Blockchain, suffrage et forfaitures

A quelques semaines des élections présidentielles, les candidat(e)s rivalisent de lyrisme sur la question de la souveraineté technologique.

Et plus personne ne songe pour autant à leur intenter un procès en “souverainisme” (horresco referens !) Ne boudons donc pas notre plaisir. Mais sur ce sujet comme sur tant d’autres, où se trouve la garantie que les engagements pris la main sur le coeur seront suivis d’effets, une fois que le peuple aura choisi à qui confier les clefs de la Maison France ? Nulle part. Et ça n’est pas encore hélas en consignant les programmes électoraux dans le grand livre de la blockchain que nous nous préviendrons de nouvelles forfaitures.

Nous ne voudrions surtout pas donner de mauvaises idées à un bébé licorne. Quoique…

L'innovation technologique est un domaine où le monde privé et le monde de la défense ont un intérêt commun à travailler en 'équipe

France'.

Le Capitaine de frégate Nicolas Malbec est chef de la planification des opérations au Commandement de la Cyberdéfense et directeur du cursus Cyberdéfense de l'École Hexagone. Cet entretien a été publié le 4 février 2022.

1/ Quelle est votre fonction au sein du ComCyber et en quoi cela consiste-t-il ?

Au sein du commandement de la Cyberdéfense, je suis en charge de la planification des opérations. Il s'agit de préparer des options militaires dans le cyberespace pour accompagner les Armées dans leur manœuvre d'ensemble. Les Armées françaises agissent dans les trois domaines de lutte que sont la Lutte Informatique Défensive (LID), la Lutte Informatique d'Influence (L2I) et la Lutte Informatique Offensive (LIO). Dans le détail, ces opérations sont classifiées et je ne puis en dire plus.

2/ La cyberdéfense est garante de la souveraineté nationale. Qu'est-ce donc que cette souveraineté dont le monde va aujourd'hui jusqu'à contester le mot ? De quelle manière la cyberdéfense en est-elle garante ?

Fondamentalement, la souveraineté nationale, c'est le caractère d'un État qui n'est soumis à aucun autre État. L'article 3 de la Constitution souligne que cette souveraineté appartient au peuple qui l'exerce par ses représentants et par la voie du référendum. Dans le domaine numérique la soumission peut arriver plus vite qu'on ne le croit : extraterritorialité du stockage des données des citoyens ou des entreprises stratégiques, dépendance de pays tiers pour la fourniture de matériels stratégiques (75% des semi-conducteurs sont produits à Taïwan, pays qui par ailleurs est le seul à atteindre la précision nanométrique pour la gravure des composants), dépossession de l'exclusivité de battre monnaie (émergence des

cryptomonnaies), etc. À son niveau, dans son aspect défensif, la cyberdéfense va combattre pour préserver la confidentialité, l'intégrité et la disponibilité des données et des systèmes d'information des Armées. Cela passe par le choix des matériels et des architectures de sécurité et par la supervision de la cybersécurité des réseaux. La cyberdéfense va aussi rechercher une forte résilience en préparant le pire. En cas de crise cyber, des équipes de réponses à incident sont déployées pour analyser les attaques et restaurer les systèmes. Pour les systèmes critiques, des plans de continuité et de reprise d'activité sont mis en œuvre.

3/ Que pensez-vous des relations qui existent entre le monde privé (entreprises mais aussi banques et VC) et le monde de La Défense sur les sujets technologiques (en termes d'investissement, au sens large) ?

Ces relations sont organisées pour le ministère des Armées par la Direction Générale de l'Armement qui est responsable de la politique de soutien à la BITD (Base Industrielle et Technologique de Défense). La DGA s'appuie en partie sur l'Agence d'Innovation de la Défense qui met en œuvre la politique ministérielle en matière d'innovation et de recherche scientifique et technique. En novembre 2019, une convention a été signée entre le Ministère des armées et 8 grands maîtres d'œuvres industriels et principaux équipementiers. Ce partenariat s'articule autour de 4 piliers : le partage de l'information au sein d'un cercle de confiance, l'évolution de l'organisation et l'établissement de gouvernance partagée, l'acculturation et la sensibilisation au cyber et la volonté commune de maîtriser les risques cyber sur l'ensemble de la chaîne de soutien de défense.

Ces relations avec les entreprises sont indispensables pour développer les outils dont les Armées ont besoin. Mais ça marche dans les deux sens : par exemple, dans le domaine des outils d'identification (de radars, d'images, de sous-marins, etc.) basés sur des intelligences artificielles, les

entreprises ont besoin des données opérationnelles recueillies sur le terrain par les Armées pour alimenter correctement leurs algorithmes d'apprentissage profond. L'innovation technologique est un domaine où le monde privé et le monde de la Défense ont un intérêt commun à travailler en « équipe France », sans oublier, bien sûr, d'y associer le monde de l'éducation et de la recherche. Pour procéder à des échanges de données opérationnelles classifiées, il faut un tissu national d'entreprises de confiance.

4/ Pierre Bellanger a beaucoup théorisé sur l'analogie entre les eaux territoriales et extra-territoriales et les mers numériques. L'actualité vous incite-t-elle à filer la métaphore ?

La haute mer, c'est la res nullius par excellence, la promesse d'une liberté de naviguer et d'agir à sa guise. Cette liberté de mouvement irrigue l'âme et les mœurs du marin : « Homme libre, toujours tu chériras la mer ! » et partant des grandes nations maritimes. Pourtant cette extra-territorialité est de plus en plus limitée par les traités (notion de zone économique exclusive de la convention de Montego Bay qui éloigne à 200 nautiques des côtes la haute mer et même jusqu'à 350 nautiques en prenant en compte le plateau continental !) ou par les contestations du droit international (revendications chinoises sur la mer de Chine). Les flots numériques constituent un vaste océan mondial appelé l'Internet. Historiquement sous contrôle organisationnel, physique et logique des États-Unis, il pouvait toutefois jusqu'à récemment faire penser à un vaste espace de liberté sans frontière. Cependant, les États ou les grandes entreprises mondiales du numérique ont tendance à mettre sous contrôle des pans entiers de ce vaste océan numérique, créant des mers intérieures ou des lieux de passage obligés. Ainsi la Russie élabore son RuNet en tissant un réseau dédié de routeurs et de datacenters à ses frontières, la Chine est prête à s'abriter derrière son great fire wall, et les géants

américains du numérique représentent plus de 50% des investissements dans les câbles sous-marins. On le voit, la liberté de navigation doit être défendue avec force aussi bien en mer que dans le cyberespace !

5/ Comprenez-vous que l'on puisse communiquer publiquement sur nos vulnérabilités ? ***(Ex : quand la présidente de la Commission européenne déclare que nous serons toujours dépendants de puissances étrangères en matière de semi-conducteurs).***

Les affaires de dépendance en matière de semi-conducteurs ne sont pas secrètes et ne concernent pas que les Européens. Il suffit de regarder le poids de Taïwan dans la manufacture des semi-conducteurs de précision. Dans un régime démocratique, il est important que les citoyens aient conscience de l'état de sa Défense. À ce titre, les autorités militaires sont régulièrement entendues par les députés et les sénateurs pour rendre compte des succès rencontrés mais aussi des difficultés, y compris matérielles, pour remplir les missions confiées. Ce discours de vérité permet d'orienter les politiques publiques et l'effort de Défense.

6/ Un bon cybercombattant, est-ce un bon militaire qui maîtrise l'environnement technologique et ses menaces, ou un bon ingénieur qui saurait tenir un fusil ?

On m'a déjà posé la question à propos de l'officier de marine ! La réponse est similaire : le cybercombattant est avant tout un militaire qui a le culte de la mission et qui est prêt à tous les sacrifices pour l'accomplir. Il doit néanmoins être compétent dans son domaine de lutte et dans le cas qui nous intéresse il doit avoir une maîtrise approfondie de l'environnement cyber et de l'arsenal numérique qu'il y déploie. Cela dit, tous les cybercombattants ne sont pas des ingénieurs : nous avons aussi des juristes, des linguistes, des experts en marketing digital ou en géopolitique, etc.

7/ Que vous inspire le développement fulgurant des drones et la perspective d'un monde peuplé d'objets connectés produits dans des pays potentiellement ennemis ?

Les drones armés sont aujourd'hui, notamment suite au conflit dans le Haut-Karabagh, des armes incontournables des champs de bataille. Utilisés en essaims, éventuellement pilotés par une intelligence artificielle capable d'exploiter leurs capteurs (camera, radio, …) ils sont caractéristiques d'une transformation numérique du champ de bataille qui peut conduire à des tactiques de rupture et à un rééquilibrage des forces en faveur non plus du belligérant le plus riche en matériel mais du plus innovant.

8/ Le haut lieu de la cybersécurité, c'est Paris ou Rennes ? (joke)

Avec le TGV, et un temps de transport de moins d'une heure trente on peut dire que Rennes fait désormais partie de la banlieue parisienne (joke). Sans compter les visioconférences qui permettent de garder le lien en toutes circonstances. Les dispositifs rennais comme le Pôle d'Excellence Cyber et parisiens comme le campus Cyber se complètent harmonieusement. On pourrait ajouter que la cybersécurité n'est pas cantonnée à ces territoires. Je pense par exemple à Toulon qui comprend le centre support cyber de la Marine ou une bonne partie des effectifs cyber de Naval Group.

9/ Quels sont les outils ou logiciels français que vous utilisez à titre professionnel ou personnel ?

La direction interministérielle du numérique (DINUM) met à la disposition des agents de l'État des systèmes numériques collaboratifs souverains comme Tchap (une messagerie type Whatsapp), Osmose (un portail collaboratif) ou la webconférence de l'État (un portail de visioconférence). Je suis utilisateur de ces solutions. Je pense qu'il est indispensable d'employer ce type de solutions souveraines

plutôt que leurs concurrentes étrangères, et lorsqu'elles ne donnent pas complètement satisfaction, il existe des équipes de développement à l'écoute et capables de faire évoluer les produits.

10/ Si vous deviez résumer en quelques lignes la pensée qui gouverne votre enseignement à l'École Hexagone ?

L'école Hexagone m'a demandé de diriger le cursus cyberdéfense qui ouvrira au mois d'octobre 2022 à Versailles. L'idée est de répondre à la pénurie de talents cyber dont la France a besoin en s'appuyant, lorsque c'est possible, sur des enseignants issus soit du monde de la cyberdéfense, soit d'entreprises proposant des solutions de sécurité souveraine. C'est le cas par exemple de Stormshield ou d'HarfangLab. Non seulement les étudiants recevront les enseignements techniques des meilleurs spécialistes du domaine, mais en plus ils seront sensibilisés aux enjeux géopolitiques du cyberespace et à la guerre économique que se livrent les États et les entreprises. Ils seront aussi formés à travailler dans un environnement de crise cyber grâce à des wargames réalistes.

11/ Vous êtes nommé DSI de la France, quelle est la première mesure que vous défendez ?

Je pense que de nombreuses initiatives portées par la DINUM vont déjà dans le bon sens (Création du socle interministériel de logiciels libres, sites data.gouv.fr et api.gouv.fr, généralisation de FranceConnect, …). Après, il me semble important de disposer d'un plan stratégique pour garantir la souveraineté dans tous ses aspects : enseignement, recherche, tissu industriel, approvisionnements stratégiques, hébergement, capacités de calcul, services cloud, arsenal juridique (à doser avec précaution car il ne doit pas être un frein à l'entreprenariat français), etc.

12/ Face à l'omniprésente menace virale (informatique), de quelle nature est selon vous la meilleure réponse à apporter ?

