exigences en matière de rémunération. Ainsi, le cabinet Aravati signalait en novembre 2021 une augmentation de +10,6% en moyenne des salaires IT en France métropolitaine par rapport à 2020. De telles évolutions peuvent aussi entraîner **de fortes tensions au sein même des équipes** entre jeunes recrues qualifiées aux exigences salariales élevées et collaborateurs plus âgés. Face à ces phénomènes de pénurie et d'augmentation des salaires, les entreprises innovent dans le recrutement des jeunes collaborateurs en utilisant les réseaux sociaux et notamment Tik Tok pour attirer de nouveaux talents. Mais, le manque de profils hautement qualifiés oblige aussi les directions informatiques à déployer le *low code* ou le *no code* pour permettre à des profils peu techniques de développer leurs propres solutions informatiques. L'objectif à terme serait de déployer ces outils au sein des équipes métiers des entreprises sous la supervision de la DSI, en évitant au maximum le *shadow IT*, soit le déploiement par les équipes métiers d'outils informatiques échappant à leur contrôle.

NOUVELLES FORMES DE TRAVAIL ET ENGAGEMENT DES COLLABORATEURS

Par ailleurs, **une part croissante d'individus sont à la recherche de sens** dans leur activité professionnelle et d'un rééquilibrage entre leur temps de travail et leur temps privé. Les réseaux sociaux influencent de plus en plus les jeunes collaborateurs sur la perception qu'ils ont du travail. En témoigne le phénomène « *Quit my job* » sur Tik Tok (où de jeunes Américains se filment en train de démissionner), symptomatique du phénomène plus général de la « grande démission » particulièrement observé aux États-Unis. En 2021, plus de 31 millions de salariés américains ont ainsi quitté leur emploi, à la faveur de la crise sanitaire qui a participé d'une exacerbation de leur mal-être au travail. 40% d'entre eux n'avaient pas d'autre contrat en vue lorsqu'ils ont franchi le pas. En France, le nombre de démissions en CDI a bondi de 10,4% en juin 2021 et de 19,4% en juillet 2021 par rapport aux mêmes périodes en 2019. Les ruptures anticipées de CDD se sont elles situées 25,8% au-dessus du niveau atteint deux ans auparavant (Dares, 2021). Ce phénomène est aussi constaté dans les entreprises du secteur des services informatiques qui ont connu une vague record de démission (source : Les Échos, février 2022). Alors que les employeurs interrogés supposent que leurs salariés démissionnent à cause d'une situation de burn-out ou d'un mauvais salaire, les individus indiquent, en réalité, qu'ils quittent leur emploi parce qu'ils ont perdu de vue le sens de ce dernier et ne se sentent pas reconnus. Selon une enquête de l'Institut Montaigne, 42% des jeunes de 18-24 ans choisissent leur emploi « par passion », premier critère devant le salaire. Pour Goldman Sachs, **ce « mouvement antitravail »** pourrait relever d'un réel mouvement de fond et peser à l'avenir sur l'économie. Pour les entreprises, c'est un goulet d'étranglement supplémentaire. La perte d'intérêt des individus pour le système de salariat traditionnel, tel qu'il est encore majoritairement pensé aujourd'hui, renverse les rapports de force entre employés et employeurs.

Le télétravail imposé massivement pendant la crise sanitaire a par ailleurs entraîné des bouleversements durables dans la manière de concevoir le travail au sein des entreprises. Les générations nouvellement arrivées sur le marché n'auront ainsi jamais connu un mode de travail totalement en présentiel. La renégociation des contrats incluant le télétravail montre que ce modèle tend à s'imposer au sein des entreprises, y compris les plus réticentes. Ces dernières font d'ailleurs le constat général que leurs équipes ont des difficultés à revenir dans les bureaux malgré l'incitation de leurs managers. Les effets bénéfiques du télétravail sont maintenant largement connus : réduction du temps de transport, organisation personnelle facilitée... Cependant, les effets négatifs pour les entreprises et les collaborateurs sont aussi à prendre en compte. Dans les précédents rapports, nous avions mis en exergue les effets psychologiques néfastes du télétravail sur les salariés. À ces effets, s'ajoutent la difficulté pour les entreprises à diffuser un esprit de corps et une culture commune auprès des équipes éloignées des bureaux.Le télétravail empêche également une délimitation claire du temps de travail, phénomène accentué par l'usage des outils numériques qui permettent de joindre les collaborateurs à tout heure.

La généralisation du télétravail pose aussi la question de l'avenir du parc immobilier professionnel, la revente des bureaux inutilisés impactant le marché immobilier dans des quartiers jusqu'à présent largement occupés par les entreprises, comme le quartier de la Défense. Les entreprises basculent en effet de plus en plus vers un modèle *flex office*, qui ouvre des espaces modulables dans lesquels les collaborateurs peuvent s'installer au gré de leurs besoins. Le télétravail fait également le succès des espaces de *coworking* qui peuvent être loués par les entreprises pour réunir leurs équipes ou par le collaborateur lui-même pour travailler à côté de chez lui. Ainsi, l'entreprise WeWork qui avait connu des difficultés financières lors des deux dernières années, a annoncé des revenus supérieurs à ses estimations sur le premier trimestre 2022.

Face à ces bouleversements, les entreprises naviguent à vue, à la recherche de la meilleure formule pour **fidéliser leurs collaborateurs**, en particulier dans les domaines les plus concernés par la pénurie des talents, mais aussi pour conserver du lien à l'heure d'une numérisation croissante des relations de travail. Beaucoup se laissent aussi tenter par **l'usage du numérique comme moyen de contrôle des salariés**. Une note de l'OCDE affirmait, en novembre 2021, que les métiers de management seraient les plus bouleversés par le développement de l'intelligence artificielle et que 63% des entreprises françaises avaient déjà ou souhaitaient adopter des outils de supervision numérique de leurs collaborateurs pour organiser le travail à distance (source : OCDE, 2021). D'autres, à l'inverse, **encouragent l'auto-organisation au sein des équipes**, y compris dans quelques DSI qui mettent l'accent sur les *soft skills* plutôt que sur les *hard skills*. De la même manière, certaines parient sur de futures révolutions technologiques pour garantir la pérennité d'une culture d'entreprise commune (via le métavers par exemple, voir champ 1), quand d'autres souhaitent, au contraire, replacer l'humain et les relations sociales au cœur de leur modèle et s'intéressent, notamment, aux problématiques d'inclusivité.

À moyen-terme, les organisations devront très certainement continuer de **repenser le format et l'identité de leurs collectifs de travail** mais aussi envisager de nouvelles modalités de fonctionnement, par exemple pour intégrer et gérer des individus ne souhaitant pas se fidéliser. La possibilité de cumuler plusieurs activités salariées est une des pistes envisageables pour s'adapter à ces évolutions. Dans la même veine, **le concept de la semaine de quatre jours** tend déjà à se développer aujourd'hui dans plusieurs organisations qui souhaitent répondre aux attentes de leurs salariés en termes d'équilibre entre vie privée et vie professionnelle. L'Espagne a lancé, à l'automne 2021, une expérimentation de cette formule auprès de deux cents organisations avec, pour objectif, de l'étendre par la suite à toutes les entreprises nationales si elle s'avérait concluante. Globalement, les entreprises pourront avoir à développer une approche flexible et hyper-personnalisée de leurs employés.

Point de vue

LES CINQ FORCES DES LEADERS DE DEMAIN

« Face aux enjeux économiques, environnementaux, sociétaux, politiques et juridiques actuels, les dirigeant•e•s d'entreprise leaders de demain seront celles et ceux qui auront su tirer parti de cinq forces interdépendantes ».

