Dérive du modèle français de cybersécurité : origines, conséquences, remèdes

Christian DAVIOT

Ancien conseiller stratégie du directeur général de l'ANSSI

Introduction

L'analyse froide et désincarnée des textes administratifs qui étayent le modèle français de cybersécurité viendra en son temps, dans des manuels qui tomberont de la main des lecteurs tant l'amphigouri de certains de ces textes reflète peu les circonstances exceptionnelles et les débats passionnés qui les ont générés. Il est vrai que ces textes n'ont été pas rédigés pour rappeler une évidence : les gouvernements, administrations, parlements, entreprises et organisations non gouvernementales français et étrangers qui ont contribué directement ou indirectement à imaginer, développer et… fragiliser la cybersécurité française sont animés par des êtres humains aux cultures, niveaux de compréhensions, visions, motivations professionnelles ou personnelles pour le moins diverses.

La responsabilité de la dérive est collective. 2020 est probablement une année charnière pour le modèle français de cybersécurité. Il semble donc utile de rappeler succinctement ce qui en a fait la force, en fait la faiblesse aujourd'hui et les conséquences qu'engendrerait une dérive trop prononcée de ce modèle. Et de proposer quelques pistes.

2007 – 2017 : la construction

Si aucune allusion n'y est faite dans la lettre de mission[1] confiée en août 2007 à un ancien secrétaire général de la défense nationale, l'attaque informatique subie par l'Estonie quelques mois plus tôt est dans les esprits et dans les débats des membres de la commission de préparation du Livre blanc sur la défense et la sécurité nationale.

Préfacé - donc endossé - par le Président de la République et publié en juin 2008, le Livre blanc[2] institue un « Conseil de défense et de sécurité nationale », annonce la mise en place d'une capacité de lutte informatique offensive et la création d'une agence chargée de la sécurité des systèmes d'information relevant du Premier ministre et de la tutelle de ce qui devient le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN).

Les fondamentaux du modèle français de cybersécurité sont ainsi posés. La sécurité des systèmes d'information est un sujet interministériel, les capacités offensives relèvent quant à elles du ministère de la défense. Ce choix contraste avec ceux des états alors les plus actifs dans le domaine, qui ont confié défensif et offensif à leurs services de renseignement.

---

[1] http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/Lettre_mission_JCMallet.pdf

[2] http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html

Durant les mois qui suivent la publication du Livre blanc, la combinaison parfaite du Secrétaire général de la défense et de la sécurité nationale - conseiller d'État - et d'un de ses conseillers - X-télécoms - pour appréhender le sujet avec la hauteur de vue nécessaire et la compréhension technique indispensable, permet la préfiguration de la future agence sur la base d'une des directions du SGDSN. L'Agence Nationale de la Sécurité des Systèmes d'Information, l'ANSSI, naît le 7 juillet 2009. Le décret[3] de création de l'agence la rattache au Secrétaire général de la défense et de la sécurité nationale et n'en fait pas une simple direction du SGDSN. Il l'installe comme service à compétence nationale - elle peut intervenir sur l'ensemble du territoire -, et comme « autorité nationale en matière de sécurité des systèmes d'information » chargée de multiples missions dont celle de coordonner les travaux interministériels dans son champ de compétence. L'agence compte alors moins d'une centaine de personnes, essentiellement des ingénieurs civils et des militaires.

Le Parlement vient alors de voter la loi « Création et Internet » qui envisage l'installation d'un mouchard[4] sur les ordinateurs soupçonnés de télécharger illégalement, via internet, des œuvres protégées. Cette mesure technique, faille de sécurité potentielle, a bien été identifiée par les promoteurs de l'agence qui ont choisi de ne pas intervenir auprès des cabinets ministériels lors de l'élaboration du projet de loi ou auprès des députés au cours des débats parlementaires : trop d'incompréhension technique des sujets.

Dès l'automne 2009, l'ANSSI entame l'élaboration d'une stratégie. Adoptée début 2010 par le comité stratégique de la sécurité des systèmes d'information prévu par le décret de création de l'agence, la stratégie de la France en matière de défense et sécurité des systèmes d'information répertorie une quarantaine d'actions regroupées en quatre objectifs et sept axes de travail. Elle sera le seul leg du comité, organe à caractère consultatif qui ne trouvera pas son équilibre de fonctionnement, notamment en raison de la présence intermittente d'intervenants de la direction de la modernisation de l'État alors attachée à Bercy. Le comité sera supprimé en 2015.