Il faut continuer à investir sur les moyens organisationnels et techniques pour éviter les attaques. Mais il faut aussi et surtout miser sur la résilience de nos systèmes. Qu'est-ce que je fais si je suis attaqué ? Suis-je capable d'évaluer les dégâts ? Suis-je capable de restaurer mes données et mes systèmes ? Ai-je des modes de fonctionnement dégradés ou de secours ? Comment vais-je gérer ma communication de crise (externe et interne) ? Si j'en ai les moyens je m'entraîne régulièrement à faire face au pire.

13/ Que vous inspire le fait que de très nombreux OIV aient choisi / eu la liberté d'héberger leurs données sur des clouds américains ?

Il faudrait regarder au cas par cas. En cybersécurité, la base est de conduire une analyse de risque. Les risques identifiés ont-ils été supprimés, couverts ou formellement acceptés ? Le tout est bien d'avoir conscience de ce que l'on fait et d'être en mesure d'assumer ses choix.

---

e-fortification

Nous célébrons aujourd'hui la Journée mondiale et européenne de la protection des données. Par un malheureux hasard du calendrier, notre Ministère de la Justice a été hier la victime d'une demande de rançon des hackers de Lockbit 2.0.

Les cybercriminels menacent de publier dans deux semaines les données volées. Pas un symbole de force comme un puissant État ou même de charité, comme un hôpital, ne semble donc aujourd'hui susceptible d'arrêter l'action criminelle de ces groupes. La souveraineté technologique peut dès lors être aussi entendue comme la capacité des structures régaliennes à ne pas se laisser dicter leur conduite, particulièrement sous

la menace.

En attendant, et au regard de cette épée de Damoclès moderne, il y a fort à parier que la moitié de l'économie mondiale sera demain consacrée à l'e-fortification de l'autre.

Il faut considérer la souveraineté numérique sur toute sa chaîne de valeur.

Gaël Duval est fondateur visionnaire et "militant" de /e/ foundation, une alternative éthique et souveraine aux géants américains et chinois du smartphone. Cet entretien a été publié le 28 janvier 2022.

1/ /e/ est un système Android « déGooglisé ». Il dispose du noyau open-source d'Android, sans aucune application Google ni service Google qui accède à nos données personnelles. Il est compatible avec toutes les applications Android. Comment vous êtes-vous lancé dans ce projet titanesque ?

Il y a quelques années j'ai commencé à m'interroger sur ma dépendance croissante aux outils des GAFAM, j'avais un iPhone, j'utilisais de plus en plus les services de Google. Pourquoi, alors que j'ai passé la première partie de ma vie professionnelle à créer des produits open source, autour de Linux, pourquoi en étais-je arrivé là ? Dans le même temps, j'ai commencé à prendre conscience de ce qui se passe sur la collecte des données personnelles, du modèle publicitaire… Ce qui se passe dans nos smartphones, tous les jours et en permanence, personne ne l'accepterait d'autres services traditionnels, comme le courrier, le téléphone…

Et pourtant on en est là : entre 6 et 12 Mo de données personnelles sont captées chaque jour pour chaque utilisateur d'un smartphone Android (80% du marché) ou Apple (20% du marché). Ces données, ce sont nos vies personnelles, là où l'on se trouve, avec qui on correspond, le contenu de nos échanges… tout ça va chez les géants du net pour nourrir des modèles économiques reposant sur la publicité ciblée. Et cette situation délétère et mondiale, qui repose sur des monopoles de fait, elle a également des impacts colossaux sur notre souveraineté, sur notre économie, sur nos démocraties…

J'ai commencé à détailler tout ça dans un article qui est paru en 2017 dans La Tribune, et qui a ensuite été repris et complété en Anglais dans un ouvrage collectif traitant de plusieurs sujets technologiques, publié en 2018. J'y défends la thèse que la recherche de souveraineté numérique doit être considérée sur toute sa chaîne, en partant des couches d'infrastructures comme les réseaux et les systèmes d'exploitation, sur lesquels reposent toutes les autres couches intermédiaires et applicatives, et ceci à l'échelle Européenne.

Ayant assez vite réalisé que le sujet n'intéressait pas nos grands visionnaires politiques depuis De Gaulle, je me suis dit que le constat, la réflexion et tout le bla-bla à ce sujet étaient inutiles si on ne propose pas dans le même temps des produits et des solutions réalistes, utilisables par tous, et qui "cochent les cases" de cette maitrise technologique fondamentale pour notre indépendance.

C'est de là qu'est parti le projet "/e/OS" (Murena maintenant) qui propose d'une part un système d'exploitation mobile qui, par défaut, n'envoie pas de données chez Google, et d'autres part un ensemble de services en ligne en lien avec l'OS : mail, calendrier stockage cloud, édition de documents en ligne… Nous utilisons quasiment exclusivement des briques open source, ce qui nous permet à la fois de ne pas partir d'une feuille blanche, et aussi d'avoir une approche "preuve par le

code source” qui est totalement absente de la plupart des systèmes d’exploitation du marché, y compris les rares qui commencent à se positionner sur la défense des données personnelles des utilisateurs, comme Apple. On explique ce que font nos produits, comment ils le font, et on le prouve.

2/ Un smartphone qui n’envoie plus de données, ça peut donc servir ?

Il permet d’avoir une vie numérique tout à fait normale, sans se faire micro-cibler, sans partager ses données personnelles avec Google… Beaucoup de nos utilisateurs nous rapportent régulièrement à quel point ils ont été surpris d’avoir pu basculer si naturellement vers nos produits.

3/ Eu égard à la dimension stratégique de votre activité, comment expliquez-vous que les pouvoirs publics (ou privés) ne s’en soient pas emparé pour permettre son accélération et son déploiement partout ?

Même si ça commence à bouger, ma compréhension de cette situation à ce stade c’est que la plupart des “décideurs” sont juste des suiveurs de tendance, sans aucune vision stratégique. Ils sont d’ailleurs souvent issus de formations qui ne comprennent absolument rien à la technologie, et malheureusement font souvent passer leur carrière avant l’intérêt des citoyens.

Je constate néanmoins une grande sympathie pour notre projet et son ambition au sein de beaucoup d’institutions liées à l’Etat et de plus en plus au niveau Européen. Mais au niveau politique, l’aveuglement reste globalement total. Et malheureusement ça fait plus de 40 ans que ça dure. On reparle de De Gaulle ?

4/ Vous communiquez sur ce qu’il y a en moins dans votre OS. Qu’y a-t-il en plus ?

La sérénité et la liberté !

Un petit exemple pour illustrer : les pastilles qui s'affichent sur les icônes des applications. Traditionnellement elles sont rouges et un nombre correspondant aux notifications en attente vient s'ajouter. Ça fait partie des mécanismes mis en place par de nombreuses sociétés pour capter continuellement l'attention des utilisateurs ("économie de l'attention"). Elles reposent sur la psychologie du "Fear of Missing Out" (la peur de manquer quelque chose d'important). Et bien nous avons pris le contrepied en les passant du rouge au vert, et en n'affichant pas le nombre de notifications qui attendent. On souhaite de-stresser nos utilisateurs.

Un autre exemple : notre navigateur web intègre un bloqueur de pubs par défaut.

Evidemment sur la protection des données personnelles on introduit aussi pas mal de choses. La base est saine : un papier récent de chercheurs de l'Université d'Edimbourg et de l'Université Dublin a montré que /e/OS était le seul OS mobile qui n'envoyait pas de données personnelles hors du smartphone.

Nous indiquons également dans notre store d'applications le nombre de pisteurs (ce sont comme de cookies, mais pour les applications) détectés dans chaque application (on utilise d'ailleurs pour ça une technologie qui a été créée en France par Exodus Privacy). Ça permet à l'utilisateur d'avoir une première idée si l'application qu'il s'apprête à installer est là pour le micro-cibler ou pour rendre le service pour lequel il souhaite l'utiliser.

La deuxième étape, c'est un projet sur lequel nous travaillons depuis plus de un an. Il va permettre aux utilisateurs de très facilement couper ces pisteurs, s'ils le souhaitent, et de leur donner d'autres outils très simples à utiliser, pour "passer sous les radars".

5/ Le fairphone que vous commercialisez peut-il dans votre

esprit devenir un fer de lance de notre souveraineté numérique ?

C’est pour le moins je crois une démonstration parfaite de ce qu’on peut faire au niveau européen, avec une convergence fabuleuse entre le développement durable, la protection personnelle, l’indépendance technologique, l’économie : notre projet crée des emplois et près de 80% de notre chiffre d’affaire est à l’export !

Mais pour aller plus loin et prendre une place significative sur ce marché, nous devons nous financer de manière importante, pour aller davantage vers le grand public.

Il reste en outre de gros sujets : les places de marché des applications mobiles, qui font l’objet de monopoles inacceptables. Mais aussi la dépendance au hardware : où sont les usines pour fondre du silicium, et créer des chipsets ? Plus en Europe malheureusement. Et pourtant notre savoir-faire dans ces domaines est encore d’un niveau extrêmement élevé.

6/ À combien évaluez-vous le budget marketing qui pourrait faire de /e/ un OS grand public (si c’est votre objectif) ?

Budget marketing, mais pas seulement : la dépendance au matériel est forte, le produit doit innover constamment. Donc on parle a minima de budgets de plusieurs dizaines de millions d’euros. Pour donner un exemple connu : l’Essential Phone qui avait été créé par le fondateur d’Android il y a quelques années a coûté 80M€ à développer. La R&D d’une grande entreprise chinoise bien connue dans notre secteur c’est 70 000 personnes. Ça donne une idée des échelles et des enjeux.

7/ Sur le marché des téléphones mobiles, est-ce que le meilleur moyen de prendre un avantage compétitif sur les géants, ça n’est pas désormais réfléchir à l’appareil “d’après” (forme, matériau, énergie, technologie) ?

C’est un argument qu’on entend souvent : “on a loupé le

dernier train, prenons le prochain” ! Sauf que… sans rattrapage préliminaire, en particulier sur les couches d’infrastructures comme les réseaux ou le système d’exploitation, c’est vain. On le voit parfaitement avec ce qui se passe aujourd’hui dans le cloud, ce sont ceux qui ont la main sur les technos qui mènent la danse. Et ça va être la même chose pour l’Intelligence Artificielle, ce sera la même chose pour l’informatique quantique. Encore une fois, il faut considérer la souveraineté numérique sur toute sa chaîne de valeur.

Et ce n’est sans doute pas suffisant : l’Europe est encore sur la réthorique du sacro-saint “tout marché qui doit être libre à tout prix”. Sans entrer dans un débat politique, posons-nous déjà simplement la question de la réciprocité des pratiques commerciales avec les Américains, avec les Chinois… Eux-mêmes, malgré leurs discours et leur dogme, passent leur temps à mettre en place des mesures protectionnistes pour leurs marchés. Arrêtons d’être des bisounours asservis.

Donc il me semble qu’à un moment il faut avoir le courage de dire à nos partenaires : vous appliquez telle ou telle mesure protectionniste, et bien tant que ce sera le cas nous allons le faire également au niveau européen.

Enfin il y a la question de la nécessaire régulation.

8/ Comment votre activité est-elle affectée par la crise des semi-conducteurs ?

Ça a rendu assez chaotique la deuxième moitié de 2021 sur les approvisionnements de smartphones. Les mois d’octobre et novembre en particulier ont été assez horribles, et nous avons encore des listes d’attente de plusieurs centaines de clients qui attendent de pouvoir commander un smartphone Murena avec /e/OS.

9/ On ne jure plus aujourd’hui que par les “entrepreneurs”. Est-ce cette fibre-là qui vous a animé jusqu’ici ou une autre

?