Par Yves BERNAERT
Accenture Technology Europe CEO

La première est **la réinvention totale de l'entreprise**. Après le temps de la résilience, est venu le temps de renforcer les efforts afin d'assurer la pérennité de son activité face aux nouveaux imprévus. Grâce à une transformation compressée, les dirigeant•e•s peuvent allier l'optimisation des coûts et l'évolution des applications. Ainsi, le cloud, la data, l'AI sont devenus autant de technologies incontournables qui doivent être intégrées au cœur de l'entreprise. Or, même si l'intégralité des entreprises européennes ont réalisé leur migration sur les dernières années, seules 12 % d'entre elles exploitent le cloud à son plein potentiel.

La seconde est **la création et l'engagement des talents**. Dans un contexte de « grande démission », où les talents deviennent plus volatiles, il est indispensable de repenser l'expérience employé•e. Les dirigeant•e•s doivent s'attacher à recruter des talents qui, au-delà de leurs compétences métiers, partagent une curiosité et la conviction que la technologie est génératrice d'opportunités, car chaque entreprise est une entreprise technologique. Dans mon organisation par exemple, des programmes d'intrapreneuriat sont mis en place, permettant à nos collaborateur•ice•s de développer des prototypes qu'il•elle•s transformeront parfois en start up, contribuant à leur épanouissement personnel. Il leur a également été proposé d'adopter la semaine de 4 jours ou le télétravail à la carte, leur offrant plus d'autonomie et un meilleur équilibre vie professionnelle / vie personnelle.

La troisième est **le développement durable**. La majorité des entreprises se sont d'ores et déjà fixé des objectifs de responsabilité sociétale et environnementale pour répondre aux nouvelles attentes de leurs employé•e•s, client•e•s et partenaires, ainsi qu'aux nouvelles régulations. La technologie représente un outil formidable pour répondre à ces objectifs, en particulier de décarbonation et plus globalement aux objectifs de développement durable (ODD) fixés par les Nations Unies. Je prendrais pour exemple la filtration de l'eau aux UV mise en place par l'association 1001fontaines, que j'ai le privilège de présider. En facilitant un accès pérenne à l'eau potable aux populations vulnérables sur la base d'un modèle d'entrepreneuriat social, l'impact de 1001fontaines rayonne sur 9 des ODD.

La quatrième est **le métavers (Internet 3D)**, qui permet d'accélérer l'adoption d'une myriade de technologies, incluant la réalité virtuelle, le jumeau numérique, la blockchain, ou encore le « *edge computing* ». Révolutionnant déjà la façon dont nous vivons et travaillons, la question n'est plus de savoir s'il faut y être, mais comment y être. À l'instar des premiers sites Internet, les précurseurs du métavers gagneront le temps précieux de l'expérimentation pour devancer leurs concurrents. Certains leaders ont déjà passé le pas pour différents usages, comme Mars, Disney, BMW ou encore Nike.

Enfin, la dernière est **le continuum de la révolution technologique**. La technologie des sciences – celle de l'espace, de la *food tech*, et d'autres - sont autant de technologies innovantes qui auront un impact sur l'activité des entreprises. Pour l'heure, il n'est pas nécessaire de toutes les appréhender avec des convictions précises, mais au moins d'en mesurer le potentiel, seul ou au sein d'un écosystème de partenaires.

Créer un environnement pour que les gens osent entreprendre et laissent libre cours à leur imagination est, selon moi, LA clé de tous les possibles. Aussi conclurais-je en citant Marc Twain : « *Ils ne savaient pas que c'était impossible alors ils l'ont fait* ».

Mondialisation régulée par les équilibres géopolitiques
p.78

Vers une Europe puissance dans un monde régionalisé
p.82

Une Chine conquérante dans un monde bipolaire
p.86

Far West, colonies digitales et cartels numériques
p.90

02

Actualisation *des* scénarios *sur les futurs* numériques

OBJECTIFS ET AMBITIONS

À la suite de la veille prospective, le Rapport d'Orientation Stratégique paru en 2021 proposait quatre scénarios des futurs numériques à horizon 2030-2035.

Ces scénarios avaient été construits selon la méthode dite d'analyse morphologique, qui consiste à :

- **identifier les variables-clés du sujet étudié, ici les rapports de force politiques et économiques à échelle mondiale et européenne et leurs impacts sur le numérique à l'horizon 2030-2035;**
- **construire des hypothèses prospectives pour chacune de ces variables afin de couvrir le champ des possibles;**
- **construire des scénarios contrastés et plausibles à horizon 2030-2035 en combinant ces hypothèses.**

Ces scénarios sont donc des archétypes de mondes possibles, qui articulent de manière cohérente les éléments collectés via la veille présentée dans les champs de transformation. D'autres trajectoires pourraient, bien entendu, être tracées. Il est aussi envisageable que ces scénarios puissent coexister ou se succéder dans les quinze prochaines années. C'est particulièrement vrai concernant l'échelle européenne, où plusieurs trajectoires apparaissent possibles. Les configurations les plus extrêmes à horizon de 10-15 ans seraient la structuration forte de l'Union européenne, unie autour de politiques, de principes et de capacités technologiques communs ou alors, à l'opposé, sa dissolution progressive. Pour chacun des scénarios, des trajectoires-types très contrastées ont été choisies, mais ne préjugent pas de l'avenir de l'Union européenne. Elles cherchent plutôt à illustrer le carrefour auquel se tient l'UE aujourd'hui, confrontée à des choix décisifs pour son avenir, qu'ils soient politiques, économiques ou législatifs. Les décisions des États membres dans la décennie à venir auront d'importantes répercussions sur le visage de l'Europe en 2030-2035. Nous n'excluons pas, toutefois, la possibilité d'une trajectoire d'entre-deux à horizon 2030-2035, qui serait un mélange des récits contrastés présentés ici.

À l'aune des événements de l'année 2021-2022, les quatre scénarios prospectifs envisagés il y a douze mois apparaissent particulièrement robustes. Ils ont été actualisés grâce à une matrice, permettant de croiser les trajectoires qu'ils dépeignent avec les évolutions les plus récentes. Ils ont aussi été à nouveau soumis aux regards critiques d'experts et de membres du Cigref afin d'éprouver leur cohérence. Ils donnent à voir une large palette des futurs envisageables, au regard des nombreuses incertitudes auxquelles les organisations sont aujourd'hui confrontées. L'objectif de cette partie est donc de lister, dans un premier temps, ces incertitudes, puis d'actualiser et de réévaluer la vraisemblance des scénarios, afin d'offrir des clés de lecture des événements les plus récents aux lecteurs et de proposer quelques réflexions stratégiques sur cette base aux membres du Cigref, exposées dans le troisième et dernier volet de ce rapport.

Les scénarios présentés ici sont une version synthétique et actualisée des scénarios développés plus extensivement dans le Rapport d'Orientation Stratégique publié en 2021, accessible librement en ligne.

DE NOUVELLES INCERTITUDES ONT ÉMERGÉ

Difficile d'ouvrir une réflexion sur les mondes numériques possibles, et donc, nécessairement, sur les rapports de force internationaux, sans mentionner la guerre déclenchée par la Russie en Ukraine, en février 2022. Ce conflit, dont l'issue est encore incertaine, pourrait, néanmoins, rebattre en profondeur les cartes géopolitiques et géoéconomiques pour les dix prochaines années. Parmi les nombreux points d'attention, retenons ainsi :

Le futur incertain de la Russie. Le pays a, certes, remis l'idéologie au cœur des relations internationales, et ce au détriment de toute rationalité économique, prenant ainsi l'Europe au dépourvu. Néanmoins, la Russie voit peser sur son économie de lourdes sanctions internationales et mène une guerre, semble-t-il, au-dessus de ses moyens humains et matériels. Ainsi, entre janvier et avril 2022, la Russie enregistrait un excédent commercial de 95 milliards de dollars grâce à la hausse des prix du blé et des énergies, mais a vu sa monnaie plonger de 16% en mai 2022 (source : Les Échos, mai 2022).

