La ResNumerique : De la sécurité des systèmes d'information vers un numérique de confiance, il est temps d'agir.

Stéphane MEYNET
Président, CERTitude NUMERIQUE

Bien définir la « chose »

Sécurité numérique, cybersécurité, sécurité des systèmes d'information… autant de termes que nous mélangeons tous allégrement pour désigner au final ce qui tendrait à rendre l'usage de nos moyens numériques le plus robuste possible. Aïe ! Encore des termes ambiguës - moyens numériques et robustes - qui sans définition partagée laissent libre cours à l'imagination et l'interprétation, source de complications et d'échecs.

Pour traiter correctement et sérieusement d'un sujet, il faut d'abord bien le définir et s'assurer que l'on parle tous de la même chose. C'est ce que l'on m'a toujours appris. Et que je n'ai pas toujours mis en application : pourquoi définir ce qui est évident ? Erreur, car le diable se cache souvent dans les détails.

Derrière ce préambule quelque peu provocateur, l'idée est de simplement souligner que cette difficulté de langage, de définition, non résolue à ce jour, cache une réalité très concrète : le champ d'action que confère chacune des appellations citées ci-dessus varie. C'est pourquoi il est important de définir clairement « la chose », l'objet sur lequel nous devons concentrer nos efforts pour construire une politique efficace adaptée aux enjeux d'aujourd'hui en termes de confiance numérique.

Un périmètre qui évolue et se transforme

Si l'on parle de sécurité des systèmes d'information (SSI), l'objet important au final est l'information et donc sa sécurité, quel que soit son support. Ce support, historiquement le papier, devient aujourd'hui majoritairement numérique, à tel point d'ailleurs que l'État s'est fortement engagé dans la dématérialisation pour de nombreux services.

Donc, logiquement, la sécurité des systèmes d'information se transforme en sécurité des systèmes numériques qui, au-delà d'être bientôt le principal support à l'information, recouvre également d'autres systèmes : les systèmes de production de nos usines, les systèmes pilotant nos infrastructures vitales, nos infrastructures sur les territoires… jusqu'à nos équipements médicaux « implantés » chez les patients.

Mais cette transformation vers le numérique met à l'écart une partie du champ d'action historique de la sécurité des systèmes d'information : la sécurité des supports d'information autres que numériques. Et si l'on parle de sécurité de l'information, qui a priori englobe la sécurité des systèmes d'information, le champ s'élargit encore pour traiter d'un tout autre sujet ô combien important et régulièrement mis à « l'honneur » ces derniers temps : celui de la désinformation, des fakenews et de l'influence.

Cette longue introduction montre combien une réflexion de fond sur la clarification et la gouvernance de ces sujets devient aujourd'hui nécessaire.

Laissons de côté le sujet de la sécurité de l'information dans son sens noble et large[1] pour revenir à la sécurité des systèmes numériques voire la sécurité (du) numérique.

Confiance et sécurité numériques : la « ResNumerique »

Tout d'abord, ne perdons pas de vue que la sécurité numérique n'est pas une fin en soi et qu'elle est inutile si elle ne sert pas une « chose » plus large. Petite provocation encore, car nous savons tous que la sécurité numérique est indispensable. Faut-il le rappeler, elle contribue à renforcer la confiance dans nos systèmes numériques essentiels à notre quotidien, à nos métiers, à notre développement, à notre protection… et à notre souveraineté.

En France, la question de la sécurité numérique est traitée au travers d'une organisation spécifique intégrant notamment l'Agence Nationale de la Sécurité des Systèmes d'Information et les ministères disposant chacun d'une chaîne fonctionnelle et opérationnelle dédiée. Elle a fait l'objet d'une réglementation abondante, dont la désormais très célèbre et première du genre Loi de Programmation Militaire 2014-2019 et son article 22 à destination d'une catégorie spécifique d'organisations, à savoir les Opérateurs d'Importance Vitale. Une réglementation qui depuis 2014 n'a cessé de s'enrichir, sous l'impulsion notamment de l'Union Européenne qui s'est saisie pleinement de ce champ depuis la Stratégie de Cybersécurité européenne de 2012.

La France dispose également d'un écosystème fort en matière de sécurité numérique comprenant des acteurs de renommée internationale et de nombreuses start-up, ce qui mérite d'être souligné car insuffisamment mis en valeur par le passé.