Ceux qui me connaissent bien savent que mon désir d'entreprendre remonte à loin. Enfant J'ai créé des journaux, que je vendais en porte à porte dans mon village, ado j'ai créé un logiciel de prévision météo que je vendais sur disquettes, j'ai créé plus tard un label de musique, puis un deuxième… bref je ne sais pas faire autre chose ! Et ma formation en informatique m'a amené très naturellement à créer des sociétés. C'est d'ailleurs frappant de voir à quel point l'entreprenariat, qui était un concept presque honteux dans les années 90, est devenu tellement à la mode.

10/ Est-il une entreprise ou une personne dans le monde avec laquelle vous rêveriez de collaborer sans lui avoir jamais encore demandé ?

David Bowie et Jimi Hendrix, mais c'est trop tard.

Plus sérieusement, je trouve l'entreprise TESLA et Elon Musk fascinants dans le sens où absolument tout au début de l'aventure de entreprise aurait dû les pousser à renoncer. Mais grâce à une vision ambitieuse, grâce à énormément de travail, grâce à des prises de risque considérables, grâce à une ténacité et une volonté sans faille de réussir, ils arrivent à bouleverser totalement le marché automobile et à changer le monde.

C'est un grand enseignement pour tous les entrepreneurs. C'est aussi un sacré enseignement pour les donneurs de leçon et les adeptes du renoncement et de la servitude volontaire.

On ne peut pas gagner une guerre sans livrer bataille.

Métavers à moitié vide

On ne parle que de lui. Le nouvel Alter Mundi, où tout sera, vous le verrez bientôt à travers vos holo-bésicles, tellement mieux !

C’est un peu le pendant virtuel de la conquête spatiale, un far west technologique riche de mille promesses; La perspective offerte à chacun d’une…Seconde Vie. Naturellement, surtout si l’on a vu et apprécié Ready Player One, cela ne peut que faire battre nos coeurs adulescents. Mais à y regarder de plus près, est-ce là autre chose que la course ad extra d’un monde lassé de lui-même ? Pendant ce temps, du côté de la physique quantique, un autre genre d’explorateurs découvre patiemment, à soigneux coups de pinceaux, les lois de la conscience, du temps, de l’espace ou de la matière…

Et vous, l’intrication, ça ne vous intrigue pas un peu ?Le cas de Schrödinger est mort. Vive le chat de Schrödinger !

Souveraineté technologique : petite éphéméride de la démission

Voilà maintenant de nombreuses années que la fine fleur de notre industrie, de nos services ou de nos **OIV (Opérateurs d’Importance Vitale)** considère que le meilleur choix à exercer consiste à « remettre les clefs » de notre maison commune à des entreprises américaines ou chinoises. Outre le fait que les motifs qui président à ces choix sont souvent contestables (les technologies françaises ou européennes « n’auraient pas

les reins assez solides »), ce palimpseste de décisions déraisonnables place aujourd'hui notre pays dans un préoccupant état de dépendance critique. Le croissant écheveau des moyens de pression qui existe entre nations et grandes entreprises technologiques donne à voir un nouveau visage de la guerre économique. Des pays ont obtenu par voie commerciale un accès privilégié à des informations ou des ressources techniques stratégiques dans d'autres pays, qui sont susceptibles de devenir des ennemis « bien connus ».

En cas de tension, de crise ou de conflit, les grandes plateformes, les fournisseurs de matières premières, de cloud ou de logiciels sont aujourd'hui pris à témoin et sommés par leur propre pays ou par l'opinion internationale de prendre des mesures de rétorsion à l'égard de leurs clients de la veille.

La liste d'une petite centaine de dates, que nous avons publiée sur notre page Linkedin, et qui ne demande qu'à être complétée, donne une petite idée de l'incapacité dans laquelle nous nous trouverions si nos prestataires extra-européens d'hier se trouvaient aujourd'hui associés à une querelle entre notre pays et le leur.

Nous ne sommes souverains ni

technologiquement ni numériquement.

Philippe LATOMBE est député de la 1ère circonscription de Vendée, et Cosimo PRETE, le fondateur de Crime Science Technology, lauréat de la French Tech. Cet entretien a été publié le 21 janvier 2022.

1/ Quelle réalité placez-vous derrière le terme de souveraineté technologique ? (Technologique et pas uniquement numérique)

Philippe LATOMBE

Le terme de « souveraineté » est un mot extrêmement galvaudé que chacun redéfinit à l'aune de son idéologie personnelle, ce qui fait que tout le monde ne parle pas de la même chose. Certains font même un micmac entre « souveraineté » et « souverainisme ». C'est aussi une notion mise à mal par la mondialisation de l'économie, de façon encore plus nette concernant le numérique, car la souveraineté se définit comme l'exercice du pouvoir sur une zone géographique déterminée. L'euphorie créée par l'illusion d'un cyberespace qui appartient à tout le monde a donc mis plus de temps à se dissiper. Si virtuel soit-il le cybermonde est le miroir des turbulences du monde réel et les reproduit. **Nous ne sommes souverains ni technologiquement ni numériquement.** Et ce constat est valable pour la France comme pour l'Europe. Où la situation devient alarmante, et la crise sanitaire a mis le doigt là où cela fait mal, c'est que nous ne sommes pas autonomes dans un nombre de domaines qui dépasse très largement le numérique ou les nouvelles technologies. La première étape consiste donc à viser l'autonomie stratégique et à assurer notre approvisionnement. Pour ce qui est du numérique et des nouvelles technologies, l'enjeu est d'autant plus crucial qu'en quelques années ces technologies ont envahi

toutes les activités humaines et sont transversales et indispensables. Pour arriver à cette autonomie stratégique, nous devons recenser méthodiquement tout ce qui peut y contribuer. Nous ne pourrons y arriver seuls et c'est là que l'échelon européen est essentiel.

Cosimo PRETE

Nos sociétés deviennent dépendantes de la technologie et des entreprises qui les contrôlent (réseaux et plateformes, télécommunications, information, santé, commerce, justice, sécurité, armée…). Il me semble que la souveraineté technologique pourrait se définir comme une interaction harmonieuse entre l'État, les citoyens, les territoires et les acteurs économiques dans l'intérêt du plus grand nombre. Puisque **la notion de frontière géographique n'a plus vraiment de sens dans le cadre du déploiement d'une technologie,** il est important d'entretenir une relation de confiance entre l'ensemble de ces acteurs. Notre société est alors souveraine dans ses choix dans la mesure où elle a la possibilité de choisir librement les solutions qu'elles souhaitent privilégier, en particulier lorsqu'elles impactent massivement les citoyens et leur quotidien (Exemple : la vaccination). Aussi, **il apparait important de distinguer souveraineté technologique et patriotisme technologique.** Ce dernier consiste à niveau technologique équivalent ou supérieur à favoriser une technologie française.

2/ Quels ont été les fruits, pour vous et pour le pays, de la mission parlementaire sur la souveraineté numérique ?

Philippe LATOMBE

Pour moi ? Ce n'est pas le plus important, loin de là, mais j'ai la satisfaction d'avoir fait un travail qui mobilise le monde de la tech et dont j'espère qu'il inspirera les politiques à venir. J'ai essayé d'être le plus exhaustif possible en multipliant les auditions et donc les

intervenants. Je continue à m'investir dans le suivi du rapport afin d'en promouvoir les propositions, avec l'espoir d'en voir rapidement les fruits, pour reprendre le terme utilisé dans votre question, pour le pays.

Cosimo PRETE

Cette mission parlementaire a été l'opportunité de témoigner, en qualité d'expert et d'entreprise de la tech spécialisée dans la sécurisation des documents d'identité, des difficultés que l'on rencontre en France pour concevoir nos documents régaliens tels que la nouvelle carte d'identité électronique et d'accéder à la commande publique.

Crime Science Technology est un cas d'école dans le marché de la sécurité qui démontre qu'il y a une distorsion entre les discours et la mise en pratique par notre administration. Au risque de déranger : **pour une même fonctionnalité, comment un donneur d'ordre appartenant 100% à Bercy peut préférer aux technologies de la French Tech classées dans le TOP 50 mondial des sécurités, des technologies qui ont plus de 30ans et appartiennent à une entreprise étrangère avec une quinzaine de procès en cours pour corruption ?** Paradoxalement, notre solution protège la carte d'identité de l'Allemagne qui se veut la plus sûre en Europe et d'autres pays de l'union nous ont sollicité pour protéger leur nouvelle CNIe en 2022.

La mission conduite par le député Philippe Latombe a mis l'accent dans ses propositions sur l'importance de "faire confiance à nos entreprises technologiques". Il s'agit notamment de "faire de nos entreprises technologiques une priorité nationale, de privilégier, en matière de commande publique, le recours aux solutions d'acteurs technologiques français ou européens".

3/ Pensez-vous que les enjeux liés à la souveraineté numérique peuvent se permettre de souffrir le jeu improductif de l'alternance politique ?

Philippe LATOMBE

Tant que nous n'aurons pas un ministère d'Etat du numérique doté d'une administration compétente et ayant autorité sur les autres ministères sur ce sujet transverse, nous souffrirons de ce que vous appelez « le jeu improductif de l'alternance politique ». Remonter notre handicap, énorme en matière de souveraineté numérique, demande une stratégie clairement formulée et planifiée, sur le court le moyen et le long terme, et qui requiert l'adhésion des parties prenantes.

Cosimo PRETE

Le dossier sur « Comprendre la Souveraineté numérique » des Cahiers Français rappelle qu'« alors que la plupart des activités humaines sont désormais régies par les technologies digitales, **les États sont entrés dans un rapport de force avec les multinationales** qui règnent sur les réseaux numériques. Il s'agit de préserver ou de reconquérir une part du pouvoir qui s'exerce dans ces nouveaux espaces, pourtant conçus pour échapper à l'emprise étatique ». Aussi, il m'apparait évident que les enjeux liés à la souveraineté numérique ne peuvent souffrir de l'alternance politique. Selon moi, il s'agit d'une composante stratégique qui mérite à part entière un ministère. Bien souvent par manque d'expertise, de conservatisme et/ou d'anticipation, nos politiques et grandes administrations se laissent dépasser par la vitesse à laquelle le monde de la tech évolue. Ils ont du mal à l'intégrer alors que les différentes communautés du monde digital ont de nombreuses attentes sur le sujet. D'ailleurs, **pour le moment, nos candidats déclarés à l'élection présidentielle ont été assez discrets sur le sujet alors qu'il ne se passe pas une semaine où l'on parle de souveraineté** !

4/ Entre une République des experts et une République des généralistes, que faire pour que la représentation nationale comprenne mieux les coulisses de la guerre technologico-commerciale que nous vivons ?

Philippe LATOMBE

Les députés sont à l'image des Français, tous utilisateurs d'Internet mais peu conscients des enjeux où, quand ils le sont, pas toujours suffisamment acculturés aux technologies pour avoir un avis pertinent. **Sur les 577 parlementaires de l'Assemblée, les spécialistes de ces questions se comptent à peine sur les doigts des deux mains.** C'est très peu quand il s'agit de légiférer sur un tel sujet. Cela m'a particulièrement frappé lors de la proposition de loi sur les contenus haineux ainsi que la façon dont s'est peu à peu élaborée une usine à gaz que le conseil constitutionnel a fait exploser en plein vol. Beaucoup de travail parlementaire et beaucoup de bruit pour rien. J'avais prêché dans le vide pendant des semaines. La grande leçon à tirer, c'est qu'il faut lutter contre un certain amateurisme, trouver un ratio équilibré entre ceux que vous appelez députés experts ou députés généralistes. **L'expertise en nouvelles technologies est sous-représentée dans l'hémicycle.** Il faut dire que les compétences requises sont complexes puisqu'elles sont technologiques, juridiques et in fine éminemment politiques et stratégiques.