Les implications stratégiques de cette guerre pour l'Union européenne. Si, d'un côté, l'UE a montré sa capacité à faire bloc et à avancer rapidement sur de nombreux sujets jusque-là enlisés (sur les questions de défense européenne, d'autonomie), elle reste, de l'autre, dépendante de la Russie (en termes énergétiques notamment), des Américains (pour garantir sa sécurité à moyen-terme) mais aussi de la Chine (dépendante à 52% en matière d'importation de produits stratégiques, données de la Commission européenne, 2021). Or les États membres sont inégalement affectés par cette situation, ce qui entraîne des tensions au sein de l'Union.

Le rôle prudent de la Chine dans ce conflit. La Chine cherche, semble-t-il, à protéger ses relations diplomatiques et économiques avec l'ensemble de ses partenaires, mais observe attentivement le déroulement de la guerre puisqu'elle est elle-même enlisée dans un conflit territorial avec l'île de Taiwan, qu'elle pourrait décider d'attaquer. Fin mai 2022, le président américain a affirmé pour la première fois depuis un demi-siècle avec grande clarté que les États-Unis seraient prêts à entrer en guerre pour défendre la souveraineté de l'île si nécessaire. Cette déclaration a participé à l'exacerbation des tensions avec la Chine. Cette dernière a ainsi rappelé à maintes reprises son soutien diplomatique à la Russie.

Les positions internationales plus fermes des États-Unis. Les USA pourraient, eux aussi, profiter de ce conflit, notamment pour réaffirmer leur influence en Europe, grâce à l'affaiblissement de la puissance russe. Ces derniers voient, en effet, l'OTAN se consolider avec la candidature historique de la Finlande et de la Suède, alors que l'alliance était considérée, il y a peu, en état de « mort cérébrale ». Les Américains pourraient aussi bénéficier de la demande européenne accrue en matières premières (céréales, gaz). De fait, les prises de position des officiels américains sur la situation ukrainienne, mais aussi sur Taïwan, sont de plus en plus tranchées et engagées. Est-ce la fin de l'*America First* et le retour de la puissance militaire étasunienne sur la scène internationale ? À court et moyen-terme, les midterms et l'élection présidentielle de 2024 pourraient changer la donne, si les forces partisanes d'un repli nationaliste reprenaient le dessus.

Les conséquences en cascade de la guerre sur les chaînes d'approvisionnement, les équilibres géoéconomiques internationaux et donc sur la stabilité de certaines industries, ainsi que de certains pays ou régions. Les pénuries de blé et la hausse des prix de l'énergie pourront avoir des répercussions sans précédent et sur le long-terme dans certaines zones du Moyen-Orient (Liban...), du bassin méditerranéen (Égypte...), dans la bande sahélienne et en Amérique latine, très dépendantes de l'Ukraine et de la Russie. Rappelons que le mouvement social et révolutionnaire du Printemps arabe, débuté en 2010 et jusqu'en 2012 dans plusieurs pays d'Afrique du nord, avait pour cause, entre autres, la hausse des prix alimentaires liée à l'arrêt des exportations russes en raison d'une canicule. De tels phénomènes déstabilisateurs pourront aussi être observés dans le secteur du numérique dont les infrastructures (réseaux, centres de stockage) deviennent de véritables actifs stratégiques. En témoignent les mouvements inquiétants de troupes russes au-dessus de câbles internet transatlantiques. Les matières premières essentielles à certains composants numériques sont déjà et pourront être de plus en plus menacées de pénurie à l'avenir. L'industrie des semi-conducteurs est, par exemple, très dépendante du néon purifié qui vient principalement d'Ukraine. Selon la Banque mondiale, le prix des métaux devrait quant à lui augmenter de 20% en 2022 et rester durablement élevé jusqu'en 2024 au moins, et ce quelle que soit l'évolution du conflit. Enfin, cette guerre pourrait participer d'une aggravation des affrontements cyber.

La résolution incertaine, enfin du conflit lui-même et ses conséquences sur le multilatéralisme international. Cette guerre pourrait-elle participer à une prise de conscience globale de l'importance de mettre à jour les mécanismes de prévention et de résolution des conflits ? ou à l'inverse va-t-elle participer à une fracture toujours plus profonde entre de grands blocs régionaux de plus en plus antagonistes ?

À ces incertitudes liées spécifiquement à la guerre Russie-Ukraine, s'ajoutent d'autres interrogations à horizon des quinze prochaines années, qu'il s'agit ici de rappeler en ce qu'elles participent à l'environnement instable dans lequel doivent évoluer les organisations. Parmi celles-ci :

Le futur de la Chine interroge, après deux ans de crise sanitaire qui ont vu le pays se replier très significativement sur lui-même, avec une reprise économique en dents de scie (même si spectaculaire dès la fin 2020) et la mise à l'arrêt de plusieurs grands projets internationaux. À moyen-terme, la Chine devrait, par ailleurs, être confrontée à des défis de plus en plus problématiques, susceptibles de l'affaiblir sur la scène internationale : une pénurie de main d'œuvre d'une part, liée à la diminution de sa population active et qui devrait s'aggraver dans un contexte où le gouvernement ne parvient pas à infléchir la trajectoire d'effondrement démographique générée par des décennies de politique de l'enfant unique, une crise climatique et environnementale d'autre part, avec de possibles répercussions économiques et politiques majeures.

Le poids et le rôle joués par plusieurs puissances aujourd'hui dites intermédiaires dans les relations internationales pourraient être appelés à se transformer significativement : la croissance démographique et économique en Inde, et, plus globalement dans l'Asie du Sud-Est, pourraient, par exemple, participer à un basculement des rapports de force globaux.

Le futur des méga-projets du numérique, promus notamment par de très grandes entreprises américaines, pose question dans un contexte marqué par les tensions sur les matières premières, les pénuries sur certains composants critiques, et, plus globalement, les crises environnementale et économique, qui obligent à repenser les priorités collectives en matière d'investissements. Les géants du numérique ne sont évidemment pas prêts de disparaître du paysage politique et économique. Mais si l'informatique quantique, l'intelligence artificielle, voire les métavers sont appelés à prendre de l'ampleur dans les années à venir, savoir pour qui et dans quelles conditions ces technologies seront développées reste une question en suspens.

SCÉNARIO

10

Mondialisation régulée *par les* équilibres géopolitiques

Actualisation des scénarios numériques sur les futurs

En 2035, la pandémie Covid-19, mais surtout la guerre qui a opposé la Russie à l'Ukraine, ont servi de déclics pour les États et pour leurs populations dans leur approche des grands enjeux planétaires. Après quelques années très mouvementées, marquées notamment par cette crise intense aux portes de l'Europe, qui s'est vue proche d'un conflit armé généralisé, les pays ont réussi à mettre en place de nouveaux instruments de régulation contraignants similaires à ceux développés à la fin de la Seconde guerre mondiale. Les institutions internationales en sortent renouvelées et renforcées. Les normes et traités actés à cette occasion s'appliquent dans le domaine sanitaire et environnemental bien sûr, mais aussi économique, militaire et cyber. Ils renforcent les Accords de Paris dans une approche intégrée de la santé humaine, animale et environnementale, encadrent strictement la prolifération des armes, initient une communauté internationale du cyberespace et favorisent la reprise des échanges commerciaux. Dans ce contexte, les tensions entre la Chine et les États-Unis persistent mais sont limitées grâce à leurs nombreuses interdépendances et s'expriment plutôt par des jeux d'influence et de *soft power.* Consolidée par la réaction unanime des États membres face à l'intervention russe des années 2022, l'Union européenne profite de ce contexte international de plus en plus favorable. Elle affirme progressivement son leadership et sa souveraineté, tout en maintenant des liens étroits avec l'Asie (notamment la Chine) et les États-Unis, consciente de la nécessité de trouver un juste équilibre entre ces géants géopolitiques et leurs giga-entreprises du numérique, afin d'assurer sa relative indépendance.