La stratégie, dont la version publique[5] ne sera publiée qu'en mai 2011 adopte une terminologie simple : la cybersécurité, état recherché, fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Fin 2010, l'ANSSI identifie une attaque informatique à des fins d'espionnage menée contre Bercy. Les informations recherchées et régulièrement collectées par l'attaquant ne laissent guère de doute quant à son origine géographique. À cette occasion, l'agence élabore une méthodologie de traitement des attaques informatiques. Associée au développement de capacités de détection des attaques informatiques initié simultanément, cette méthodologie en constante évolution depuis cette date permet aux experts de la « sous-direction opérations » de l'agence d'être sans conteste parmi les meilleurs au monde en matière de traitement de crise informatique.

Un incident significatif interviendra durant les trois mois que prendra le traitement de l'attaque : un des experts de l'ANSSI constate que l'attaquant est en ligne et qu'il est en mesure d'accéder à sa machine, ce qui permettrait vraisemblablement de l'identifier. L'officier de police judiciaire qui accompagne l'ANSSI le lui interdit au motif que cela constituerait une atteinte à un système de traitement automatisé de données relevant du code pénal… Cet incident sera le

[3] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212&categorieLien=id

[4] Cf. article 5 de la LOI n° 2009-669 du 12 juin 2009. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id

[5] https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

début d'une réflexion de l'agence sur l'aménagement du droit national, afin de permettre une réponse proportionnée aux attaques subies.

L'attaque informatique contre Bercy, que le ministère a bien voulu rendre publique à des fins pédagogiques, est l'occasion pour l'ANSSI d'élaborer une série de mesures destinées à renforcer la sécurité des systèmes d'information des administrations et, grâce au soutien sans faille des cabinets militaires du Président de la République et du Premier ministre, de les proposer à l'arbitrage, accompagnées d'un plan de développement de l'agence. Mesures et plan sont présentés lors d'un conseil des ministres[6] en mai 2011.

Juillet 2012. Les attaques contre les systèmes d'information, d'origine étatiques ou non, appartiennent aux sujets d'étude que le Président de la République souhaite voir étudiés dans la lettre de mission[7] adressée au conseiller-maître de la Cour des comptes juste revenu de sa mission à l'ONU, en vue de l'élaboration d'un nouveau Livre blanc.

Identifiant l'opportunité offerte par les travaux pour l'élaboration du Livre blanc, le directeur général de l'ANSSI, qui a constaté que les entreprises comme les administrations peinent à intégrer dans leurs priorités la sécurité de leurs systèmes d'information, décide d'utiliser la loi pour contraindre les plus sensibles d'entre elles à mettre en œuvre les politiques nécessaires. L'ANSSI participera donc très activement aux travaux de la commission du Livre blanc, notamment par une solide contribution écrite en lien avec les ministères de la Défense et de l'Intérieur et communiquée à chaque membre de la commission.

Parallèlement, pour prévenir une action de lobbying contre son projet, le directeur général ira au-devant les grandes entreprises et de leurs associations représentatives afin de leur expliquer les raisons du recours à la réglementation.

La question se pose alors de l'établissement de la liste des entreprises qui seront visées par la loi. Pour éviter tout obstacle européen, le choix est fait de retenir la liste des entreprises appartenant aux secteurs d'activité d'importance vitale, déjà visés par une réglementation acceptée par Bruxelles. Un choix imparfait, notamment parce que la liste est protégée par le secret de la défense nationale - et qu'il est difficile de mobiliser des personnels lorsqu'on ne peut pas leur en expliquer les raisons - et que la réglementation est alourdie par des textes anciens peu adaptés au développement du numérique.

Les propositions de l'ANSSI seront retenues et insérées dans le Livre blanc[8] rendu public en avril 2013.

