Sécurité du numérique : moins d'entropie et plus de stratégie ?

Christian DAVIOT
Président-fondateur de cdstrat
Senior advisor du CyberCercle

Lettre d'un citoyen engagé au (futur) Premier ministre

Monsieur le (futur) Premier ministre,

Ce nouveau quinquennat ouvre cinq années cruciales pour la France en matière de sécurité du numérique.

Aussi permettez-moi de porter à votre attention quelques propositions d'orientations relatives à l'action gouvernementale, son organisation, ses priorités, au rôle des régions et succinctement à l'international. Les administrations vous fourniront les multiples mesures techniques à prendre en parallèle.

Le numérique s'est effacé peu à peu des discours de vos prédécesseurs. Cité neuf fois dans la déclaration de politique générale d'Édouard Philippe en 2017, celui-ci n'évoquera le sujet qu'une fois dans sa déclaration de 2019 pour constater notre retard. Dans ce même exercice, Jean Castex ne cite pas une seule fois le numérique en 2020.

Sans sécurité du numérique pas de numérique, pas de développement économique, pas de transition écologique, pas de compétitivité des entreprises, pas de modernisation de l'État ni de services performants pour nos concitoyens.

La sécurité du numérique n'est pas d'abord une affaire d'ingénieurs ou de techniciens. La sécurité du numérique est d'abord une affaire de politique(s). La responsabilité des élus est majeure en ce domaine. Or, force est de constater - le diagnostic n'est que discrètement partagé - que nous avons ces dernières années régressé au niveau stratégique, désorganisé le modèle français, rendu tout à fait illisible une action essentiellement destinée aux « premiers de cordée » et presque disparu de l'international.

La régression stratégique est à la fois le fait de l'hubris de quelques-uns et d'un manque d'intérêt et de prise de conscience des derniers Premiers ministres - même si quelques réunions de rattrapage ont eu lieu ces six derniers mois qui ont donné lieu à la publication d'un décret[1], merveille bureaucratique qui aura sans doute le même avenir que le RGS.

[1] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045537693

Un peu de chronologie permet de comprendre comment nous en sommes arrivés là.

Le Président de la République avait demandé[2] en juillet 2017 au secrétaire général de la défense et de la sécurité nationale d'élaborer une revue stratégique de cyberdéfense. Ce n'était qu'une partie du sujet large qu'est la cybersécurité, mais il s'adressait alors devant la hiérarchie militaire. En février 2018, le SGDSN publiait une « stratégie nationale de cyberdéfense[3] » qui a voulu traiter de la sécurité du numérique dans son ensemble. Le document, rendu public en la seule présence d'un secrétaire d'État au numérique sur le départ, était certes pédagogique mais peu stratégique. Surtout il a fragilisé l'interministérialité vitale à la cybersécurité en créant quatre « chaînes opérationnelles » confiées à des ministères régaliens, créant ainsi autant de silos. Heureusement ces chaînes n'existent plus aujourd'hui que dans quelques « Powerpoints ».

Dans le texte du SGDSN, Bercy était marginalisé. Cette mise à l'écart a d'ailleurs été souhaitée dès l'origine par les concepteurs de la cybersécurité à la française : pour assurer le développement nécessaire de l'ANSSI en termes d'effectifs et de budget, il fallait éviter à l'agence de passer sous les fourches caudines budgétaires de Bercy. Ainsi, les décisions importantes relatives à l'ANSSI ou à la cybersécurité sont-elles prises depuis 2008 en conseil de défense et de sécurité nationale, qui est le lieu des décisions qui s'imposent à tous sans contestation possible.

Après le départ de Mounir Mahjoubi, Cédric 0 est devenu secrétaire d'État sans tutelle ou cotutelle d'aucune administration, malgré des décrets d'attribution[4] lui confiant de larges missions qu'il ne pouvait donc remplir de manière autonome et efficace.

Avec le plan de relance d'après crise sanitaire, Bruno Lemaire a lancé une OPA à 700 millions d'euros sur le sujet en préparant avec la DGE, sans concertation, une « stratégie d'accélération de la cybersécurité[5] », essentiellement centrée sur les aspects industriels du sujet, une régression par rapport à la stratégie interministérielle présentée par Manuel Valls[6] en 2015. Préfacée par le ministre de l'Économie et des Finances, elle a de justesse été reprise et présentée par le Président de la République en février 2021 [7].