MONDIALISATION RÉGULÉE PAR LES ÉQUILIBRES GÉOPOLITIQUES

Aujourd'hui, ce scénario paraît renforcé, entre autres par le poids des enjeux géoéconomiques dans l'équilibre des forces, qui apparaît clairement à l'aune de la guerre entre l'Ukraine et la Russie. La Chine, par exemple, choisit d'adopter une position prudente vis-à-vis de l'intervention russe pour préserver en priorité ses intérêts économiques. De même, les Européens et leurs entreprises sont de plus en plus favorables à une résolution rapide du conflit. Les sanctions contre la Russie participent d'une approche des relations internationales fondée sur les rapports de force économiques. Si la crise en Ukraine devait durer, voire s'aggraver, elle pourrait aussi être à l'origine d'un sursaut international pour consolider les institutions qui permettent de maintenir la stabilité globale.

Par ailleurs, la crise sanitaire puis la guerre en Ukraine ont toutes deux montré la capacité de mobilisation des pays (notamment au sein de l'UE) et de la société civile pour répondre activement à des menaces collectives mais aussi pour faire preuve de solidarité, illustrée, par exemple, par les dispositifs mis en œuvre pour accueillir les réfugiés ukrainiens. En ce sens, les technologies de l'information et de la communication ont largement permis de nourrir les échanges entre autorités politiques et scientifiques, mais aussi entre associations et citoyens, et de partager les connaissances et les moyens disponibles pour faire face aux dangers communs.

Ce scénario perd néanmoins en vraisemblance, puisqu'à l'heure où nous écrivons ce document, la réalité de la guerre aux portes de l'Union européenne est pour le moment révélatrice de l'échec des grandes puissances à réguler les conflits et à les endiguer. Elle montre aussi qu'au-delà de la rationalité économique, il existe toujours des lectures idéologiques du monde, qui sont de réelles forces motrices pour certains acteurs. Par ailleurs, les conséquences de la guerre risquent d'être critiques en termes de relance de l'économie mondiale et d'accès à l'énergie et aux ressources stratégiques à échelle internationale, avec de profondes recompositions à anticiper pour les chaînes de valeur. Cette situation vient s'ajouter aux conséquences latentes de la pandémie notamment en termes de précarisation et d'accroissement des inégalités, et aux effets actuels et à venir du réchauffement climatique. Les 10-15 prochaines années semblent donc nous conduire vers une instabilité croissante, propice à de nombreux affrontements ou conflits, y compris sous-jacents, avec l'affirmation de nouvelles formes de guerre cyber plus que jamais d'actualité et une hybridation toujours plus forte des mondes civils et militaires.

SCÉNARIO

02

Vers *une* Europe puissance dans *un* monde régionalisé

Actualisation des scénarios numériques sur les futurs

En 2035, les répercussions de la crise sanitaire, les traductions disparates du réchauffement climatique aux échelles locales mais aussi les divergences profondes entre États révélées par la guerre en Ukraine ont participé d'une régionalisation des rapports de force et des relations économiques entre pays. Cette fragmentation s'exprime dans les politiques, les normes et la situation économique des plaques régionales ainsi constituées. Elle s'accompagne aussi d'une dissolution progressive des grandes organisations internationales. Incapables de trouver un terrain d'entente, les grands États se concentrent sur leur souveraineté et leur autonomie propres, dans une logique de chacun pour soi assumée. Les chaînes de valeur et d'approvisionnement se restructurent à de plus petites échelles. La mobilité internationale est durablement entravée. Cette tendance à la régionalisation se traduit aussi dans le numérique, organisé et régulé de manière hétérogène en fonction des plaques régionales. Dans cette trajectoire, l'Union européenne, profondément secouée par le conflit des années 2022 à ses frontières, s'est fortement mobilisée pour affirmer son indépendance. Les États membres ont poursuivi et développé leurs stratégies de mise en commun des ressources, de réindustrialisation, et d'autonomie stratégique, y compris dans le domaine numérique. Ils ont aussi enfin initié et financé une politique de défense européenne tant physique que cyber. L'Europe s'affirme donc progressivement comme une puissance politique à part entière. Mais dans ce scénario, les tensions sont fortes et continues entre les plaques régionales en raison des crises environnementales voire politiques qui se succèdent, en l'absence d'approches internationales coordonnées de ces enjeux globaux.

VERS UNE EUROPE PUISSANCE DANS UN MONDE RÉGIONALISÉ

Au regard des événements récents, ce scénario apparaît considérablement renforcé. Les années 2021-2022 ont, en effet, largement été marquées par une approche désynchronisée des politiques de gestion de la pandémie Covid-19. Malgré les promesses des États les plus riches, les taux de vaccination restent, par exemple, extrêmement variables en fonction des pays, excepté en Europe où la situation est relativement homogène. Cette disparité entre les régions du monde s'accompagne de situations de précarité économique et sociale très disparates selon les pays, avec le continent africain, l'Amérique du Sud, une partie des pays du Moyen-Orient considérablement fragilisés par la crise sanitaire. Cette dernière a, par ailleurs, durablement affecté les chaînes d'approvisionnement mondiales, conduisant à des situations de pénurie sur le long-terme, comme l'a montré, par exemple, la crise des semi-conducteurs. En parallèle, plusieurs États ont affirmé leur politique de réindustrialisation et donc d'autonomie, notamment la Chine qui s'est fortement repliée sur son marché intérieur, mais aussi les États-Unis et l'Europe. De même, plusieurs États réorganisent leurs priorités et se sont retirés de certains territoires, participant à la régionalisation de problématiques toujours irrésolues (Afghanistan, Mali…). À cette situation déjà instable se greffe la guerre en Ukraine et ses répercussions majeures et là aussi hétérogènes en fonction des régions et des populations. L'intervention russe confirme malheureusement l'hypothèse émise en 2021 selon laquelle certaines puissances pourraient profiter d'une situation de déstabilisation internationale générée par la crise Covid-19 pour intervenir dans leur environnement proche et affirmer leur volonté de puissance. Les réactions des autres pays à l'attaque russe participent alors à la régionalisation du monde (abstention de plusieurs pays en développement à l'ONU pour condamner la Russie, exclusion de la Russie du SWIFT, essor de l'internet russe, renforcement des liens potentiels entre la Chine et la Russie… etc.). La possibilité de voir d'autres États s'engouffrer dans la brèche ouverte par la Russie est non nulle (Turquie, Chine…). Enfin, les conséquences de la guerre vont participer à l'aggravation des tensions préexistantes dans certaines régions du monde (pénuries, famines…).