Cosimo PRETE

Aujourd'hui, il me semble que la composante innovation/numérique soit éclatée entre différents ministères ; ils ont tous plus ou moins un conseiller technique sur le sujet. En l'état, il m'apparait assez difficile d'avoir une véritable vision transversale. **La solution d'un « Ministère du Numérique et de l'Innovation » avec une force de frappe dédiée permettrait d'offrir davantage de ressources tant sur le plan humain que financier.** De nombreux parlementaires s'intéressent aux coulisses de la guerre technologico-commerciale, certains en ont fait l'un de leur sujet de prédilection. Je serai pragmatique, rien de tel que de se confronter à la réalité du terrain et sans langue de bois. Je ne peux qu'encourager nos élus à aller à la rencontre des entreprises de la tech et

réciproquement, ce qui est déjà le cas pour une partie d'entre eux en circonscription. Nous avons un bel outil qu'est la French Tech : créons des ponts, encourageons la confrontation des idées avec les plus représentatifs de l'écosystème, voir même l'immersion. Des think-tank existent mais je pense qu'il faut aller au-delà. Les coulisses de la guerre technologio-commerciale sont un véritable enjeu de société. Il n'y a qu'à voir les difficultés que rencontrent des pépites de la tech telles que Valneva pour mettre leur produit sur le marché français en pleine crise sanitaire.

5/ Au regard des récents partenariats noués par des grosses entreprises françaises avec des prestataires américains, que dire de la notion d'OIV ? L'ANSSI fait-il correctement son travail ?

Philippe LATOMBE

Il n'y a rien à dire sur l'OIV en tant que définition légale d'un certain nombre d'organisations qui sont difficiles à tous identifier d'ailleurs car leur liste n'est pas publique. En revanche, il faut veiller, pour toutes celles qui sont estampillées pour toute ou partie de leurs activités, à ce que les partenariats avec des sociétés étrangères soient compatibles avec ce statut. Cela exclut une inféodation aux GAFAM. **Quand la SNCF choisit Amazon, non seulement elle tourne le dos aux fournisseurs français ou européen, mais elle met tous ses serveurs dans le « panier » Amazon et s'interdit toute possibilité de rétropédalage, de réversibilité.** Ce n'est pas le seul exemple, je pourrais citer Radio France qui fait héberger une partie stratégique de l'entreprise par le cloud Azure de Microsoft et c'est Orange qui sert la soupe.

L'ANSSI fait correctement son travail en fonction de son périmètre d'intervention et des moyens qui lui sont impartis. Cela ne veut pas dire qu'on ne puisse pas mieux faire.

Cosimo PRETE

Selon le SGDSN, « les opérateurs d'importance vitale sont désignés par le ministre coordonnateur du secteur qui les sélectionne parmi ceux qui exploitent ou utilisent des installations indispensables à la vie de la Nation. Les critères de choix et les objectifs de sécurité recherchés sont fixés par le ministère coordonnateur. La procédure repose, d'une part, sur une consultation des opérateurs pressentis, et d'autre part, sur une concertation interministérielle permettant une protection équivalente entre les secteurs d'activités. Le choix des OIV tient compte des éventuelles distorsions de concurrence et vise à éviter les charges indues ». Les OIV sont des acteurs de la stratégie de notre sécurité nationale. Aussi, on peut s'interroger sur le fait qu'ils soient associés de manière directe ou indirecte au « Patriot Act » américain. N'aurait-on pas pu a minima privilégier des partenariats avec des acteurs européens ? De manière plus générale, le coup d'arrêt pour le Health Data Hub démontre clairement qu'**il y a un manque de transparence sur la mise en place des marchés et que nous sommes prisonniers (voir victimes) de nos propres règles.**

Face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs, l'ANSSI a pour mission d'accompagner les opérateurs d'importance vitale dans la sécurisation de leurs systèmes d'information sensibles. La France est le premier pays à être passé par la réglementation pour mettre en place un dispositif efficace et obligatoire de cybersécurité de ces infrastructures critiques. Je respecte mais n'approuve pas que les OVI restent souverains dans leur stratégie partenariale **tant qu'il n'y a pas la mise en place d'un « Patriot Act » à la française.** Il en va de même pour les grands donneurs d'ordre dont l'État est actionnaire.

6/ On entend ici et là "plus d'État" et "moins d'État", quelle est la bonne formule en matière de financement et de développement d'entreprises innovantes d'un certain nombre

d’organisations ?

Philippe LATOMBE

Moins de lourdeurs administratives et plus d’accompagnement dans la recherche de financement, à l’export aussi. On a tendance à multiplier les mesures ce qui complexifie le parcours des porteurs de projet. L’innovation, c’est toujours une prise de risques. Or, elle pèse essentiellement sur le porteur de projet. Il y a un gros travail à faire aussi sur la commande publique et sur les délais de paiement par l’administration pour ceux qui ont été choisis. **Plus qu’une question de « plus d’Etat » ou « moins d’Etat, c’est une question d’un Etat qui est là quand il faut et où il faut.**

Cosimo PRETE

L’intervention du Président de la République lors de France 2030 me parait très claire : « On a un problème, l’innovation de rupture ne se fait plus dans les grands groupes et la valeur ne se crée plus dans les grands groupes. Ce n’est pas une offense, c’est une réalité. Donc il y a des grands groupes qui sont en train de se transformer très vite, il faut les aider. Mais **si la stratégie des grands groupes est de tuer l’innovation qui vient des acteurs qui sont les plus innovants, ils se tueront eux-mêmes à terme ou ils aideront leurs compétiteurs** […] La capacité à faire confiance à l’émergence, elle passe aussi par les politiques d’achat. Et là je parle pour l’État comme pour les grands groupes. Si nous avons des politiques d’achat qui ne sont pas cohérentes avec ce que je viens de dire du côté des grandes administrations publiques, des collectivités locales et des grands groupes français, tout ce que je viens de dire n’adviendra pas. Et donc dans la feuille de route que je donne aussi à l’équipe commando, c’est d’intégrer nos politiques d’achat. ».

7/ En quoi consisterait un programme “Choose France” dont le but serait de retenir les entrepreneurs français dans

l'hexagone ?Fiscalement, sommes-nous attractifs pour nos propres ressortissants ?

Philippe LATOMBE

Le terme « Choose » est, soit dit en passant, assez maladroit, quand on est censé s'adresser à des entreprises françaises que l'on souhaite retenir. Est-ce que fiscalement nous sommes attractifs pour nos propres entreprises ? Clairement non. Il suffit de voir le problème des management packages, où la fiscalité est clairement en défaveur de l'investissement salarié. Les start-up ont intérêt à s'expatrier dans des pays où les conditions sont plus favorables. **Il n'y a pas besoin d'être très inventif mais de reprendre des idées qui ont fonctionné ailleurs, comme en Israël, où il existe un véritable écosystème fiscal en faveur de l'innovation.** Nous pourrions par exemple encourager les start-up innovantes et toutes les entreprises d'ailleurs, en leur accordant un abattement de 50% de l'IS quand elles consacrent au moins 30% de leurs bénéfices à la R&D.

Cosimo PRETE

Aujourd'hui, en qualité de lauréat de la French Tech, je fais le constat comme beaucoup d'entre-nous que nul n'est prophète en son pays, y compris dans la Start-Up Nation. Je reprendrai les propos d'Alain Juillet, Ex- Haut Responsable à l'Intelligence Economique (HRIE) : « pourquoi a-t-on appelé un cabinet américain pour organiser la vaccination en France ? Prenons un autre exemple, celui des cartes d'identité qui semble d'actualité. Il faut pouvoir utiliser les techniques les plus modernes pour les rendre vraiment infalsifiables, contrairement à ce qu'on a connu dans le passé. Cela signifie qu'il faut pouvoir faire appel aux meilleures technologies, a fortiori lorsqu'elles existent en France. Or que constate t'on ? Exactement le contraire, car on ne respecte pas les règles élémentaires issues de l'Intelligence économique. Non seulement on ne sélectionne pas les technologies françaises

les plus efficaces qui ont fait leurs preuves ailleurs mais, bien souvent, on prend des technologies anciennes chez des interlocuteurs avec qui l'administration a l'habitude de travailler…C'est le contraire des pratiques d'une véritable start-up nation comme Israël ! ». **L'exemple américain de la DARPA a démontré que l'accès à la commande publique est un élément majeur pour l'émergence des champions. Il me semble avoir inspiré à la Défense la création de l'Agence pour l'Innovation de Rupture qui n'a pas encore son équivalent à l'Intérieur et dans d'autres secteurs stratégiques.**

En matière de fiscalité, je vous renvoie à l'actualité sur l'aberration des « managements packages ». Les salariés et les managers qui investissent dans leur entreprise sont fiscalement pénalisés par rapport aux salariés et managers des fonds d'investissement qui prennent une participation dans la même société. Cherchez l'erreur ?

8/ Les grands groupes rendent-ils aux start-up ce qu'ils leur doivent ? L'open Innovation est-elle autre chose que de l'élevage intensif intéressé ?

Philippe LATOMBE

Les grands groupes font beaucoup de nursing, de start-up washing, mais in fine se tournent trop facilement vers les solutions intégrées GAFAM (cf. Orange). Il faut que ils comprennent que les GAFAM vont finir par les tuer et que jouer la souveraineté en Europe a du sens, notamment pour maintenir de la valeur ajoutée et des emplois sur nos territoires, donc sur nos marchés. Attention à la délocalisation GAFAM. Attention à l'évasion fiscale GAFAM qui fera au bout du compte porter la charge fiscale et sociale sur peu d'épaules

Cosimo PRETE

Selon le Président de la République, le plan «France 2030» doit «réconcilier» les start-up et l'industrie, aussi je garde

espoir que les propositions de la mission “Bâtir et promouvoir une souveraineté numérique nationale et européenne” soient mises en application : Faire confiance à nos entreprises technologiques. La mise en place de véritables partenariats gagnant-gagnant encadrés juridiquement me semble fondamentales. A ce titre, je salue l’initiative de France Industrie et de l’engagement pris par les 27 industriels signataires du Manifeste des Grandes Entreprises pour soutenir les Startups Industrielles.

Par ce manifeste collectif, les industriels signataires souhaitent concrètement répondre aux besoins exprimés par l’écosystème des startups industrielles, en s’engageant à :

- Identifier en leur sein au moins un point de contact dédié aux startups,
- Développer les possibilités de coopérations technologiques (recherche finalisée, développement, et innovation) y compris au travers de la mobilité des compétences,
- Favoriser l’accès des startups aux financements, notamment en facilitant des alliances et des partenariats financiers ou capitalistiques.
- Respecter un cadre de coopération établi dans un mémorandum d’accord protecteur des uns et des autres, notamment en matière de propriété intellectuelle, de protection des données et de gouvernance,
- Co-organiser et participer à des sessions de rencontres professionnelles pour formaliser les besoins réciproques et accélérer de futurs partenariats commerciaux.
- Valoriser médiatiquement les partenariats développés avec les startups industrielles sous forme d’actions de promotion et de communication pour les faire gagner en visibilité.

9/ L’Europe veut se distinguer sur le terrain du droit. Mais on a vu récemment avec Europol qu’elle avait du mal à montrer l’exemple. Le numérique européen, comment le définiriez-vous ?