En référence à l'incident intervenu pendant le traitement de l'attaque informatique contre Bercy, l'ANSSI proposera une disposition législative supplémentaire permettant d'accéder au système d'information d'un attaquant dans certaines conditions, afin de caractériser l'attaque et d'en neutraliser les effets (pas les causes…). Les articles 21 à 25[9] de la loi de programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale seront votés à l'unanimité sur la base de l'étude d'impact rédigée par l'ANSSI.

Deux points sont à noter concernant cette législation[10] :

- Portée par l'ANSSI au niveau européen, elle servira de base à la future directive européenne

[6] http://archives.gouvernement.fr/fillon_version2/gouvernement/la-politique-de-securite-des-systemes-d-information.html

[7] http://www.livreblancdefenseetsecurite.gouv.fr/pdf/2012-07-13-lettre-de-mission-pr-livre-blanc.pdf

[8] https://www.vie-publique.fr/rapport/33131-livre-blanc-sur-la-defense-et-la-securite-nationale-2013

[9] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id#JORFSCTA000028338829

[10] Des années de travail seront nécessaires aux agents de l'ANSSI pour la mise en œuvre de ces dispositions législatives, en collaboration et transparence avec les opérateurs.

« *Network and Information System Security (NIS)* » qui sera adopté en 2016.

- L'article 22 de la loi impose pour certains systèmes l'utilisation de sondes de détection d'attaques informatiques maîtrisées[11], exploitées sur le territoire national par des personnes habilitées. Cette disposition, très contraignante, sera difficile à mettre en œuvre. Il aura d'abord fallu convaincre les industriels français de développer un produit, éventuellement associé à un service, pour un marché national réduit. Les spécificités techniques et fonctionnelles souhaitées étaient également un obstacle qu'un grand industriel a renoncé à franchir. Au final, une startup a, la première, relevé ce défi, suivie par l'autre grand industriel du secteur.

En cette même année 2013, la révélation de documents issus des services de renseignement américains et des révélations relatives à des attaques informatiques spectaculaires (Stuxnet, Shamoon) montrent que des états pratiquent non seulement l'espionnage de manière massive - l'espionnage n'est pas interdit en droit international, excepté lorsqu'il vise certaines pratiques diplomatiques - mais aussi le sabotage via les réseaux informatiques, par l'insertion dans les réseaux de bombes logiques appelés « implants » dans le jargon.

Prenant en compte la progression du numérique dans tous les secteurs de la société, les nouveaux usages et l'évolution de l'environnement international, le nouveau directeur général de l'ANSSI décide à l'été 2014 d'engager une démarche interministérielle destinée à élaborer une stratégie nationale. Un séminaire de lancement a lieu en présence de toutes les administrations concernées et de Corinne ERHEL, députée des Côtes-d'Armor, auteur, avec Laure DE LA RAUDIÈRE, députée d'Eure-et-Loir, d'un rapport sur le développement numérique de l'économie française. Des groupes de travail sont constitués, pilotés par différents ministères. Après plusieurs mois de travail, les conclusions des groupes de travail sont entérinées lors d'un séminaire de conclusion réuni autour d'Axelle LEMAIRE, Secrétaire d'État chargée du Numérique qui soutient activement la démarche et avec le cabinet de laquelle l'ANSSI a des réunions très régulières.

La stratégie nationale pour la sécurité du numérique[12] est présentée en octobre 2015 par le Premier ministre[13] et Axelle LEMAIRE devant 800 personnes réunies à Paris.

En 2016, les Etats-Unis veulent généraliser le *hack back* qui permettrait à une entreprise de répondre à une attaque informatique par une attaque informatique. Ce principe correspond à la stratégie de cybersécurité des Etats-Unis[14] fondée, comme plus largement le modèle de sécurité américain, sur la domination technologique et l'emploi de la force. Or, un tel principe est une aberration technique : l'attaquant informatique apparent n'est pas nécessairement l'attaquant réel. Mis en œuvre, le *hack back* serait un danger majeur pour le modèle français de cybersécurité, empêchant de fait l'ANSSI de remplir sa mission et serait un risque pour la survie même du numérique.