En parallèle de ces évolutions géopolitiques, l'Union européenne a consolidé ses positions face aux grandes entreprises du numérique et face aux acteurs étrangers au sens large (sanctions contre la Chine, contre la Russie). Le conflit a aussi ranimé la conscience européenne et rappelé l'importance de consolider son indépendance, y compris du point de vue militaire, même si les objectifs sont encore loin d'être atteints. De fait, l'UE renforce ses liens avec les États-Unis, ce qui participe du renforcement d'un bloc occidental sous égide américaine.
Enfin, d'ici 15 ans, de nouvelles puissances pourraient très largement s'affirmer notamment dans la région indo-pacifique (Inde, Indonésie) participant d'une évolution des rapports de forces régionaux.

NB. Comme en 2021, deux trajectoires apparaissent envisageables pour l'Union européenne dans un environnement global dégradé. La première, celle de sa consolidation progressive, est présentée dans ce scénario. La seconde, celle de son éclatement, est illustrée dans le scénario 3. Ces deux trajectoires apparaissent également vraisemblables à horizon 2035.

SCÉNARIO

03

Une Chine conquérante dans un monde bipolaire

Actualisation des scénarios numériques sur les futurs

En 2035, dans un contexte environnemental, sanitaire et géopolitique très instable, la Chine s'est affirmée comme leader des échanges internationaux. Face à la multiplication des crises, elle développe et diffuse son modèle de gestion coercitive et hyper-technologisée des problématiques, en prenant appui sur ses réseaux commerciaux et diplomatiques, établis dans le monde entier et sur tous les continents. Elle a aussi su tirer parti de la guerre en Ukraine, en renforçant ses liens économiques avec une Russie affaiblie, voire en négociant une redéfinition du statut de Taïwan dans un contexte mondial troublé. Les États-Unis, toujours concentrés sur la région Indo-Pacifique, voient d'un mauvais œil cette montée en puissance chinoise. Les tensions sont extrêmement fortes entre les deux blocs. Les cyber-attaques notamment explosent et les entreprises en pâtissent directement. Est demandé à ces dernières de choisir un camp, sur la base d'arguments principalement idéologiques. Dans ce contexte, l'Union européenne, considérablement diminuée par les répercussions de la guerre Russie-Ukraine, connaît une situation économique et politique précaire, qui l'oblige à accroître sa dépendance à des acteurs étrangers. Incapables de s'accorder sur la stratégie à adopter, les États membres adoptent des stratégies divergentes qui fragilisent d'autant plus la communauté européenne.

UNE CHINE CONQUÉRANTE DANS UN MONDE BIPOLAIRE

Au regard des événements récents, ce scénario apparaît considérablement renforcé. Ainsi, depuis l'été 2021, les tensions vont croissant dans la région indo-pacifique. La Chine a mis en œuvre un embargo sur les denrées australiennes, tandis que les Américains signaient l'alliance AUKUS dans la région et vendaient leurs sous-marins aux Australiens, participant à une course aux armements accompagnée d'un durcissement du discours sur Taïwan. L'Europe, elle, se trouve marginalisée dans le Pacifique, et peine à asseoir sa stratégie propre.

En parallèle, la Chine bénéficie d'avantages non-négligeables en termes d'accès aux ressources stratégiques sur son territoire. Ses stratégies d'investissements la placent aussi en tête du marché mondial du numérique à horizon 2030-2035 (notamment dans le cadre du développement de l'informatique quantique par exemple). Par ailleurs, la forte reprise en main des acteurs numériques chinois par le Parti et le verrouillage du pays mis en œuvre par le pouvoir justifié par la lutte contre le Sars-Cov2 révèlent la capacité de la Chine à conserver le contrôle sur sa population, ses entreprises et les puissances étrangères.

Enfin, là encore, les conséquences du conflit Russie-Ukraine pourraient largement participer à la réalisation de la trajectoire envisagée. La scission internationale entre pays qui soutiennent la Russie (ou ne disent rien) et pays qui critiquent fermement pourrait participer à la bipolarisation du monde entre un Occident affaibli d'un côté et un bloc de pays non-alignés dont la Chine pourrait être le leader (notamment au regard de ses investissements massifs dans les pays en développement). Quant à l'UE, même si elle a donné une réponse unanime aux actions russes, elle peine encore à structurer sa politique de défense. Certains États membres sont visiblement incapables de réduire leur dépendance à la Russie. D'autres envisagent de faire évoluer leur dépendance en nouant de nouveaux partenariats avec les États-Unis. Une trajectoire plus sombre pour l'Europe n'est donc pas à exclure.

SCÉNARIO

04

Far West, *colonies* digitales *et* cartels numériques

Actualisation des scénarios numériques sur les futurs

Entre 2030 et 2035, l'environnement global s'est profondément et rapidement dégradé. Déjà fragilisés par des crises sanitaires à répétition, un conflit armé enlisé aux portes de l'Europe, ou encore des vagues régulières de réfugiés, la plupart des États sont en grande difficulté financière, voire pour certains en faillite. En l'absence de moyens suffisants, les stratégies internationales coordonnées de gestion des enjeux globaux sont à l'arrêt. Dans ce contexte, les giga-entreprises du numérique, seuls acteurs à bénéficier encore d'une grande puissance d'investissement, s'imposent comme partenaires de premier choix pour plusieurs pays et entreprises, y compris en Europe. Elles diversifient leurs activités et leurs services, remplaçant, dans certains cas, les institutions publiques qui les fournissaient. L'Union européenne connaît, dans ce scénario, une trajectoire sombre, marquée par une grave crise économique et une subordination à ces entreprises étrangères puissantes.

FAR WEST, COLONIES DIGITALES ET CARTELS NUMÉRIQUES

Ce scénario apparaît aujourd'hui renforcé par la situation de déstabilisation internationale générée par la pandémie puis par la guerre en Ukraine et la multiplication voire la combinaison des crises (cf. la vague de chaleur en Inde qui menace ses récoltes et réduit encore la disponibilité du blé à échelle mondiale), avec une hausse des prix des matières premières qui participe, entre autres, au risque d'effondrement de plusieurs États. La paupérisation des populations, le ralentissement de l'économie pourraient favoriser les acteurs économiques les mieux dotés, comme les giga-entreprises du numérique qui connaissent, elles, une situation relativement stable.

Par ailleurs, le risque de voir le conflit entre la Russie et l'Ukraine s'enliser, voire escalader (plus de pays impliqués, armes non-conventionnelles utilisées...) reste une hypothèse non négligeable.

Mais ce scénario perd néanmoins en vraisemblance, dans un monde où les États réaffirment leurs capacités régaliennes plus que jamais, contre les acteurs du numérique mais aussi face aux crises actuelles et à venir, ravivant, notamment la notion de planification pour répondre aux enjeux majeurs rencontrés. Face aux grands risques des quinze prochaines années, les États, leurs instruments de régulation et de financement apparaissent aussi de plus en plus comme les assureurs de dernier ressort.

03

Messages clés *pour les* organisations

NAVIGUER DANS UN MONDE D'INCERTITUDES

Cette année encore, le Cigref a innové pour sa nouvelle édition du ROS. Afin d'inscrire plus encore ses travaux prospectifs au cœur des réflexions stratégiques de ses membres, des ateliers d'immersion pour chacun des scénarios leur ont été proposés. Ces ateliers, dont la méthodologie plus détaillée est présentée en annexe, ont permis, en sus de la veille prospective (partie 1) et de l'actualisation des trajectoires envisageables à horizon 2035 (partie 2) de stabiliser dix messages-clés pour les directions du numérique. Ces messages-clés ont pour ambition d'aider les DSI à se préparer aux transformations à venir. Les partager fait donc partie de la mission d'intérêt général que s'est fixée le Cigref dans le domaine numérique.

D'ici 2035, les directions du numérique des organisations ne devront plus simplement se préparer aux crises mais à leur enchaînement, voire à leur conjonction.

