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.