Face au lobbying américain sur ce sujet via des *think tanks* qui font la tournée des gouvernements européens, l'ANSSI convainc le SGDSN d'organiser une conférence internationale destinée à amener spécialistes du droit international, entreprises et gouvernements à se prononcer contre des actions

[11] Pour détecter une attaque informatique menée par les Martiens, il ne faut pas utiliser des équipements vendus par les Martiens…

[12] https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/

[13] https://www.gouvernement.fr/strategie-nationale-pour-la-securite-du-numerique-un-bon-equilibre-entre-prise-en-compte-de-la-3075

[14] Cf. https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/ https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

offensives dans le numérique en temps de paix[15]. D'abord pensée en petit comité à la demande du Secrétaire Général, l'organisation de la conférence s'effectue ensuite sur une base plus large, associant le ministère des Affaires étrangères et celui de la Défense. Appuyée par une étude réalisée par des professeurs de droit international [16] de l'Université Grenoble-Alpes, « Construire la paix et la sécurité internationales de la société numérique[17] » cette conférence a lieu début avril 2017 à l'UNESCO. Elle réunit des représentants de gouvernements, d'entreprises, d'ONG et des universitaires des cinq continents. Cette conférence sera également l'occasion d'un premier contact entre l'ANSSI et son homologue de la Cyberspace administration of China.

Le consensus sera général parmi les participants pour repousser le principe du hack back systématique.

Sauf rebond à venir, cette conférence aura constitué le climax du modèle français de cybersécurité.

2018 : la dérive

Début 2017, une « note blanche » est élaborée afin de nourrir les débats sur le numérique dans le cadre de la campagne des élections présidentielles. Elle met en avant les trois leviers pour le numérique et la cybersécurité que sont l'identité numérique de niveau élevé (au sens eIDAS), les villes et territoires intelligents, la 5G.

Mai 2017. Tout juste élu, le Président de la République évoque[18] la cybersécurité avec un scientifique candidat aux législatives. La réponse du Président est éclairante : il considère que la France est en retard. Ses modèles sont israéliens et états-uniens, mais il estime qu'il faut désenclaver la cybersécurité du seul domaine militaire et que ce sujet a une dimension européenne. Il évoque la nécessité de renforcer le partenariat franco-allemand sur ce thème. Le Président termine en ajoutant qu'il compte donner les moyens budgétaires nécessaires au développement de la cybersécurité en les incluant dans les 2 % du budget qu'il souhaite voir attribué à la Défense.

À cette date, le Président ne connaît donc pas l'organisation française en matière de cybersécurité. Il ignore également que le modèle français, essentiellement civil, a servi de base à la réflexion et à l'organisation européenne ou que le partenariat avec le Royaume-Uni est particulièrement riche.

Quelques semaines plus tard, dans un discours[19] à l'Hôtel de Brienne qui restera dans les mémoires pour d'autres raisons, le Président de la République demande à la ministre des Armées d'engager une revue stratégique de défense et de sécurité nationale en amont d'une future loi de programmation militaire. En osmose avec les textes et la pratique, il rappelle ensuite que « *des opérateurs des armées contribuent, sous la coordination générale du Premier ministre et en soutien de l'ANSSI, à la détection et à l'attribution des attaques et donc à la cybersécurité nationale* », et demande au Premier ministre l'élaboration d'une revue stratégique de la cyberdéfense. L'échéance de ces deux revues est fixée à la fin de l'année.

Le député européen mandaté par la ministre des Armées pour présider le comité de rédaction remet la revue stratégique de défense et de sécurité nationale courant décembre.

En parallèle, le Secrétaire Général de la Défense et de la Sécurité Nationale qui s'est vu confié la revue stratégique de cyberdéfense a engagé des travaux interministériels auxquels les administrations

[15] L'espionnage, qui n'est pris en compte dans le droit international que dans des circonstances particulières n'est pas comprise dans ces pratiques offensives.

[16] "Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés" Karine BANNELIER, Théodore CHRISTAKIS, 2017 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2957795

[17] http://www.sgdsn.gouv.fr/evenement/conference-internationale-je-suis-internet/

[18] https://www.sciencesetavenir.fr/politique/video-quand-cedric-villani-et-emmanuel-macron-parlent-de-science-pour-sciences-et-avenir_112884

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

contribuent abondamment. Devant la qualité de la revue stratégie de défense et de sécurité nationale qui prend parfaitement en compte les enjeux de souveraineté numérique, consigne est glissée d'élaborer un document plus volumineux et foisonnant. Rapporteur et administrations sont finalement court-circuités au profit d'un exercice qui aboutira à une revue stratégique de cyberdéfense[20] dont le principal mérite est être pédagogique pour le néophyte quant à l'analyse de la menace.