Dans la décennie à venir, au regard des dégradations environnementales et des trajectoires chaotiques de certaines régions du monde, il est certain que de nombreux événements viendront une nouvelle fois déstabiliser les activités des organisations au même titre que la crise du Covid-19 et le conflit entre la Russie et l'Ukraine. Pour se préparer aux quatre scénarios, et plus généralement à la multiplication de crises locales comme internationales, se succédant ou simultanées, les organisations, et particulièrement les directions du numérique devront assurer la sécurisation de leurs chaînes d'approvisionnement et de leurs ressources stratégiques (e.g. métaux critiques), le management de leurs ressources matérielles et humaines (mesures sanitaires, adaptation aux situations personnelles etc). Le numérique est en effet devenu une infrastructure critique.

Ces évolutions obligeront les organisations à mettre en place des mesures de sécurité leur permettant d'assurer leur fonctionnement malgré des ruptures dans les chaînes de valeur, via de nouveaux partenariats (avec de gros acteurs industriels comme avec des entreprises locales), mais aussi à développer leur autonomie en approvisionnements, par exemple énergétiques. Pour se préparer à de telles transformations, les organisations auront à mieux connaître leurs vulnérabilités et leurs dépendances, et à les anticiper grâce à des outils de suivi et de mesures. Elles pourront aussi développer ou renforcer leur direction spécialisée en anticipation et gestion de crises, notamment sur le volet prospectif.

Dans ce contexte, les directions du numérique pourraient avoir à réinventer leur système de gestion des risques, notamment leurs systèmes de protection face aux cyberattaques et aux risques hybrides, si les assurances traditionnelles ne sont plus en mesure de couvrir ces risques.

Ce contexte d'incertitudes et la criticité croissante du numérique est vecteur de nombreux risques pour les organisations. Pour y faire face, ces dernières ont généralement recours à des assurances. Cependant, les risques hybrides et non-conventionnels, tels que les cyberattaques, sont aujourd'hui mal couverts par les assurances. Ces dernières se transforment progressivement en système d'assistance, aidant les entreprises à traverser la crise, plutôt que d'indemniser leurs pertes d'exploitation. Si les assurances traditionnelles ne parviennent pas à proposer une offre plus holistique et systémique, les organisations devront réinventer leur système de gestion des risques, conjointement avec leurs directions du numérique, en ce qui concerne les cyberattaques.

L'évolution actuelle du système des cyberassurances est plus largement évoquée dans le champ de transformation 3.

D'ici 2035, les organisations et leurs directions du numérique seront de plus en plus partie prenante des systèmes de sécurité des États en temps de crise.

En 2035, quelles que soient les trajectoires envisagées, les États auront besoin de s'appuyer sur leurs entreprises nationales pour faire face à la multiplication des crises hybrides décrites ci-dessus. Dans l'hypothèse d'une Europe désunie et impuissante face à l'évolution des dynamiques géopolitiques et économiques (scénarios 3 et 4), les entreprises pourraient même prendre le relais sur des activités autrefois prérogatives de l'État. Mais, dans les scénarios où l'Europe maintiendrait sa puissance (1 et 2), les États pourraient aussi chercher du soutien auprès des entreprises pour les accompagner face aux crises. Les opérateurs de services essentiels (OSE) tels que décrits dans la directive NIS, et dont la liste s'est étendue dans la directive NIS 2, seront particulièrement impliqués dans la cyber-résilience des États membres de l'UE.

Pour se préparer à cela, les entreprises pourraient inventorier leurs ressources matérielles et humaines en interne, capables de participer aux systèmes de sécurité étatiques. Par exemple, l'entreprise pourrait lister le nombre de personnes ayant des compétences cyber capables d'agir en cas de cyberattaque massive sur des infrastructures d'intérêts vitaux ou encore le nombre de réservistes parmi ses collaborateurs. En temps de crise, ces ressources pourraient en effet être réquisitionnées par l'État pour participer à l'effort national.

D'ici 2035, les directions du numérique des organisations devront s'adapter à la régionalisation des normes, des réglementations et des chaînes de valeur. Cette régionalisation aura des impacts sur l'accessibilité des matières premières, le développement des infrastructures numériques et la gestion des bases de données.

La question de la régionalisation des chaînes de valeur, des normes et des réglementations est particulièrement illustrée dans les scénarios 2 et 3, dans lesquels le monde pourrait être divisé en plaques régionales, porteuses de normes et de réglementations différentes. Pour faire face à cette régionalisation, les directions du numérique devront faire des choix stratégiques pour s'adapter à la diversité des régulations régionales en termes d'accessibilité, d'usage, de développement des infrastructures, des outils et des bases de données.

Par exemple, sur un marché mondial, une entreprise du secteur de l'automobile pourrait avoir à prendre en compte la question des normes et des standards qui seraient appliqués sur chacune des plaques régionales, pour recharger les voitures ou les opérer. On peut, en effet, imaginer des normes sur la recharge électrique des véhicules du futur, lesquelles diffèreraient selon les pays et la plaque à laquelle on appartient. On peut également supposer qu'il existera des normes différentes au sujet des batteries. Une adaptation aux normes de chacune des plaques régionales serait alors nécessaire pour se maintenir sur chacune d'entre elles.

Cette régionalisation des chaînes de valeurs nécessitera une adaptation plus grande de la part des multinationales, qui devront surement faire un choix entre les différentes plaques géographiques sur lesquelles elles opèrent, et développer leur indépendance en fonction des évolutions des alliances géoéconomiques et géopolitiques.

D'ici 2035, les directions du numérique devront de plus en plus pondérer leurs choix d'investissements technologiques avec des critères tant environnementaux que de maîtrise des dépendances stratégiques.

Les organisations et leur direction numérique sont parties intégrantes de la lutte contre la crise climatique, y compris en termes de préservation de la biodiversité et des ressources naturelles, et sont amenées à se positionner davantage pour réduire les émissions de gaz à effet de serre. Elles sont attendues plus précisément sur :

- Leur utilisation d'énergies bas carbone ;
- Le développement d'innovations respectueuses de l'environnement ;
- L'allongement de la durée de vie de leurs équipements.

En plus de prendre en compte ces critères environnementaux, les organisations devront de plus en plus clarifier leurs relations aux grosses entreprises du numérique chinoises et américaines. En effet, la domination oligopolistique des géants du numérique américains est une tendance lourde à prendre en compte par les organisations pour réduire leur dépendance d'ici 2035. Ces questions devront être posées suffisamment en amont de l'implantation d'une technologie. Par exemple, l'adoption du projet de métavers par Meta pose les jalons d'une forte dépendance future, du fait des investissements qui y sont associés. Ainsi, plusieurs options pourraient être investiguées par les organisations pour diminuer leurs dépendances, comme :

- Recycler leurs *devices* pour diminuer les besoins en ressources nouvelles
- Se rapprocher des autorités publiques pour sécuriser leurs approvisionnements ;
- Fonder un groupement d'entreprises du même secteur pour disposer d'un levier de pression plus important contre les giga-plateformes du numérique, notamment dans les secteurs industriel et de l'énergie ;
- Agir à l'échelle européenne pour exiger des investissements massifs dans les secteurs d'avenir et des réglementations strictes contre les géants du numérique et pour aider les entreprises à rester indépendantes face aux grandes puissances.

L'arrivée de l'informatique quantique, plus rapidement que prévu, et celle des métavers font partie des grandes ruptures conceptuelles envisageables dans les 10 prochaines années que les directions du numérique peuvent anticiper et auxquelles elles doivent donc se préparer.