Mais qu'en est-il du « simple » numérique indispensable à nos entreprises, nos territoires, nos collectivités et notre souveraineté ? L'écosystème de ce simple numérique, celui des outils numériques, que tous nous employons quotidiennement, est fortement extra-national voire extra-européen. Comment construire alors un numérique de confiance avec, certes, un écosystème fort sur la sécurité numérique mais faible, tout du moins en apparence, sur le numérique, brique pourtant essentielle ? Bien évidemment, la filière sécurité numérique peut renforcer la sécurité de solutions numériques que nous ne maîtrisons pas et assurer la protection, dans le sens de la confidentialité, de l'information. Mais elle est totalement impuissante dès lors qu'il s'agit d'assurer la résilience (encore un terme à définir) des solutions numériques. La disponibilité de nos outils numériques est bien souvent, pour l'utilisateur que nous sommes, plus importante que la confidentialité des données.

Le choix des solutions numériques : un dilemme ?

La crise sanitaire a renforcé notre dépendance au numérique et le besoin de disponibilité des solutions, tout le monde en est désormais convaincu. Le recours aux outils de visioconférence par exemple a été pour beaucoup une bouée de sauvetage, que ce soit dans la sphère professionnelle ou personnelle, et le seul moyen d'assurer la continuité d'activité et le lien social avec nos proches.

[1] Les lecteurs pourront consulter l'étude du Sénat : « désinformation, cyberattaque et cybermalveillance : l'autre guerre du Covid-19 » (avril 2020) qui aborde très concrètement le sujet.

Dans ce contexte, bien évidement particulier, le volet sécurité numérique a clairement été relégué au second plan. Mais finalement ne l'était-il pas déjà auparavant ? Dans le cadre de la transformation numérique de notre société, le recours au numérique relève ni plus ni moins que de la compétitivité des organisations. Face à ce constat et cette nécessité d'évoluer rapidement, la question à résoudre pour beaucoup est en premier lieu celle du choix des outils numériques. Pour faire court, ce choix se résume aux critères suivants : « on veut que ça marche, que ce soit simple à utiliser et que ça ne coûte pas trop ». Et la sécurité ? La réponse est que la sécurité est nécessairement intégrée lorsque l'on choisit des solutions comme celles de Microsoft, Amazon, Google et les autres. En pratique, il faut bien reconnaître que ces entreprises investissent lourdement dans la sécurité numérique, en plus de répondre aux autres critères recherchés par les utilisateurs. Donc pour une PME, une ETI, une association ou une collectivité locale le choix est évident, d'autant plus que les alternatives, lorsqu'elles existent, ne sont pas ou peu connues. Pas de dilemme!

Le devoir de souveraineté numérique

Le Sénat a publié en octobre 2019 un rapport d'information fort intéressant sur le devoir de souveraineté numérique[2]. Ce rapport propose un ensemble de pistes, dont celle de la souveraineté numérique à travers une véritable politique industrielle soutenant le développement des technologies clés. Néanmoins, les besoins numériques, rappelés lors de la crise du Covid-19, ne relèvent pas nécessairement de technologies clés, tout du moins pas dans le sens où on l'entend habituellement dans « la communauté cyber » (IA, big data, blockchain, supercalculateur, 6G par exemple).

Où sont alors les solutions numériques de confiance pour les entreprises, les collectivités, les associations et les particuliers ?

Quels sont les acteurs publics et privés en France qui traitent de la « ResNumérique », cette chose fondamentale pour notre société ? Quels sont les acteurs qui adressent ce marché ?

Un constat d'échec

Le rapport du Sénat souligne un point crucial en rappelant, pour illustrer le propos, l'échec du projet de cloud souverain : « L'État a investi dans deux projets rivaux, CloudWatt et Numergy, au début des années 2010 en choisissant de ne pas inclure OVH, acteur pourtant déjà très développé dans le cloud. Ce projet a été poursuivi par les gouvernements successifs jusqu'à son échec en 2016. Les raisons officielles de cet échec : pas d'adhésion du marché. Au final, Orange a annoncé officiellement la fermeture de CloudWatt en début d'année et l'État, selon la presse aurait perdu 56 millions d'euros dans l'histoire. ». Le chiffre de 150 millions de pertes pour l'État a parfois même été avancé[3].

Une décision politique complexe

Faut-il effectivement pour l'État impulser la création de solutions (sous-entendu souveraines) venant concurrencer celles proposées par les GAFAM qui ont aujourd'hui l'adhésion du marché ?

La réponse des pouvoirs publics actuels tend à renvoyer vers les acteurs privés et leur capacité d'investissement, mais aussi sur les lois du marché.