Il faudra revenir plus longuement sur ce document qui sera publié par l'ex-secrétaire général après son départ sous le titre de « Stratégie nationale de cyberdéfense[21] ».

Point nodale du texte, quatre chaînes opérationnelles sont mises en place. Une chaîne « protection » confiée à l'ANSSI, une chaîne « action militaire » qui relève du ministère des Armées, une chaîne « renseignement » menée par les services et une chaîne « investigation judiciaire » suivie par les ministres de l'Intérieur et de la Justice. Une comitologie est également instaurée qui entérine le fait que les grandes décisions concernant la cybersécurité sont prises en conseil de défense et de sécurité nationale.

Si le processus décisionnel est formalisé, la création de quatre chaînes opérationnelles signe la fin de la singularité du modèle français de cybersécurité par l'éclatement des responsabilités et le déséquilibre des arbitrages pour la défense et contre l'économie.

2020 : le déclin ou le rebond

S'il faut rester optimiste par nécessité, les discours donnés et les actes engagés depuis trois ans sont contradictoires et finalement peu rassurants. À l'issue d'une période où l'activité de la France ne s'est pas tout à fait arrêtée grâce au numérique, constats et réflexions sur le modèle français de cybersécurité sont tenus par la prise en compte du numérique dans son ensemble.

Faire du modèle français de cybersécurité un avantage concurrentiel[22] pour la France est une responsabilité collective. L'action du gouvernement est évidemment clé, comme l'est l'audace des administrations, comme le sont les choix des entreprises, l'analyse transverse du Parlement, la stimulation apportée par les ONG. Mais c'est en premier lieu de vertus dont nous devons faire preuve. D'humilité, de volonté et de courage.

L'humilité, comme point de départ.

Il nous faut reconnaître que nous ne donnons pas au numérique la priorité qu'il mérite. Norbert WIENER avait anticipé la capacité du numérique à absorber le reste du monde. « *La sociologie et l'anthropologie sont avant tout des sciences de la communication, et relèvent en tant que telles de la cybernétique en général. Cette branche particulière de la sociologie qu'est l'économie, qui s'en distingue en ce qu'elle possède de meilleures mesures numériques de ses valeurs que le reste de la sociologie, est une branche de la cybernétique en vertu du caractère cybernétique de la sociologie elle-même. »,* écrivait l'inventeur de la cybernétique, en 1956[23] ! Du quotidien des PME à celui des états, de la conduite de la guerre à la transition écologique, des échanges familiaux aux délires transhumanistes, rien ne peut s'envisager désormais sans le numérique et sa cohorte de sujets liés. Pas de retour en arrière possible.

Or, il faut remonter jusqu'au siècle dernier pour trouver un ministre en charge du seul portefeuille du numérique[24]. Si le secrétaire d'État en charge du

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

[21] https://www.economica.fr/livre-strategie-nationale-de-la-cyberdefense-sgdsn,fr,4,9782717869941.cfm

[22] Michael PORTER, "L'Avantage concurrentiel des nations", Dunod, 1993

[23] N. WIENER, I Am a Mathematician, Cambridge (Ma), MIT Press, 1956, p. 327.

[24] François FILLON, ministre des Technologies de l'information et de La Poste dans le premier gouvernement d'Alain JUPPE en 1995.

numérique dans le premier gouvernement de ce quinquennat était placé auprès du Premier ministre - comme la cybersécurité, le numérique est interministériel par nature - il était vingt-deuxième et dernier dans l'ordre protocolaire. Son successeur, exilé à Bercy, se retrouve trente-et-unième sur trente-cinq et a perdu l'autorité sur la direction interministérielle du numérique. Aujourd'hui, le secrétaire d'État chargé de la transition numérique et des communications électroniques, partagé entre Bercy et la cohésion des territoires, est trente-huitième sur quarante-deux membres du gouvernement. Sans importance réelle pour le grand public, ordre protocolaire et décrets d'attribution sont regardés de près par les administrations qui jugent ainsi de l'importance du sujet aux yeux du Président de la République - leur seule référence utile.