Philippe LATOMBE

La situation du numérique européen est comparable à celle du numérique français, selon le bon vieux principe du « aux mêmes causes, les mêmes effets ». De mauvaises habitudes ont été prises dès le début et, malheureusement, perdurent. Quand la CJUE intervient, l'administration européenne a bien du mal à se plier aux décisions juridiques qui ont été prises. **La CJUE est par excellence le lieu de la défense juridique de la souveraineté et des libertés à l'ère numérique.**

Les DSA, DMA et Data Act sont des initiatives nécessaires, et il est impératif de les adopter rapidement si l'on veut éviter le lobbying, mais ensuite **il faudra nourrir une véritable réflexion stratégique sur le numérique, du hardware (puces) jusqu'aux innovations post-quantiques en cours et à venir,** ce qui demande un commissaire, vice-président de la commission, et une version européenne de la Darpa, qui soit puissante et écoutée, pas seulement composée de fonctionnaires européens, mais aussi de dirigeants, à la fois fins stratèges et managers agiles.

Cosimo PRETE

L'actualité récente a titré que « Europol se fait épingler pour stockage illégal de données d'enquêtes de police ». L'équivalent européen de la Cnil, le European Data Protection Supervisor (EDPS), a annoncé le lundi 10 janvier 2022 avoir ordonné à Europol de supprimer un large éventail de données que l'agence de police européenne a amassé en dehors de tout cadre légal. Un constat qui interroge également sur le cadre des collectes de données réalisées par les polices du vieux continent notamment dans le cadre du pass sanitaire. Je ne vous cacherai pas que cette situation soulève de nombreuses interrogations. Il me semble intéressant d'avoir une approche transversale du numérique : technologique, socio-économique, normative/légale. L'affirmation de la souveraineté numérique est devenue un fil rouge dans la définition et la mise en

œuvre de la gouvernance européenne. Les technologies numériques sont en train de changer la vie des citoyens. Il appartient à l'Union Européenne de faire en sorte que cette transformation profite aux citoyens et aux entreprises. « Celle-ci doit maintenant renforcer sa souveraineté numérique et fixer des normes au lieu de suivre celles des autres, en mettant clairement l'accent sur les données, les technologies et les infrastructures ».

10/ Il y a 300M de francophones dans le monde. Est-ce que cela vous inspire de possibles initiatives sur le terrain du numérique ?

Philippe LATOMBE

300 millions de francophones, c'est le chiffre de l'OIF. Il est contesté. Certaines estimations sont beaucoup moins optimistes et avancent 130 millions, car elles prennent en compte ceux dont le niveau de français en permet une maîtrise suffisante pour un usage courant et quotidien, voire professionnel. Par ailleurs, **si vous prenez l'exemple de l'Afrique, les Américains et maintenant les Chinois ont fait main basse sur les marchés. On peut parler de cyber-colonialisme.** S'il y a des créneaux où la France peut encore espérer s'implanter, ce serait plutôt dans des niches technologiques très spécifiques comme la cybersécurité, la télé-médecine, les nouvelles technologies agricoles ou le télé-enseignement, et cela demande un accompagnement, notamment concernant la sécurisation des projets d'implantation.

Cosimo PRETE

J'aurais un clin d'œil pour le programme French Tech Tremplin qui vise à faire en sorte que l'écosystème de La French Tech soit aussi riche et pluriel que la société dont il est issu. Il a été conçu pour rééquilibrer les chances et faire en sorte que tous les talents aient accès aux mêmes avantages que les

entrepreneurs issus de milieux plus privilégiés. En qualité de membre du jury, j'ai eu la chance de découvrir des candidats qui ont des projets passionnants. Peut-être une opportunité de découvrir dans la prochaine newsletter de « Souveraine Tech » le détail de ce programme et le témoignage des candidats !

---

3 questions à Philippe Caduc, PDG de l'ADIT / 17 janvier 2022

Vous venez d'annoncer l'entrée du fonds Sagard dans le capital de l'ADIT ? Pouvez-vous nous expliquer l'objectif de cette opération ?

Chacun a bien compris l'importance croissante que prennent les métiers de l'intelligence stratégique et économique, de la compliance et de la protection des actifs stratégiques des entreprises. Le contexte géostratégique, marqué par une nouvelle vigueur des tensions interétatiques, par le renforcement d'acteurs interétatiques criminels ou terroristes ainsi que par la numérisation pose un ensemble de défis qui nécessitent de disposer d'une masse critique, d'une présence globale et de capacités pointues dans de nombreux domaines d'expertise.

Dans ce contexte, nous travaillons à renforcer le leadership français, européen et francophone de l'ADIT sur l'ensemble des métiers. Sagard est aujourd'hui en négociations exclusives avec Parquest, le fonds qui nous soutient depuis 3 ans. A l'issue de ces discussions, il devrait devenir notre premier actionnaire, à un niveau proche de la majorité en capital. L'Etat conservera une action de préférence, et Parquest, BPI

et Amundi resteront actionnaires. Nous sommes très heureux de l'intérêt de Sagard pour l'ADIT. C'est un fonds créé en France il y a près de 20 ans, qui accompagne les PME françaises dans leurs stratégies de développement, en France et à l'international. Il est basé en France et regroupe des investisseurs majoritairement européens, aux côtés de la famille québécoise Desmarais. Sagard bénéficie d'une excellente réputation : ils ont accompagné plus de 35 entreprises françaises dont des actifs stratégiques comme Souriau et Sabena et ils ont investi à plusieurs reprises aux côtés de la BPI.

L'entrée de Sagard au capital de l'ADIT va nous donner les moyens de poursuivre notre stratégie.

Comment la gouvernance de l'entreprise va-t-elle évoluer ?

Rien ne change dans la raison d'être, dans le management et la préservation des enjeux de souveraineté. L'autonomie stratégique et géostratégique de L'ADIT est plus que jamais préservée avec des actionnaires financiers qui continuent d'investir et d'autres qui vont permettre le développement international de L'ADIT.

L'augmentation du nombre d'actionnaires financiers aux côtés de l'Etat, de la BPi est une garantie d'autonomie stratégique. Nous sommes dans une logique de consortium de fonds, Sagard prenant une part d'actionnaire de référence inférieure à 50%

Le capital reste majoritairement français, auprès des 3 actionnaires actuels qui restent (Parquest, Bpifrance et Amundi).

Sagard est un FPCI français à capitaux majoritairement européens (les deux tiers); géré par une société de gestion française dont les associés sont français.

Les droits de BPi et la souveraineté de l'Adit ont encore été renforcés lors de cette opération.

L’Etat continue d’exercer son contrôle et son agrément avec les serveurs, la gouvernance, et les habilitations.

Sagard pourra contribuer à soutenir de le développement de l’Adit sur le marché francophone et sur le marché nord américain et consolider sa position de champion français du secteur

Quels sont les grands enjeux et perspectives l’ADIT pour les années à venir ?

Le renforcement actionnariat se fait dans la continuité des étapes précédentes avec une vraie stratégie au regard des enjeux d’européanisation et d’internationalisation du business. Cela doit permettre à court, moyen et long terme d’adosser l’ADIT à des actionnaires stables et de confiance lui permettant de poursuivre sa stratégie de consolidation du secteur, tout en ouvrant à la société de nouvelles perspectives de marché à l’international.

Notre projet est de continuer à bâtir un groupe français, avec un siège à Paris et à dimension souveraine, mais aussi européen, francophone et transatlantique. Par-dessus tout, nous serons toujours autonomes et indépendants, aucun actionnaire ne devant avoir un droit de regard sur les dossiers traités pour tous nos clients.

Vous aurez compris que nous annoncerons différentes opérations dans les prochaines années, dans différentes zones géographiques, et que nous allons accroître notre présence dans des environnements neutres, non-alignés entre les Etats-Unis et la Chine.

Allo Houston ?

Le 7 janvier, la Revue du Digital a publié une nouvelle intitulée “Nucléaire français : un Data Lake Microsoft pour entraîner ses intelligences artificielles”.

Nous sommes le 14 janvier, et les sondes de la conscience politique peinent encore à identifier des signes de vie sur la planète parlementaire. Si d’aventure vous avez un de ses habitants à portée de main et que vous maitrisez les premiers gestes de secours, n’hésitez pas à le ranimer ou à lui tendre un verre de schnaps. Merci. En attendant, préparez-vous à entendre les justifications les plus capillotractées au fait que des données relatives aux installations d’un Opérateur d’Importance Vitale (OIV) soient amenées à être exposées de près ou de loin à l’attention d’une multinationale étrangère.

Nous ne sommes plus à ça près.

Dans le domaine du Cloud l'alliance Euclidia est une chance pour les acteurs Européens de proposer et de rendre visible un catalogue en mesure de remplacer les

produits dominants.

Ophélie Coelho est spécialiste en géopolitique du numérique à l'Institut Rousseau. Cet entretien a été publié le 14 janvier 2022.

1/ Figurez-vous parmi les tenants de la souveraineté numérique, et le cas échéant, de quelle espèce particulière êtes-vous dans cette famille bigarrée ?

Aucun acteur, même une Big tech, ne peut prétendre aujourd'hui maîtriser l'ensemble de son "territoire numérique".

Les interdépendances entre les acteurs techniques constituent un phénomène normal du monde numérique, autant pour la couche logicielle que celle des infrastructures. Rappelons simplement que pour produire réseaux et terminaux, il est nécessaire d'extraire des métaux qui sont répartis inégalement sur la planète, avec des écarts de quantité et de qualité. Certains pays sont des territoires plus favorables à l'installation des serveurs nécessaires à la vie numérique, tout simplement parce qu'ils sont localisés dans des zones froides : Google installe de nombreux centres de données en Finlande où l'eau de mer du golfe de Finlande permet de réduire sa consommation d'énergie. La France est également un territoire intéressant pour ces infrastructures gourmandes en eau et sa facture énergétique reposant sur le nucléaire. Ainsi, les interdépendances du monde numérique commencent par le territoire, ses richesses, sa géographie, son histoire.

Mais dans cet environnement, il y a de très grandes disparités de pouvoirs. Nous le voyons aujourd'hui dans la difficulté que rencontrent les États européens à réguler les grandes entreprises du numérique, principalement les Big techs américaines. Dans une certaine mesure, les États-Unis sont eux-mêmes confrontés à cette difficulté, et la politique antitrust de l'administration Biden fait face à sa propre

dépendance aux géants du numérique.

Pour toutes ces raisons, il me semble que le terme “souveraineté” associé au numérique réduit parfois le périmètre d’analyse. Il me paraît plus juste de parler de dépendances numériques, d’en mesurer les conséquences afin d’apprendre à les gérer et à en sortir lorsque celles-ci deviennent critiques.

2/ Face aux Big Techs, quel est selon vous le meilleur moyen de reprendre la maîtrise de notre destin technologique ?

Nous devons sortir de la logique de « transformation numérique » à bas coût, et engager une véritable stratégie industrielle pour le numérique.

Le concept même de « transformation numérique » , associé aux politiques de modernisation des États et des entreprises portées au niveau national et européen, a été très néfaste au numérique européen. Il a conduit à l’accélération de l’adoption des produits issus des GAFAM, dans un contexte où la réglementation ne garantissait aucun garde-fous dans l’usage primaire et secondaire des données numériques. Les travaux de la Commission européenne ont produit avec peine un droit du numérique qui ne peut fonctionner que sur le principe de confiance, puisqu’elle n’a en aucun cas accès au code des produits et ne peut donc contrôler l’ensemble de la chaîne numérique.

Aujourd’hui, la seule manière de sortir de cette situation critique de dépendance est d’établir une stratégie industrielle qui repose sur la maîtrise des technologies et non sur l’illusion d’une réglementation à l’aveugle.