Force est de constater que la mise en œuvre de cette « stratégie » se révèle cacophonique.

Le choix a été fait de subventionner les « premiers de cordée » via des appels à projets, des appels à manifestations d'intérêt dans de multiples domaines, avec des délais souvent très courts[8] ne permettant pas à tous les acteurs de répondre, notamment les moins parisiens. Nulle part n'est disponible une vision d'ensemble de ces initiatives.

[2] https://www.elysee.fr/emmanuel-macron/2017/07/13/discours-d-emmanuel-macron-a-l-hotel-de-brienne

[3] http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

[4] Décrets du 10 avril 2009 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038359072/ et du 14 août 2020 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000042237946/

[5] https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/02/210218_dp_cyber_vfinale.pdf?v=1645019943

[6] https://www.gouvernement.fr/actualite/strategie-nationale-pour-la-securite-du-numerique-un-bon-equilibre-entre-prise-en-compte-de-la-3075
https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/

[7] https://www.elysee.fr/emmanuel-macron/2021/02/18/strategie-nationale-cybersecurite

[8] La palme revient sans doute à l'AMI sur l'identité numérique ouvert sur une période de 14 jours ! https://www.entreprises.gouv.fr/fr/aap/numerique/politique-numerique/appel-manifestation-d-interet-sur-l-identite-numerique

Il aurait été souhaitable de travailler à de vraies politiques publiques coordonnées qui touchent un large éventail d'administrations, d'institutions et de collectivités, d'acteurs économiques ou de particuliers. Soutenir la filière, bien sûr, mais sous réserve que l'ensemble de l'écosystème en soit bénéficiaire au sein d'un plan d'ensemble suivi et dont l'impact doit être contrôlé. Dans le débat depuis 1993, le levier de la commande publique en faveur des PME-PMI, souvent les plus innovantes, pourrait enfin y être intégré.

Même embarras sur la coordination. Il y a désormais deux coordinateurs de la cybersécurité nationale dans deux de vos (futurs) services : le directeur général de l'ANSSI, acteur historique de la cybersécurité, et le coordinateur national de la stratégie cybersécurité au SGPI. Devant cet embrouillamini, l'ANSSI semble avoir renoncé à la conduite d'une stratégie nationale et à sa mission interministérielle pour se concentrer sur ses capacités opérationnelles, un domaine d'excellence de l'agence. Quant à la DGE de Bercy, elle ne donne manifestement pas les moyens de remplir pleinement sa mission au coordinateur du SGPI.

Les deux derniers secrétaires d'État au numérique ont décidé d'arrêter la politique : peut-être la manière dont leurs sujets ont été traités n'est-elle pas étrangère à cette décision…

Un signe politique doit être donné à tout l'écosystème.

Plutôt qu'un secrétaire d'État, il serait aujourd'hui plus efficient de nommer un ministre délégué chargé du numérique afin qu'il participe aux conseils des ministres concernés, qui vous serait directement rattaché pour être en mesure d'agir à l'interministériel, et doté d'un décret d'attribution qui lui donne autorité et moyens.

Le choix est vaste. Nombre de parlementaires s'intéressent à la cybersécurité et ont travaillé sur ce sujet.

Deux critères peuvent aider au choix du (ou de la) ministre délégué(e) qui devra :

- d'une part, avoir la capacité à différencier cybersécurité (attention portée aux attaques informatiques) et sécurité de l'information (attention portée à la propagande, aux fausses nouvelles) : ce ne sont ni les mêmes métiers ni les mêmes acteurs. D'ailleurs depuis 2009, dans les instances internationales, la France reproche ce mélange des genres à la Russie comme à la Chine. Il est vrai que, dans la perspective de la campagne électorale officielle, le SGDSN a donné le mauvais exemple en envoyant aux médias fin mars une lettre[9] signée par le directeur général de l'ANSSI qui évoque à la fois la partie cyberattaque (mission de l'ANSSI) et la partie influence (mission de VIGINUM). Une attaque informatique peut permettre d'identifier des éléments utiles à une campagne d'influence : il aurait donc été logique que le SGDSN, auquel est rattaché VIGINUM, endossât cette lettre plutôt que l'ANSSI, dont la mission n'est pas le contrôle politique des réseaux ;

- d'autre part, éviter la fascination pour les capacités sans limite des technologies, quelles que soient les atteintes portées aux libertés ou à la vie privée. L'acceptabilité par les citoyens est un facteur clef pour l'utilisation des technologies en matière de sécurité et l'équilibre délicat libertés publiques-performances sécuritaires est ici un enjeu démocratique fondamental.