L'informatique quantique et les métavers sont les deux réalisations technologiques émergentes identifiées comme particulièrement stratégiques pour les organisations dans les dix prochaines années. Elles vont provoquer une profonde révolution des usages du numérique et des politiques de cybersécurité à laquelle les organisations et leurs directions numériques doivent d'ores et déjà se préparer.

Le caractère stratégique de l'informatique quantique et des métavers est plus largement détaillé dans le champ de transformation 1.

D'ici 2035, les directions du numérique devront gérer la pénurie de talents en Europe mais aussi dans les pays émergents.

La guerre des talents est une tendance lourde qui perdurera dans les quatre scénarios envisagés à horizon 2030-2035. Que l'on évolue dans un monde mondialisé (scénario 1 et 4) ou dans un monde régionalisé (scénario 2 et 3), la concurrence entre les entreprises pour attirer les collaborateurs dotés des bonnes compétences sera de plus en plus vive. Par ailleurs, cette concurrence pourrait être particulièrement déséquilibrée, dans les trajectoires où l'UE, affaiblie, est à la merci des géants du numériques (scénario 4) ou des puissances politiques étrangères (scénario 3). Dans ces scénarios, les entreprises pourraient être particulièrement incitées à développer leurs activités dans des zones géographiques différentes, pour maintenir leur place dans l'économie mondiale. Le développement des activités de l'entreprise dans des zones géographiques différentes nécessiterait alors de diversifier les équipes.

Cette situation pourrait contraindre les directions numériques, plus que n'importe quelle autre direction en raison des tensions RH sur ce secteur, à :

- Faire évoluer les conditions de travail, pour les rendre encore plus attractives ;
- Clarifier l'identité/la mission de l'entreprise pour répondre à la quête de sens des collaborateurs.

Pour répondre à cela, le renouvellement des modalités de recrutement, un investissement plus important dans la formation des collaborateurs et une amélioration de la qualité de vie au travail via une politique sociale plus engagée font partie des moyens accessibles aux organisations pour se rendre attractives.

Au-delà d'une action sur les collaborateurs, d'autres stratégies pourraient permettre aux organisations de lutter contre la pénurie des talents, notamment en développant le *low code/no code* pour ouvrir les tâches IT basiques à des collaborateurs aux compétences limitées dans ce domaine.

D'ici 2035, les directions du numérique devront être des parties prenantes croissantes de l'engagement RSE des organisations, à la demande tant des collaborateurs que des clients et seront redevables devant les actionnaires et la direction générale.

En 2035, la concurrence entre les acteurs économiques sera maintenue, voire accentuée. Cette concurrence s'exercerait à une échelle mondiale dans les scénarios 1 et 4. Elle serait plutôt locale dans les deux autres scénarios marqués par une régionalisation du monde. Ainsi, la capacité d'une entreprise à démontrer une empreinte environnementale faible et à favoriser la qualité de vie au travail sera un marqueur de distinction face aux concurrents pour attirer de nouveaux collaborateurs. Au-delà de cet aspect concurrentiel dans la guerre des talents, les clients porteront également une attention particulière et croissante sur les efforts entrepris par les organisations pour réduire leur empreinte environnementale numérique, et sur le respect qu'elles porteront aux valeurs d'égalité, de non-discrimination et de juste rémunération au sein de l'organisation.

Les enjeux environnementaux et sociétaux au sein des organisations sont développés dans le champ de transformation 2.

D'ici 2035, les directions du numérique pourront être de plus en plus confrontées à des mouvements de résistance internes et sociétaux contre la tendance à l'hyper-technologisation.

Les mouvements de résistance au numérique, ou plus globalement aux nouvelles technologies, se sont accentués au cours des dernières années, par exemple contre la 5G et le métavers suite à l'annonce de Mark Zuckerberg, et notamment lors de la crise sanitaire. Ainsi, ces mouvements devraient continuer à se développer dans les dix prochaines années, alimentés par les crises environnementales et sanitaires à venir. Ces mouvements pourraient créer une ligne de fracture croissante au sein de la société, entre partisans des nouvelles technologies et personnes réticentes ou souffrant d'illectronisme ou disposant d'un accès limité à internet. *Ce point est davantage détaillé dans le champ de transformation 1.*

Maillons essentiels de la société, les organisations accompagnées par leur direction du numérique, ont donc un rôle à jouer pour lutter efficacement contre cette fracture numérique :

- Communiquer de manière transparente sur leurs activités numériques (empreinte environnementale du numérique, investissements technologiques, respect des données personnelles et de la vie privée de leurs clients...) ;
- Inclure tous les collaborateurs dans les évolutions technologiques en proposant des formations en interne ;
- Lutter contre les disparités d'accès à internet parmi les collaborateurs de l'entreprise.

D'ici 2035, la forte composante géopolitique et stratégique du numérique et sa contribution croissante à la performance économique de l'entreprise conduira à réévaluer le positionnement des directions du numérique au sein de la direction générale.

L'augmentation des cyberattaques ces dernières années a permis de démontrer l'importance du numérique au sein des organisations, la mise hors-service de leur système d'information ayant occasionné un arrêt total ou partiel de leurs activités. De même, le conflit ukrainien a entraîné une forte médiatisation sur l'utilisation de l'arme cyber dans le champ politique et pourrait alors entraîner une prise de conscience collective autour des risques cyber.

Le direction du numérique n'est plus considérée comme une fonction support parmi d'autres. Ses budgets augmentent pour répondre aux enjeux cyber et d'innovation technologique nécessaires pour demeurer compétitif. Sa position sera donc valorisée au sein de la direction générale au cours des dix prochaines années. Cette recomposition de la gouvernance des organisations est à envisager dès aujourd'hui.

Membres du Conseil d'orientation stratégique

MEMBRES CIGREF

Jean-Claude **Laroche**
DSI d'Enedis, Président du Cigref et du COS

Jean-Michel **André**
Groupe SEB, CIO VP information systems

Bernard **Duverneuil**
Elior Group, CDIO

Jean-Christophe **Lalanne**
Air France KLM, EVP IT

Christophe **Leblanc**
Société Générale, Group Head of Ressources and Digital

Agnès **Mauffrey**
Sodexo, Global CIO

PERSONNALITÉS QUALIFIÉES

Yves **Bernaert**
Accenture,
Europe CIO

Hugues **Ferreboeuf**
The Shift Project,
Chef de projet

Jean-Gabriel **Ganascia**
Sorbonne Université,
Comets (CNRS), CERNA

Henri **Isaac**
Université Paris-Dauphine,
Renaissance Numérique

Julien **Nocetti**
IFRI, Chercheur associé,
Centre Russie/NEI

Mathieu **Weil**
Chef du service de
l'économie numérique, DGE

Cécile **Wendling**
AXA, Directrice de la stratégie
de sécurité, de l'anticipation
des menaces et de la recherche

Remerciements *& équipe* de publication

Le Cigref souhaite chaleureusement remercier les membres du Conseil d'orientation stratégique et tous les membres du Cigref pour leur contribution riche et stimulante. Plus particulièrement, nous remercions toutes les personnes et notamment nos membres qui ont pris le temps de participer aux ateliers proposés cette année et qui ont ainsi permis d'enrichir la réflexion stratégique et prospective du Cigref.

François BANOS - RENAULT
Laurent BENDAVID - DASSAULT AVIATION
Claudio CIMELLI - MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE
Stéphane DELMARE - EDF
Côme DERKENNE - BPIFRANCE
Alain ESCAFFRE-FAURE - AIRBUS
Sylvain GIRARD - HAGER GROUP
Christophe HUERRE - THALES
Hervé LAGASSIÉ - GROUPE BPCE
Alain LAROUSSE - LOXAM
Vincent NIEBEL - EDF
Laurent POUPON - BNP PARIBAS
Rosanne SERRANO - DASSAULT AVIATION
Olivier SERVOISE - ENGIE
Marc-Michel STACK - BNP PARIBAS
Laurent TRELUYER - AP-HP

Pour la troisième année consécutive, nous remercions également l'équipe de Futuribles, partenaire historique du Cigref, pour son accompagnement sans faille dans l'élaboration de cette vision prospective.