Pour cela, il nous faut mettre en place une stratégie de remplacement des dépendances critiques, en commençant par les secteurs sensibles comme celui de la santé, de la sécurité ou de l’énergie. Nous avons des acteurs européens matures sur de nombreux sujets techniques, et d’autres qui nécessitent

simplement des améliorations ciblées pour fournir le service adéquat. Dans le domaine du cloud par exemple, l'alliance Euclidia est une chance pour les acteurs européens de proposer et de rendre visible un catalogue en mesure de remplacer les produits dominants. Pour un État qui souhaiterait un service cloud proposant également du machine learning, il est possible d'inclure au catalogue des entreprises européennes spécialisées sur ces sujets. Mais pour cela, les États doivent aussi sortir de leur position de simples clients et accompagner les entreprises du secteur dans la constitution d'un catalogue adapté à des projets stratégiques.

Nous avons également besoin d'assumer un protectionnisme ciblé, et la commande publique peut être un outil au service de la souveraineté numérique. Concernant les aides d'État, l'Europe s'est imposé un cadre limité, laissant perdurer une timidité budgétaire que n'ont pas les États-Unis ou la Chine en matière de financement des technologies : l'article 107 du Traité sur le fonctionnement de l'Union européenne (TFUE) interdit les aides d'État qui auraient vocation à « fausser la concurrence ». Mais le TFUE prévoit aussi des dérogations aux limites budgétaires imposées aux États, qui leur permettent d'activer des programmes de financement indépendants de la Commission européenne. Dans l'article 107, le point 3.b dispose en effet que les aides d'États peuvent être activées si celles-ci sont « destinées à promouvoir la réalisation d'un projet important d'intérêt européen commun ou à remédier à une perturbation grave de l'économie d'un État membre». Au-delà du financement public, il s'agit également de renforcer la protection de nos entreprises innovantes de toutes ingérences ou prise de contrôle par des acteurs dominants. Il existe déjà des limites établies pour le rachat et la prise de capital, mais cette attention ne prend pas en compte la mise en dépendance technologique.

Bien d'autres leviers existent encore, que nous n'utilisons pas.

3/ Faites-vous une distinction entre les États-Unis et la Chine au regard de la concurrence / dépendance que ces deux pays représentent pour les nations européennes ?

En Europe, nous sommes majoritairement dépendants des technologies américaines. C'est donc d'abord vis-à-vis des acteurs étasuniens que nous devons trouver un équilibre. Mais cela ne veut pas dire qu'il est préférable d'opter dans le futur pour des technologies chinoises. Dans une récente étude, j'analyse la stratégie industrielle chinoise et j'aime à rappeler les écueils du numérique chinois tout en détaillant les choix stratégiques qui permettent à la Chine d'atteindre aujourd'hui une certaine forme d'indépendance numérique.

Notre faiblesse repose dans l'absence de stratégie industrielle pour le numérique, quand ces deux pays appliquent un protectionnisme ciblé en faveur de leurs géants technologiques.

4/ Trouvez-vous la politique numérique gouvernementale lisible et cohérente, à défaut d'être opportune ou efficace ?

Je pense qu'il y a une prise de conscience, de la part de certains responsables politiques, que des erreurs ont été commises sur des projets anciens ou plus récents, comme le Health Data Hub. C'est le résultat d'une forte médiatisation du sujet de la souveraineté numérique depuis deux ans, qui jusque-là n'intéressait que les spécialistes, et il y a probablement plus de non-avertis qui comprennent aujourd'hui le problème des dépendances numériques.

Mais malgré les débats et le récent rapport produit par la commission des Affaires étrangères ou la mission d'information sur la souveraineté numérique à l'Assemblée nationale, le gouvernement s'est jusqu'à présent contenté de mettre en place des garde-fous accessoires et a poursuivi dans sa lancée du "Cloud de confiance". Ce dernier favorise et accélère pourtant l'adoption des technologies issues des Big techs, sans

stratégie alternative pour s'en défaire.

En voulant aller trop vite et en faisant toujours le choix de la transformation numérique à bas coût, on accélère des dépendances bien souvent irréversibles.

5/ Le Vieux Continent a l'air de croire que le droit qu'il édicte palliera son manque de pugnacité sur le marché du numérique. Pensez-vous que cela suffira ?

Le droit du numérique est très influencé par les lobbies des géants du numérique, devenus ces dernières années à la Commission Européenne plus puissants que ceux du pétrole. La stratégie "DSA 60-Days Plan Update" de Google, dévoilée par la presse française en 2020, décrivait par exemple très bien les techniques d'influence employées par l'entreprise auprès des législateurs en charge de la formulation du Digital Services Act (DSA) et du Digital Market Act (DMA).

Par ailleurs, même une fois que le droit s'applique, le législateur peine à le faire respecter. Rappelons que Facebook a refusé en décembre dernier de suspendre les transferts de données de l'UE vers les États-Unis alors même que la Commission irlandaise de protection des données a formulé un ordre préliminaire dans ce but suite à l'annulation du Privacy Shield par la Cour de justice de l'Union Européenne (CJUE).

Enfin, à aucun moment le législateur n'a accès au code informatique du produit, ni n'a la possibilité de suivre les transferts d'informations une fois les données collectées. Comment faire appliquer un droit sans avoir la possibilité de contrôler le respect ou non de ce droit ?

Tout cela, et d'autres points encore, constituent de véritables faiblesses pour l'application d'un droit du numérique dans le contexte actuel. Cela nous éclaire sur le fait qu'il ne suffira pas d'édicter des règles et des limites légales pour rétablir l'équilibre, et que la maîtrise des technologies est un passage obligé.

Nous ne pouvons continuer à être de simples clients de plateforme attendant patiemment la réponse du service après vente.

6/ Que vous inspirent les partenariats "pragmatiques" noués par les entreprises françaises avec les Molochs du numérique ? (Orange, Atos, Thalès, SNCF, Engie, GAIA-X, AFP, BPI etc.)

Je crois qu'on parle plutôt de "partenariat stratégique", en particulier dans le domaine du cloud. Et ils sont en effet stratégiques pour certaines de ces entreprises : Orange, Atos et Thalès ont tout intérêt à rester les alliés économiques des AWS, Microsoft et Google qui dominent le marché. Car ces partenariats leur permettent de tirer profit, au moins temporairement, de la délégation technologique. Dans ce genre d'alliance, ils ne produisent pas eux-mêmes les services qu'ils vendent et deviennent de simples intermédiaires. Cela les conduit évidemment à assumer la responsabilité légale en cas de problèmes techniques ou de fuite de données. En somme, c'est presque du dropshipping adapté au cloud.

Ces partenariats, pour des acteurs comme Orange, concernent d'autres activités comme les câbles sous-marins de télécommunication ou la stratégie de développement commerciale en Afrique. Et cela ne concerne pas qu'Orange, mais de nombreuses entreprises de télécommunication qui délèguent progressivement la charge technologique et financière de leurs services et infrastructures aux Big techs, tout en se positionnant comme des partenaires territoriaux importants dans leur développement. C'est particulièrement vrai en Europe : Deutsche Telecom (T-Systems), Telecom Italia, Telefonica, Vodafone … et d'autres encore ont tous signé un ou plusieurs partenariats stratégiques avec Google, Amazon ou Microsoft.

En ce qui concerne les choix de la SNCF, de la BPI, de Sanofi ou encore de l'AFP, il est légitime de se demander si ces entreprises ont une équipe chargée de la gestion des risques. En effet, comment comprendre que des entreprises ou des

administrations stratégiques pour le pays choisissent de confier des données parfois sensibles à des entreprises soumises aux enjeux d'extraterritorialité du droit, dans un contexte où la CJUE a reconnu (certes avec dix ans de retard…) les risques de surveillance des données par l'administration américaine ? Comment comprendre la confiance aveugle dans les acteurs technologiques que sont les Big techs, au regard de tout ce que l'on connait de leurs écarts passés et présents, quand tout développeur sait qu'il est tout à fait possible d'accéder aux données des utilisateurs d'un produit numérique, notamment en phase de recherche et développement ?

7/ Le numérique, qui a crû sur la promesse d'une liberté accrue pour les hommes et les peuples, est devenu en parallèle un arsenal de moyens de contrôle au service des gouvernements et un prétexte à l'assistanat personnel. Comment revenir à l'esprit des origines (pas celui d'Arpanet ou MilNet) ?

Je ne pense pas qu'il soit possible de "revenir à l'esprit des origines". D'abord parce qu'internet, tel qu'il a été conçu, permet la surveillance du réseau. Il n'a pas été conçu par défaut pour protéger les données des utilisateurs. À partir de là, n'imaginez pas qu'un pays qui dispose des possibilités techniques de surveillance s'en prive ! Ensuite, parce que cet esprit n'a pas survécu à la démocratisation d'internet. Si au départ le réseau des réseaux n'était utilisé que par quelques passionnés, le web est vite devenu un outil stratégique pour les entreprises et les États ainsi qu'une opportunité de marché qui s'est exprimé en tout premier lieu avec la bulle internet des années 2000. L'esprit des origines, qu'on retrouve dans la philosophie du libre mais aussi dans l'universalisme des Lumières, n'est malheureusement pas compatible avec la recherche des intérêts particuliers qui dominent nos sociétés.

8/ Votre homonyme Paulo Coelho encourage le "piratage des livres". Que pensez-vous du changement de notre rapport à la propriété, notamment des objets de culture, alors que croît

tranquillement l'économie des jetons non fongibles (Non Fungible Token, NFT) ?

Quand Paulo Coelho a commencé à "pirater" ses propres livres, c'était dans les années 2000. À ce moment-là, il n'existait pas de liseuse permettant de lire confortablement un livre, et on peut comprendre que les lecteurs ne lisaient que quelques chapitres sur leur écran d'ordinateur avant d'acheter le livre. Les ventes ont donc été impactées positivement par la mise en ligne gratuite des ouvrages de Coelho à cette époque. Il faut aussi prendre en considération le fait que l'auteur ne partait pas de rien : il était déjà connu et traduit dans de nombreuses langues, et la diffusion du livre numérique profitait ainsi de sa notoriété internationale. Un auteur inconnu qui ferait la même chose aujourd'hui, quand bon nombre de lecteurs utilisent quotidiennement une liseuse, ne pourrait probablement pas vivre de son travail.

Comme beaucoup, je me pose des questions sur la pertinence de l'économie des NFT dans le monde de l'art. Dans un contexte où beaucoup d'artistes ne parviennent pas à vivre de leur art, cela pourrait en théorie permettre à certains de se rémunérer. Mais quant à savoir si une œuvre numérique équivaut à une œuvre matérielle… C'est très subjectif, et ce qui compte à mon avis est surtout la qualité de l'œuvre en premier lieu. Là-dessus, l'économie des NFT favorisera-t-elle la diffusion de chefs d'œuvres ou la mise sur le marché d'une multitude de produits du fast art ?…

Concernant l'accès et la diffusion des savoirs, nous vivons à un époque où une vie entière ne suffirait pas à lire et intégrer l'ensemble des connaissances qui nous parviennent quotidiennement. Privilégier la qualité à la quantité, limiter le nombre d'informations et être capable de conserver notre capacité de concentration est un enjeu majeur pour nos sociétés à l'ère numérique.

Je ne peux donc qu'espérer que la lecture de cette newsletter

aura valu la peine de dépenser votre temps de cerveau disponible

Noces funestes et doigts dans la prise

L’année commence fort avec l’annonce des noces funestes entre Amazon et… Stellantis (ex-PSA).