Voilà pour l'échelon politique.

[9] Réf : 758/ANSSI/DIR/NP du 24 mars 2022.

Vous devrez également veiller aux nominations à la tête des administrations qui traitent du numérique et de sa sécurité.

Le désintérêt d'Édouard Philippe et surtout de son dircab pour le numérique avait entraîné le renvoi dos à dos du secrétaire d'État et du directeur interministériel du numérique et du système d'information de l'État (DINUM) qui avait pourtant engagé une dynamique très innovante de transition numérique de l'État. La DINUM s'est effondrée en perdant nombre de ses talents après le choix, pour le remplacer, d'un dirigeant pour le moins controversé.

Récemment, le directeur général de l'ANSSI a annoncé son départ de l'agence. Le secteur privé sera évidemment ravi de l'accueillir, mais il y aurait sans doute d'autres missions à lui confier au sein de l'État. Accompagner le ministre délégué par un Haut-commissaire dédié au travail avec les administrations est certainement une option. Il pourrait par exemple étudier le moyen d'attirer, de rémunérer au bon niveau et de garder les ressources humaines les plus performantes et les plus utiles pour accomplir les missions défensives et offensives. Dans certaines administrations sensibles, le turnover est en effet dangereusement élevé. Favoriser la mobilité des effectifs entre les différentes fonctions publiques serait également déterminant.

Plus largement, les ressources humaines sont critiques pour garantir la cybersécurité du pays.

L'apprentissage du code au collège ne suffira pas. Donner les clefs de compréhension du numérique et éduquer les citoyens dès le plus jeune âge aux usages sécurisés du numérique est devenue une urgence – comme l'avait d'ailleurs identifié la Stratégie nationale pour la sécurité du numérique de 2015. Vous pourriez vous inspirer d'Israël dans l'identification des jeunes talents. De plus, le numérique comme la cybersécurité ne se limite pas au code informatique. Toutes les disciplines, notamment le droit et les relations internationales, y concourent.

J'en viens à quelques priorités qui pourraient animer votre action.

D'abord, la mise en évidence à l'occasion de la crise sanitaire de l'importance d'une vraie souveraineté qui permet de gérer les dépendances, au-delà des discours simplificateurs.

Ainsi faut-il tirer les enseignements de l'échec français et européen en matière d'informatique en nuage. Après le fiasco Cloudwatt et Numergy - quel autre État aurait eu l'idée de créer deux concurrents pour ne pas froisser la Commission européenne ? -, nous nous sommes mis en situation de dépendance à long terme vis-à-vis des acteurs américains sans avoir laissé une chance aux PME françaises du domaine. Après leur entrisme dans Gaia-X, les leaders américains du cloud ont piégé les grands acteurs français dans un scénario connu : dépendance aux licences dont le coût augmentera, version n-1 des technologies et rachat lorsque les acteurs français étranglés auront acquis les parts de marché.

Ensuite, le constat qu'il n'y a pas de perspective d'émergence d'acteurs français de niveau mondial à courir après des technologies numériques développées par d'autres. D'une part, parce que dans ce domaine, le premier arrivé prend instantanément une part conséquente du marché, mais également parce que l'effort de rattrapage est généralement hors de portée - voir la mésaventure d'un moteur de recherche « français ». La lecture de la dernière livraison du tableau de bord de la

recherche[10] élaboré par la Commission européenne est explicite. Deux exemples : aux États-Unis, les cinq budgets annuels de recherche les plus importants sont investis par des entreprises du numérique (de 10 à 20 milliards de $) ; dans le classement européen, la première entreprise du numérique n'arrive qu'en 8ème position (4 milliards d'€) ; Alphabet, Huawei, Microsoft investissent chacun en recherche environ 20 milliards de $ chaque année !