[2] « le devoir de souveraineté numérique » rapport du Sénat (octobre 2019)

[3] https://www.solutions-numeriques.com/securite/arret-de-cloudwatt-fin-de-partie-pour-le-cloud-souverain-finance-par-letat/

En effet, pourquoi faudrait-il s'acharner à dépenser de l'argent public à hauteur de ce qu'investissent, si toutefois cela est possible, les GAFAM si au final les utilisateurs préfèrent ces solutions ? Nous ne pouvons que partager cette analyse.

Faut-il alors contraindre, par la réglementation, certains utilisateurs à utiliser des solutions alternatives aux GAFAM lorsqu'elles existent ou existeront, et s'affranchir ainsi des lois du marché ?

Sur ce sujet, les États-Unis ont récemment signé un décret présidentiel interdisant l'achat d'équipements fabriqués à l'étranger par les acteurs du réseau de production et de transport d'électricité, secteur d'importance vitale. Voilà qui laisse à réfléchir ! Pour rappel, notre article 22 de la LPM n'impose rien de tel. La « seule » contrainte pour les Opérateurs d'Importance Vitale en termes de choix de solutions concerne les sondes de détection pour laquelle la loi précise que les Opérateurs doivent mettre en œuvre des sondes qualifiées. Si cela limite aujourd'hui le choix (seulement deux sondes qualifiées), cela n'exclut pas pour autant des solutions étrangères à l'avenir.

Faut-il alors être plus contraignant et imposer des solutions nationales ou européennes, à l'image du récent décret américain, et engager une politique industrielle pour construire ou renforcer ces solutions?

Cette question délicate se pose en ce moment même en ce qui concerne le choix des équipements pour la 5G.

Le temps de l'action

Une véritable réflexion doit donc être menée quant à notre politique publique pour un numérique de confiance. Le rapport du Sénat préconise de mener une revue précise de nos avantages et de nos faiblesses dans l'économie numérique. 200 % d'accord !

Il ressortirait peut-être que :

- la France dispose de créateurs de talents qui peinent parfois à réunir des fonds pour développer des solutions numériques utiles et qui contribueraient à repositionner la France sur les rails de la souveraineté numérique ;
- lorsque les start-up développent des solutions innovantes, parfois avec le soutien et des fonds public, elles peinent, pour ne pas dire échouent, à franchir la marche conduisant à l'industrialisation et sont rachetées par des entreprises étrangères (« StartNoUp ») : notre pays ne serait-il qu'un pays de « start » mais « up » pour les autres ?
- le marché numérique pour les PME/TPE et collectivités semble à l'abandon et manque de solutions simples et de confiance (cf. supra) ;
- la France dispose d'un fort écosystème numérique, mais il n'est pas ou peu soutenu et n'est que trop peu visible, surtout pour les petits acteurs ;
- l'éducation nationale, les universités et les organismes de recherche pourraient, voire même devraient, être des lieux de (re)développement de la souveraineté numérique et montrer l'exemple à nos futures générations. La crise COVID-19 a révélé les lacunes dans le domaine du numérique pour certains de ces acteurs : n'y aurait-il pas là une opportunité à saisir ?
- la commande publique est plus souvent un frein qu'une aide pour développer une souveraineté numérique. Ce sujet a été mainte et mainte fois évoqué.
- la normalisation dans le domaine numérique est un secteur insuffisamment investi par la France, alors qu'il permettrait d'appuyer le développement d'une politique pour un numérique de confiance ;

- les territoires, en particulier les Régions, peuvent réunir les conditions favorables pour développer un numérique de confiance. La Région Auvergne-Rhône-Alpes par exemple a lancé le projet de campus numérique, sans oublier d'intégrer le volet sécurité numérique.

Pour résumer, les idées et les énergies ne manquent pas pour développer un numérique de confiance. À nous maintenant et sans tarder « d'agir efficacement ensemble » en commençant peut-être par cette proposition du Sénat en complément d'une réflexion sur notre gouvernance nationale en matière de confiance numérique[4]. De nombreux experts annoncent l'arrivée d'une crise numérique à court terme : ne reproduisons pas, en attendant qu'elle arrive, le slogan « on n'a pas de pétrole mais on a des idées » scandé durant la crise énergétique des années 70.

Il est temps d'avoir de vraies politiques publiques, réalistes et adaptées aux enjeux pour nos organisations et nos territoires sur cette chose qu'est le numérique.

[4] Des propositions comme la création d'un ministère du numérique, d'un ministre d'État ou d'un haut-commissaire en charge du numérique pour renforcer la vocation interministérielle ont été avancées à plusieurs reprises.