Voilà que l’Europe prend la route sous assistance et surveillance américaines. C’est à se demander si notre industrie n’est pas prise de tendances suicidaires… Alexa n’a t-elle pas récemment conseillé à une fillette de 10 ans de mettre ses doigts dans une prise électrique ? Dieu seul sait la nature du conseil qu’elle pourra bien nous donner sur l’autoroute !

Heureusement, ce qui est défait par des Hommes peut être refait par d’autres.

Pourquoi la NSA aurait-elle seulement ciblé les banques suisses via les serveurs Sun

Solaris vendus désormais par Oracle ?

Dimitri Nokovitch est fondateur et président d'ArmadAI. Cet entretien a été publié le 7 janvier 2022.

1/ Que recouvrent les domaines de la gouvernance des identités et accès, et des habilitations ?

La Gouvernance des Identités et des Accès informatiques (GIA) permet de définir « qui est qui » en tant que personne et utilisateur du système d'information, « qui est où dans l'organisation » et « qui fait quoi », pour définir quels droits d'accès accorder.

Elle concerne la gestion des RH, les opérations, la sécurité d'accès à ses ressources, notamment les plus précieuses contre les fraudeurs et les pirates informatiques.

C'est une évolution de la gestion des accès informatiques réalisée par des administrateurs techniques de manière plus ou moins manuelle.

Le gestionnaire de comptes d'utilisateurs et d'accès le plus connu, c'est Edward Snowden. Parce-qu'il était qu'administrateur du système Sharepoint de la NSA, il a pu naviguer dans les répertoires de cette agence, y consulter les documents qui paraissaient intéressants avant de les exfiltrer comme on sait.

La Gouvernance des identités et des accès en mode SaaS augmentée par de l'IA, va bien au-delà de ce que faisait Snowden. Elle automatise des tâches d'analyse et de gestion et traite des volumes de données impossibles à administrer humainement.

Elle peut donc, le cas échéant automatiser ce qu'a fait Edward

Snowden dans une logique de double-usage.

2/ Nos grandes entreprises vous semblent-elles bien préparées aux risques afférents ?

Tous les RSSI sont conscients que la GIA est LE sujet qui donne accès aux clés du Royaume. Mais les dimensions extraterritoriales et d'Intelligence économique échappent à beaucoup d'entre eux. Or, les leaders du secteur sont soumis au PATRIOT Act, CLOUD Act, etc… Microsoft l'a admis, sur une injonction d'un tribunal, ils n'ont d'autre choix que donner accès aux données de leurs clients pour que des investigations soient menées en toute discrétion par les services de renseignement.

Effectuez des recherches sur Google en combinant le nom du leader de la GIA avec les sigles NSA, SAIC (fournisseur historique de solutions de la NSA), Federal agencies ou le nom du Général Hayden, ex-directeur de la NSA. Et rappelez-vous ce que Snowden soulignait quant à l'importance des partenariats technologiques des éditeurs américains avec cette agence. **Demandez-vous ce qui peut se passer dans plus de la moitié des groupes du CAC 40 qui envisagent de basculer vers les versions SaaS d'outils soumis au CLOUD Act et vendus par des sociétés dont des plaquettes marketing US ont des liens qui pointent vers le site de la NSA.**

3/ En l'état actuel de cette gouvernance, diriez-vous que l'économie française est à livre ouvert ?

Le livre est ouvert depuis les tout débuts d'lnternet pour les entreprises ainsi que l'a révélé la Radio Télévision Suisse. L'an dernier, dans « Temps Présent », elle dénonçait **la société Sun Microsystems qui a livré pendant des années des serveurs dotés de portes dérobées matérielles et logicielles qui ont réduit à néant le Secret Bancaire Suisse.**

En France comment la SG ou BNPPARIBAS ont-elles été harponnées techniquement et conduites à payer jusqu'à 6,5 milliards

d’euros? Pourquoi la NSA aurait-elle seulement ciblé les banques suisses via les serveurs Sun Solaris vendus désormais par Oracle ? Un des membres du Campus Cyber…

Mais avec les fournisseurs de solutions de GIA soumis aux lois extraterritoriales nous entrons dans une nouvelle dimension. Plus les entreprises utilisatrices amélioreront la qualité de leurs données avec ces outils, plus elles simplifieront l’exploitation d’informations concernant leur structure opérationnelle, leurs chaînes de responsabilités, le support de leurs activités, systèmes, ressources et personnes clés.Pour mener le cas échéant des opérations autrement plus efficaces et rapides que celle qui a été lancée contre Alstom.

4/ Comment expliquez-vous que les avertissements publiés sur ce sujet, notamment par vous, n’aient pas été pris en considération ?

La Gouvernance des Identités et des Accès est une thématique peu connue, hormis des spécialistes. C’est quand on voit ce que son double usage recouvre qu’on réalise l’ampleur de la menace, notamment au niveau des groupes du CAC 40.

La DGSI et la DRSD ont montré un total désintérêt au sujet porté à leur attention, notamment via le GICAT sur une situation ubuesque que nous lui avions remontée. Mais les représentants de la DGSI arboraient des stylos avec le logo de Palantir. Alors ceci explique peut-être cela.

Il y a une forme de naïveté vis-à-vis des fournisseurs US de la part de toutes sortes de gens influencés par des années de soft-power et de Marketing rassurant. Genre : « C’est vous qui avez les clés de chiffrement et la réversibilité est garantie ».

Cas exemplaire, la BPI ayant retenu AWS pour supporter le PGE (Prêt Garanti par l’Etat) et exposée par Franck DeCloquement dans Atlantico.

Il y a aussi ceux qui ne veulent ni parler, ni entendre, ni voir par peur et/ou par intérêt, refus d'assumer des mauvais choix.

Des sociétés de conseil sont dépendantes de leurs relations avec des leaders américains qui les invitent à répondre à des appels d'offres « Editeur/Intégrateur » portant sur des centaines de milliers d'euros de vente de prestations. Il y a enfin des associations et cercles professionnels dont les événements, parfois de grand luxe, sont commandités à grand frais par ces fournisseurs. CQFD

5/ Comment articulez-vous la question de l'identité numérique et celle de la gouvernance des accès ?

Usurper une identité et utiliser un mot de passe compromis c'est une chose.

Mais ce qui est vraiment important pour l'usurpateur, c'est exploiter l'identité compromise pour disposer d'accès à des systèmes et à de l'information stockée dans les répertoires de l'organisation.

Les outils de Gouvernance d'identités et d'accès peuvent donner accès aux clés du Royaume car ils fournissent des informations qui vont bien au-delà de la simple identification d'une personne.

Ils révèlent la localisation des employés dans l'organisation opérationnelle et géographique, leurs relations opérationnelles et hiérarchiques, les sujets sur lesquels ils travaillent. Notamment les sujets sensibles.

Avec la puissance de traitement offerte par l'IA et le Big Data, ces outils peuvent traiter des dizaines de millions de droits pour identifier les quelques milliers qui sécurisent l'accès à des informations confidentielles.

C'est ce que nous sommes capables de démontrer logiquement et

pratiquement avec notre propre outil que nous avons pu qualifier dans de grandes et très grandes organisations.

6/ Avec la question de l'hébergement et celle des logiciels bureautiques, la gouvernance des accès constitue t-elle le troisième pilier d'une souveraineté numérique française menacée?

Et comment ! Les GAFAM attaquent la souveraineté des données concernant Monsieur et Madame « Tout le Monde ». Les GAM-IAM, Google, AWS, Microsoft et les fournisseurs de solutions de GIA/IAM, posent une menace sur la souveraineté des données internes des entreprises. Et **le RGPD n'offre pas une protection suffisante des données et des métadonnées des personnes morales.**

Avec la GIA augmentée par de l'IA, on ne parle pas de la santé du système digestif de Monsieur ou Madame X, on parle de l'organisation interne de la personne morale Y, de sa chaîne de commandement et de ses assets sensibles. Mais avec le modèle Chinois, on va être confronté à pire encore avec un modèle centralisé en Chine pour gérer les accès informatiques aux systèmes de la Route de la Soie.

Le champion Chinois s'appelle BambooCloud. Retenez ce nom.

Ses partenariats technologiques intègrent HUAWEI sur les accès à des infrastructures importantes, des villes, des aéroports. Les accès informatiques de HUAWEI France sont eux-mêmes gérés à partir de la Chine.

C'est BambooCloud qui supportera les accès informatiques de la Route de la Soie.

Alors que se passerait-t-il en cas de mésentente entre un groupe multinational qui intégrerait la supply-chain chinoise et qui s'écarterait des exigences de cette hyper-puissance?

On lui couperait ses accès informatiques aussi nettement que

les Russes le font en ce moment avec le gaz vis-à-vis de l'Allemagne en plein hiver.

7/ Vous avez créé une technologie au Canada. Pourquoi la France vous a-t-elle amené à aller le chercher là-bas ?

En France, on n'aurait jamais eu financièrement la possibilité de réaliser le projet ArmadAI. Et pendant la pandémie, la société n'aurait pas survécu sans le soutien du Canada. La vision régalienne de la cybersécurité présente beaucoup plus d'atouts que le modèle Français, tiré essentiellement par le « Privé » sans la direction de l'Etat vers un intérêt commun. Le modèle fiscal au Canada est aussi très incitatif. Les remboursements de frais de R&D sont de l'ordre de 45% à 50% contre 25% en France. Les subventions sont plus généreuses pour des programmes de R&D et avec des conditions d'accès qui favorisent des entreprises en démarrage et pas seulement celles qui sont en phase de croissance. **Au Canada, il y a des accès aux marchés publics qui sont l'équivalent du Small Business Act américain avec un écosystème qui laisse leur chance aux jeunes pousses.**

8/ En quoi la France devrait-elle selon vous s'inspirer du modèle canadien ?

La France devrait créer un ministère de la Cybersécurité, comme au Québec, avec des pouvoirs règlementaires pour éviter les dérives, compromis, conflits d'intérêts et tiraillements qu'on constate dans les initiatives du Privé. GAIA-X en est le parfait exemple.

Au Canada, on a conscience du risque américain alors que ce pays fait lui-même partie des « Five-Eyes ». Alors on donne des moyens aux entreprises nationales.

La France et les entreprises françaises devraient donner leur chance aux alternatives locales et rejeter le « Nice to Have » américain quand le sujet relève de la Souveraineté numérique et qu'il y a des acteurs nationaux en lice.

Le Gouvernement Fédéral finance directement et indirectement toute sorte de projets avec pour objectif que les startups aient leur premier grand client et à la clé entre 500 K et 1000 K $ selon qu'on parle de projets civils ou militaires.

La France devrait avoir un Small Business Act et ouvrir la perspective de premiers clients au niveau Gouvernemental, puis du soutien étatique vis-à-vis des entreprises privées ?

La France devrait aussi s'aligner sur le Canada en termes de financement de R&D pour compenser la pesanteur de la fiscalité.

9/ Est-ce bien sérieux de ne laisser qu'aux mains de l'entreprise privée des sujets numériques qui touchent bien souvent à la souveraineté nationale ?

Avec le SecNumCloud de l'ANSSI, c'est une bonne chose que des « risques résiduels » soient évoqués au regard du risque extra-territorial et du cyber-espionnage. Les RSSI peuvent alors prendre des décisions au regard de leur appréciation du risque.

Mais qu'en est-il quand c'est trop tard, que les décisions ont été prises par d'autres, que l'entreprise est sous surveillance/tutelle et qu'un choix d'alternative Souveraine pourrait être interprété comme une tentative de dé-vassalisation ?