Nous sommes d'un point de vue industriel vis-à-vis du numérique comme était la France en 1945 vis-à-vis de l'atome. Il suffit de lire, pour s'en convaincre, l'ordonnance de création du CEA[11]. Plutôt que de tenter de rattraper notre retard sur des technologies existantes, inventons les technologies et les services de demain, pour le numérique et sa sécurité. Nous avons les chercheurs, les ingénieurs, les entrepreneurs nécessaires. Le fait que l'entreprise qui a déposé le plus de demandes de brevets en 2021[12] en Europe soit Huawei n'est pas une fatalité. Une dynamique a été initiée au sein du Campus Cyber qui rassemble des ressources publiques et privées. Pourrait-être étudiée l'opportunité de créer un Commissariat au numérique [13] qui rassemblerait les forces de recherche publiques de l'ensemble du territoire national et les communautés du logiciel libre. Une des premières missions de ce commissariat - virtuel dans un premier temps pour contourner les obstacles administratifs -, consisterait à établir la cartographie de la recherche nationale dont nous ne disposons que partiellement aujourd'hui. C'est un des effets délétères de la logique de guichets, d'appels à projets ou à manifestation d'intérêt : la méconnaissance du tissu national.
Un think tank dédié au numérique, d'ailleurs prévu par la revue stratégique du SGDSN en 2018, pourrait accompagner cette création.

J'en viens à l'articulation entre ce qui relève des administrations centrales et ce qui devrait être délégué.

C'est une des leçons que nous devons tirer de la gestion de la crise sanitaire : lorsque les régions ont été impliquées dans la lutte contre la COVID-19, tout est devenu plus efficace. Ainsi des vaccinations plus nombreuses grâce à la création de « vaccinodromes » au plus près des citoyens. Il nous faut envisager une crise virale informatique et la possibilité que nombre de particuliers, d'acteurs économiques, de collectivités territoriales et d'administrations soient infectés, par exemple par un rançongiciel. Nos modes d'action devraient également être décentralisés pour être plus efficaces.

En 2015, le Premier ministre a annoncé la création d'un GIP qui accompagnerait dans la sensibilisation et le traitement des attaques informatiques les publics que l'ANSSI ne pouvait assister directement. Maladroitement baptisé « Cybermalveillance. gouv.fr » par le SIG - encore un de vos (futurs) services -, suggérant que l'État crée une plate-forme de cybercriminalité, le GIP ACYMA est constitué début 2017 et rassemble des représentants de l'État, des utilisateurs, des prestataires et des offreurs de solutions et de services. Il a créé une plate-forme de sensibilisation et d'assistance aux victimes d'actes de cybermalveillance en leur proposant une assistance de proximité construite sur l'adhésion à

[10] The 2021 EU industrial R&D investment scoreboard https://iri.jrc.ec.europa.eu/sites/default/files/contentype/scoreboard/2021-12/EU%20RD%20Scoreboard%202021%20FINAL%20online.pdf

[11] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000521964/

[12] https://www.epo.org/news-events/news/2022/20220405_fr.html

[13] Je sais que cette proposition avait été portée sans succès au cabinet de Lionel Jospin alors Premier ministre.

une charte de prestataires informatiques répartis sur tout le territoire national.

Dans le cadre du Plan de relance, l'ANSSI, qui bénéficie d'une enveloppe de 136 Millions d'euros, écrit aux présidentes et présidents de régions, quelques jours avant les élections régionales (!), pour leur proposer de créer un CSIRT, « *un centre de réponse aux incidents cyber au profit des entités implantées sur le territoire régional* », destiné à traiter « *les demandes d'assistance des acteurs de taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations) et les [mettre] en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires*[14]». L'agence s'engage à subventionner les régions volontaires pendant trois ans, à charge de ces régions d'inventer le modèle économique susceptible de prolonger la vie du CSIRT. Outre le fait que seules sont aidées les régions candidates, que le financement n'est assuré que pour trois ans, ce dispositif, lorsqu'il sera opérationnel, fera doublon avec celui créé en 2017.