D'abord produit à destination des membres du Cigref, ce rapport s'adresse à l'ensemble de l'écosystème du numérique et à toutes les personnes intéressées par les enjeux numériques et plus globalement aux futurs possibles envisagés sous le prisme du numérique.

Rédaction

Cigref

Henri d'Agrain, Délégué général
Aurélie Chotard, Chargée de mission

En collaboration avec **Futuribles**

François de Jouvenel, Directeur
Marie Ségur, Chargée d'études

Contributions équipe Cigref : **Vanessa Dewaele, Flora Fischer, Frédéric Lau, Marine de Sury, Élena Silvera, Martin de Richecour**
Relecture : **Chantal d'Agrain**, Directrice des contenus, Cigref
Communication : **Baptiste Chauveau**, Chargé de communication, Cigref

Direction artistique et graphismes : **Baptiste Chauveau**, Chargé de communication, Cigref
Illustrations originales : **Vincent Roland** (deusexmuraena.com)

Date de publication : **Octobre 2022**

Annexe

MÉTHODOLOGIE DES ATELIERS PROSPECTIFS 2021-2022

Quatre ateliers prospectifs ont été organisés pour les entreprises membres du Cigref, entre Décembre 2021 et Mars 2022, chacun portant sur l'un des quatre scénarios tracés dans le Rapport d'Orientation Stratégique du Cigref 2021. Leur ambition :

- **Incarner les conséquences stratégiques des quatre scénarios prospectifs ;**
- **Proposer des pistes d'action pour se préparer à un certain nombre de ruptures possibles envisagées dans les scénarios ;**
- **Mais également, impliquer les membres du Cigref dans le processus et les méthodes de la prospective.**

Lors de ces ateliers, les participants étaient invités à s'imprégner des trajectoires proposées, grâce à une vidéo immersive et une présentation des points spécifiques du scénario. Ensuite, les participants étaient divisés en sous-groupes et amenés à se projeter dans une entreprise fictive :

- « Energeia » : une entreprise du secteur infrastructures, réseaux et énergie ;
- « Banka » : une entreprise du secteur banque, assurance, mutuelle ;
- « Industria » : une entreprise du secteur de l'industrie automobile.

L'atelier était ensuite divisé en quatre temps :

- Temps 1. Éléments de contexte.

Les participants disposaient de ce premier temps pour s'approprier le scénario et le jeu de rôle.

- Temps 2. « Nous sommes en 2035 ».

Les participants imaginaient les conséquences du scénario sur leur entreprise fictive :

  - Au quotidien ;
  - Dans son écosystème ;
  - Dans son environnement global.

- Temps 3. « Nous sommes de retour en 2022 ».

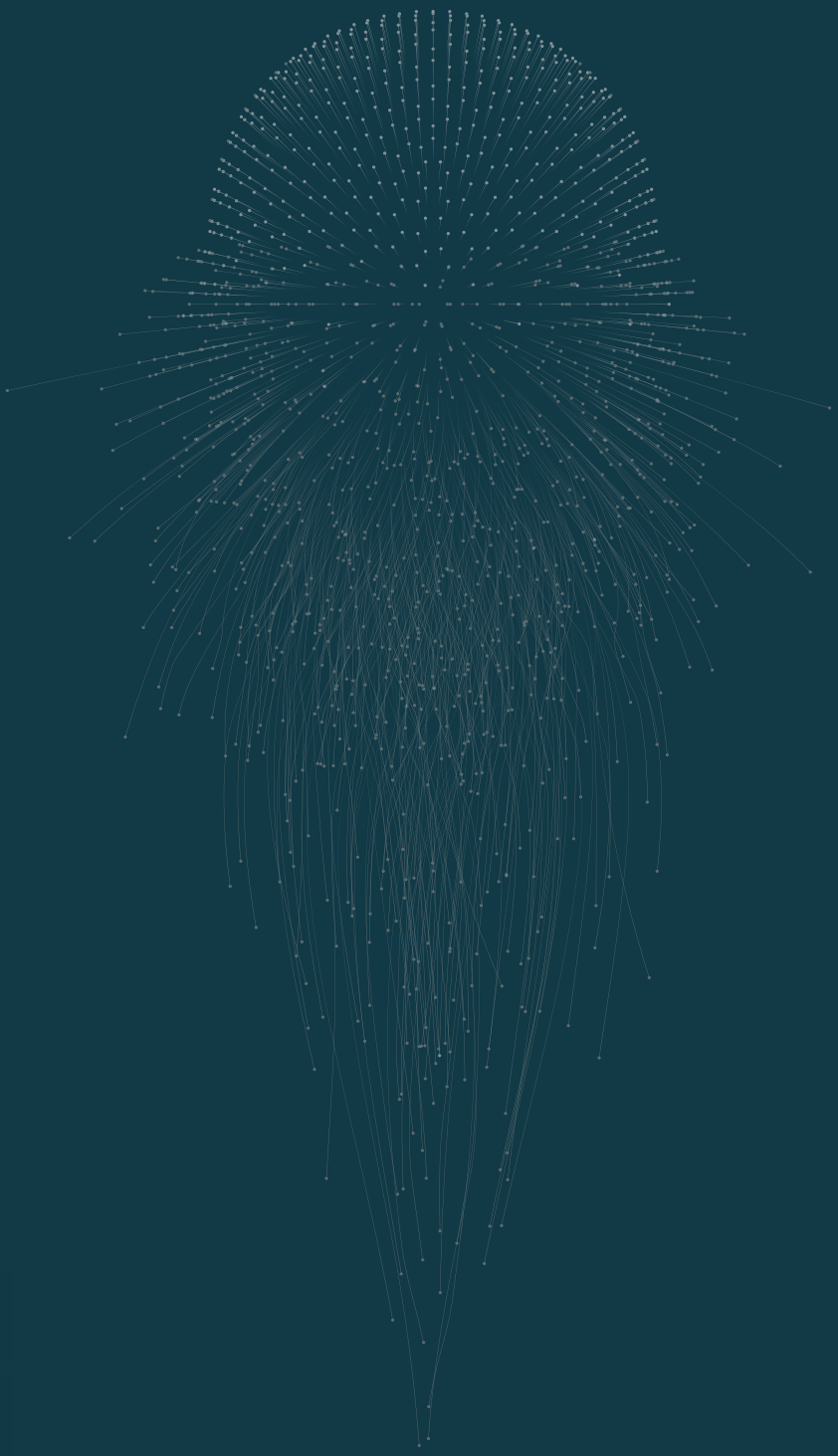
Les participants réfléchissaient aux actions que leur entreprise pourrait entreprendre dès maintenant pour se préparer au scénario.

- Temps 4. « Vous sortez du jeu de rôle ».

Les participants réfléchissaient globalement aux forces et vulnérabilités apportées par le numérique dans le scénario.

Ces ateliers ont permis de nourrir l'actualisation des scénarios et la troisième partie de ce rapport sur les messages-clés à l'attention des directions du numérique des entreprises.

Ce rapport a été réalisé par HandiPRINT, entreprise adaptée qui emploie 120 personnes en situation de handicap, dans la gestion globale de documents imprimés. Plus d'informations : www.handi-print.fr



Cigref

21 avenue de Messine
75008, Paris
www.cigref.fr