Que se passerait-il aux USA, en Russie ou en Chine si un obscur RSSI aimant voyager décidait de retenir un SaaS de gestion des accès à une supply-chain supportant des intérêts souverains, soumis à une législation extraterritoriale et dont le responsable des partenariats serait un ancien agent du FSB, d'un service secret US ou du Diaochabu ? Une mise au pas vigoureuse ! Mais pas en France où **c'est un non-sens que l'ANSSI et la DRSD n'aient pas un pouvoir d'injonction quand des échelons subalternes d'entreprises stratégiques font des choix inconsidérés qui exposent leur organisation au risque**

d'Intelligence Economique, de perte de souveraineté ou de grands marchés.

10/ A part les personnels militaires, qui voyez-vous porter les sujets de souveraineté numérique de manière absolument incorruptible ?

Comme l'énonçait Edgar Morin : « la frontière est difficile à trouver entre compromis et compromission ».

Et dans le cas de la cybersécurité, il ne devrait pas y avoir de compromis et de conflits d'intérêts. Faute d'un ministère de la Cybersécurité comme au Québec, le SGDSN devrait porter le sujet en priorité du fait de sa position dans l'organigramme d'Etat, de sa nature et de ses branches, dont l'ANSSI qui devrait avoir un pouvoir d'injonction.

Le pôle d'excellence cyber de Rennes, dont les membres sont fortement connotés « défense » et OIV me paraît être le meilleur garant de la souveraineté numérique. HEXATRUST devrait jouer le même rôle que les « grappes » canadiennes évoquées précédemment avec le même genre de financement étatique qu'in-Sec-m ou SCALEAI au Canada. Ainsi ce sont des critères souverains et impartiaux qui s'imposent.

Je suis très réservé quant au Campus Cyber de la Défense. Qui a laissé entrer des fournisseurs de solutions soumises au CLOUD Act et suspectées d'être dotées de back-doors matérielles et logicielles ? L'un des principaux acteurs du Conseil en GIA, qui est un des premiers signataires, supporte le partenaire de la NSA que j'évoque régulièrement depuis plus d'un an. Notamment en déployant la solution de ce dernier dans le Groupe Caisse des Dépôts et Consignations…Quel intérêt pour une entreprise innovante comme la mienne, qui annonce clairement la couleur en termes de souveraineté, de rejoindre un écosystème compromis comme celui-ci ? Mais avec la vague de souveraineté actuelle, il faut donner une chance de revenir dans le giron de l'Eglise.

11/ Pouvez-vous décrire les conditions nouvelles dans lesquelles 'l'Eglise serait remise au milieu du village » sur ces questions ?

L'indignation soulevée par les agissements des hyper-puissances doit être le moteur d'un renouveau du patriotisme.

La première condition, c'est la volonté d'agir avec le sens de l'Etat, du patriotisme et de l'intérêt général. Comme le général de Gaulle a su le faire et comme Israël, les USA, la Chine ou la Russie le font.

La seconde condition, c'est comprendre que dans toutes sortes de domaines, et de GIA notamment, il y a une dimension culturelle. Même les patriotes de la dernière heure et de la dernière seconde devraient comprendre que la Souveraineté est une opportunité et que collaborer avec des fournisseurs étrangers n'est ni éthique, ni logique à long terme.

La troisième condition, c'est de considérer que l'innovation des petites structures doit être portée par l'Etat et les grandes entreprises au lieu d'être négligée.

Un PoC gratuit à la Société Générale, c'était le prix du "Banking Cybersecurity Innovation Award »s dans lequel nous étions finalistes. Alors que notre service aurait permis d'économiser des millions d'euros en coûts opérationnels comme nous avons pu l'analyser dans un groupe de 250.000 employés. Qui préfère faire par lui-même ou acquérir une solution d'un leader…

En Chine, BambooCloud va surclasser le leader mondial de la GIA, parce-que l'Etat et les grandes organisations chinoises l'ont fait prospérer en comprenant les enjeux sur le long terme. Et pas avec des micro-projets ou des PoC gratuits.

12/ Croyez-vous encore dans la vertu de la loyauté contre le pouvoir de l'argent ?

Dans le secteur de la gestion des accès informatiques, **des Français sont parfaitement au fait des enjeux et de leur collaboration indirecte avec des services étrangers.** Leur situation est embarrassante et les réduit à la gêne et au silence quand on les confronte à une réalité factuelle. Mais c'est secondaire. Leurs fins de mois sont logiquement et humainement prioritaires.

Les dirigeants de cercles professionnels dont les événements et coûts de fonctionnement sont financés parfois depuis plus de 15 ans par des fournisseurs américains ne vont pas du jour au lendemain renoncer à des commandites conséquentes.

Ils se raidissent quand leur loyauté est mise en cause mais une fois encore entre compromis et compromission, la frontière est mince.

A terme, je suis confiant si la vague actuelle de souveraineté s'amplifie, sauf si elle est portée par les mauvaises personnes et qu'elle n'est qu'un élément de langage.

13 / Êtes-vous un tenant de la souveraineté nationale ou de ce que certains appellent la « souveraineté européenne" (en fait communautaire) ?

Il n'y a pas en Europe de creuset d'intégration suffisamment fort autour de valeurs et de langues véhiculaires communes. Et il y a une allégeance de trop nombreux pays vis-à-vis des USA.

Je suis donc un tenant de la souveraineté des nations au sein d'une communauté européenne car chaque nation dispose de ses particularités culturelles et d'intérêts divergents.

En me basant sur mon expérience multiculturelle et dans un domaine dans lequel j'évolue depuis plus de 20 ans, je ne crois pas à une souveraineté européenne imposée à tous, ni à une McDonaldisation occidentale ou européenne de la gestion des identités numériques des personnes physiques et morales.

L’expérience de Smart City menée par Google à Toronto que ses citoyens ont rejetée est exemplaire. La question des données personnelles a été très importante : elle a fait polémique du début à la fin du projet qui, s’il avait pu être validé par Toronto, l’aurait été à des conditions trop contraignantes pour Google.

Et je pense qu’un modèle Chinois qui découlerait du déploiement massif de télésurveillance dans des villes françaises soulèverait le même rejet des citoyens.

Il y a donc une ouverture pour un modèle souverain Français qui devrait être porté par HEXATRUST et l’Etat Français avec un verrouillage total quand il y a des acteurs nationaux en lice.

Mais cette ouverture est très mince et je n’y crois pas d’ici la fin de ma carrière professionnelle.

14/ La question du financement est cruciale. Pensez-vous que la France arrose les bonnes plantes avec la “French Tech” ?

En France les conditions d’accès au financement de R&D sont désespérantes. En 2018, nous avons été sollicités par France IA pour présenter un projet à Bercy parmi 5 autres. Mais nous avons seulement servi de faire-valoir. Nous avons été encouragés par l’ANSSI à postuler à un programme de financement mais nous ne remplissions pas les critères et nous avons renoncé.. A la BPI France, on ne prête qu’aux riches ou pas grand-chose. **Alors qu’au Canada, pour 1 dollar investi dès la première année d’existence nous avons reçu 1 dollar sans passer par les conditions lourdes imposées en France.**

Au final, nous avons reçu 250.000 dollars de remboursement de R&D et 50.000 dollars de subvention non remboursable.

Toutes les sociétés innovantes sont ainsi arrosées quand elles ont un bon projet malgré peu de revenus ce qui est nécessairement le cas pendant leur période de R&D. Donc, même

si je suis Français dans l'âme, la French Tech n'arrose pas les bonnes plantes et elle n'a pas su retenir ArmadAI de ce côté de l'Atlantique.

15/ Vous êtes élu président de la République, avec quelle vision emportez-vous les Français ? Et quel profil nommez-vous au poste de DSI de la France ?

Le Général de Gaulle incarnait un esprit de patriotisme, de résistance, d'intégrité et de volonté dans l'adversité et alors qu'il ne représentait rien ou pas grand-chose au départ. C'est l'indignation et le refus de s'avouer vaincu qui l'a conduit à réaliser de grandes choses, notamment sur le plan industriel. Aujourd'hui, c'est l'indignation contre les abus des hyper-puissances, le rejet des compromissions et du Tout Pour Ma Gueule (TMPG) qui devrait emporter les Français vers un modèle fièrement Gaulois, pour le patriotisme, et inspiré par les Lumières pour les valeurs humanistes

Pour ce qui concerne le profil de DSI de la France, je vote pour l'ancien DSI du MINARM et actuel directeur du pôle Cyber de Rennes. Du moins s'il revient sur sa position sur le choix de Microsoft qu'il a pris au MINARM en son temps…

16/ Dans bien des domaines, les Etats-Unis nous tiennent encore la main. Sommes-nous vraiment libres de lâcher la leur ?

Dans mon domaine précis, la gestion des identités et des accès numériques, la réponse est clairement « oui ». Nous sommes différents et nécessairement meilleurs avec notamment la société UserCube parce-qu'adaptés à notre culture.

Nombre de préconisateurs et d'utilisateurs choisissent les USA par atlantisme, mimétisme, facilité, frilosité. Ce ne sont pas les USA qui nous tiennent la main. C'est une partie d'entre nous qui demandent la leur en rejetant des alternatives nationales. **De nombreuses innovations qui réussissent aux USA sont réalisées par des Français que la France n'a pas su**

retenir. Songez au défunt Philippe Courtot, fondateur de Qualys. Une licorne installée à San Francisco. Je pense aussi à Khai Minh Pham, un visionnaire méconnu qui en 2002 proposait EasyPlanet, l'équivalent de ce que propose 20 ans plus tard FaceBook avec Metavers.

iSource et CEGETEL auraient pu financer et lancer des espaces virtuels à la Metavers dès la version 2.0 de l'Internet. Mais Khai Minh est reparti dégouté à San Diego où il a lancé une startup en IA médicale tout aussi visionnaire. Il y a enfin les fondateurs de Business Objects qui ont d'emblée choisi de devenir Américains parce-qu'ils auraient végété en France. Comme tant d'autres… qui reviennent sous un autre drapeau parce-qu'on a rien fait en France pour les retenir.

17/ Le soft power français, est-ce que cela existe ?

Oui.

C'est **la conjonction du coq gaulois pour la volonté de souveraineté et de l'esprit des lumières pour l'humanisme**. On pourrait lui redonner du lustre en tant qu'alternative aux hyper-puissances Américaine, Chinoise et à la Russie. Avec un refus de vassalisation commençant par soi-même. Mais ce soft-power doit être porté par la bonne personne. Et pour l'heure, nous l'attendons comme le Messie des Juifs orthodoxes ou la réincarnation du Général de Gaulle. Elle tarde à venir et le képi du Général prend la poussière.

Qui se soucie du

“panamazonisme” ?

Dans un article publié dans l’Usine Digitale en 2015, le CTO d’Amazon déclarait : “80% des entreprises du CAC 40 utilisent le cloud d’AWS”.

Il serait intéressant de savoir si les 20% de récalcitrants ont, depuis, abjuré ou non. Peut-être est-il encore des moyens de les amener à la lumière, par la force ou la raison ? Voyons, qu’ils admettent donc publiquement “la robustesse et la résilience” du cloud américain ! Ah…Attendez, on nous souffle à l’oreillette qu’AWS a connu une nouvelle panne hier, 16 décembre. De nombreux services ont été affectés, tels que Duo, le service d’authentification à deux facteurs et de sécurité des points de terminaison, et Zoom. Qu’une grosse partie de l’économie mondiale s’appuie désormais sur un seul et même opérateur ne semble émouvoir personne. Cette concentration que l’on pourrait appeler “panamazonisme” constitue une vulnérabilité monumentale pour le monde.

Mais vous allez voir qu’il se trouvera bien chez nous de petits commis de la grosse entreprise pour nous expliquer que tout est sous contrôle. Vous vous souvenez ? PLAY : “Robustesse et résilience”.