Ce n'était apparemment pas suffisamment entropique. En janvier dernier, a ainsi été annoncée la « *mise en place d'un équivalent numérique de « l'appel 17 » afin que chaque citoyen puisse signaler en direct une attaque cyber et être mis immédiatement en relation avec un opérateur spécialisé*[15] ».

Il est difficile de proposer une action publique plus illisible et moins économe de l'argent des Françaises et des Français ! Là encore une action d'ensemble, coordonnée et lisible par tous, s'impose.

Plus largement, nous devons mieux impliquer nos régions - toutes nos régions - dans ce domaine de la cybersécurité, notamment au nom de leur mission de développement économique. En s'appuyant sur Cybermalveillance.gouv.fr et les préfectures, elles sont le bon niveau administratif pour mettre en place les politiques qui prennent en compte les caractéristiques humaines, industrielles et universitaires de leur territoire. Elles ont également la clé de notre résilience. Ce sont elles qui devront faire face demain aux conséquences en termes de sécurité du développement des villes et territoires « intelligents » dont l'État ne se préoccupe pas aujourd'hui malgré les concrétisations rapides de ces projets - voir le dispositif ONDIJON porté par la Métropole de Dijon.

Pour conclure cette lettre trop longue, quelques mots sur l'Europe et l'international qui mériteraient également un développement important.

La guerre en Ukraine a obéré la visibilité de la présidence française du Conseil de l'Union européenne dans d'autres domaines que celui de la diplomatie. Or les initiatives en matière de cybersécurité et de numérique sont désormais davantage portées par la Commission que par la France. L'action à mener dans les années à venir devrait également porter sur la redéfinition des aides publiques au niveau européen pour que soit soutenue une véritable politique industrielle, à l'image de ce que font les États-Unis ou la Chine.

À l'international, a été lancé en 2018 « l'Appel de Paris [16] » issu d'une conférence internationale organisée par l'ANSSI à l'UNESCO en 2017. Les diplomates ont réussi à faire signer ce début d'engagement au respect de certaines règles à plus de 80 États, dont les États-Unis, 700 acteurs

[14] https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/programme-dincubation-de-csirt/

[15] https://www.elysee.fr/emmanuel-macron/2022/01/10/deplacement-du-president-de-la-republique-a-nice

[16] https://pariscall.international/fr/

économiques et près de 400 ONG. Mais, en cinq ans, seuls des groupes de travail ont été créés, et encore, début 2021 seulement. La France dispose avec cet appel d'un instrument qui peut pacifier le cyberespace, à un moment de l'Histoire où tout est possible et où une attaque informatique serait susceptible de conduire à la mort de vastes populations, à la destruction d'infrastructures vitales, à l'arrêt d'économies entières. Il y a quelques années, le chef du Conseil de sécurité russe, Nikolaï Patrouchev, avait indiqué au secrétaire général de la défense et de la sécurité nationale que tant qu'il n'y aurait pas de traité international encadrant et limitant l'action offensive des États dans le cyberespace, la Russie ne s'interdirait rien. Il est temps d'agir aussi pour redynamiser les actions dans le cadre de l'Appel de Paris.

L'OCDE, avec l'animation active de l'ANSSI, a réalisé un travail de fond sur les vulnérabilités logicielles[17], qui a fait consensus parmi ses 38 pays membres. Nous avons la chance d'avoir parmi les entreprises françaises des championnes de ce sujet qui, bien mené, par exemple en abordant la question du marché gris, peut avoir un impact significatif sur la cybersécurité mondiale et ainsi renforcer la place de la France.

Vous le voyez, la cybersécurité recouvre des sujets bien plus larges que « seulement » techniques ».

Elle est aujourd'hui un pilier de nos sociétés dans lesquelles s'accélère la fusion entre le numérique et l'activité humaine - et demain le corps humain. Dans ses aspects défensif et offensifs, la cybersécurité est un enjeu majeur pour notre développement économique, social, pour notre sécurité globale, pour notre place sur la scène internationale.

Monsieur le (futur) Premier ministre, votre fonction vous oblige.

[17] https://www.oecd.org/fr/numerique/ieconomie/securite-numerique/