Pour les administrations et les entreprises, elles aussi attentives, le numérique n'est donc pas une priorité du gouvernement. Ce sujet a d'ailleurs été le grand absent des discours de politique générale des deux Premiers ministres du quinquennat. Dans ces conditions, comment s'étonner que la France ne soit que dans la moyenne des pays européens en matière de numérique[25] et, à vrai dire, en retard par rapport aux pays avec lesquels elle prétend se mesurer ?

Il nous faut reconnaître que nous devons à nos choix successifs la situation délicate dans laquelle se trouve notre pays. « *Nos vrais ennemis sont en nous-mêmes* »[26]. Dans les années 1990, celles de la fin de l'Histoire et du capitalisme mondialisé triomphant, les énarques de Bercy se gaussent des travaux[27] du rapporteur général du budget au Sénat qui prophétise que les délocalisations des usines vers les pays à bas coût de main d'œuvre entraineront le départ des laboratoires de recherche et à terme une perte de souveraineté. Au tournant des années 2000 c'est un ingénieur diplômé d'une grande école française, aux commandes d'un équipementier français d'envergure mondiale des télécoms qui eut cette idée folle d'imaginer un groupe industriel sans usine. Dans le numérique comme dans d'autres secteurs, nous payons aujourd'hui les conséquences de la faillite de la pensée d'une part des élites françaises.

Il nous faut reconnaître que, centrés sur nous-mêmes, nous ne voyons que tardivement l'évolution rapide de notre environnement économique et politique. En 2024 selon le World Economic Forum[28], l'économie française passera de la sixième à la dixième place des économies mondiales. La Chine devancera les Etats-Unis et quatre pays asiatiques seront dans les cinq premières places, la Russie arrivera en sixième position. Le contexte de guerre froide Etats-Unis vs Union soviétique dans lequel ont été formés, raisonnent et agissent aujourd'hui encore les fonctionnaires occupant les plus hauts postes de responsabilité est dépassé. Pour se préparer à vivre dans un monde différent il faudrait s'appuyer sur les connaissances et les expériences des universitaires et des entrepreneurs habitués aux cultures, usages et marchés de ces pays.

Or « *L'idée est l'ennemie capitale des souverains*[29] ». Pour l'administration qui a fait sienne cette maxime impériale, il ne faut pas sortir du confort de la reproduction

Les études et rapports d'experts, les rapports parlementaires ne sont ainsi généralement pas lus à la hauteur de ce qu'ils pourraient apporter comme idées, et surtout comme actions. Les administrations préfèrent généralement ruminer des idées déjà digérées dans le silo voisin de ministère « compétents ».

Les personnes porteuses d'idées ou de pratiques nouvelles sont rarement tolérées dans le temps. Ainsi,

[25] Indice relatif à l'économie et à la société numériques (DESI, France, 2019). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59990

[26] Jacques-Bénigne BOSSUET. Oraison funèbre de Marie-Thérèse d'Autriche, reine de France.

[27] https://www.senat.fr/rapports-senateur/arthuis_jean83011j1992.html

[28] https://www.weforum.org/agenda/2020/07/largest-global-economies-1992-2008-2024

[29] "Maximes et pensées de Napoléon". Honoré DE BALZAC

le départ du premier secrétaire d'État chargé du numérique, officiellement pour des raisons de campagne électorale, s'est parallèlement accompagné de l'exfiltration de la seule personne en mesure de mener à son terme la transition numérique des administrations en favorisant l'expérimentation et le développement agile. Jugé trop remuant et trop créatif, il a été remplacé à la tête de la direction interministérielle du numérique par un profil plus conforme au feutre administratif. Son départ a été suivi d'une hémorragie des compétences de la DINUM.

Les organismes censés accompagner l'évolution de la société sont eux-mêmes victimes de la recherche d'économies lorsqu'ils ne sont pas soutenus. Ainsi le gouvernement a décidé en 2019 de la suppression de l'Institut national des hautes études de justice et de sécurité qui, sous la conduite d'Hélène CAZAUD-CHARLES avait pourtant mis en place, parmi d'autres sujets, un cycle de formation aux enjeux de la cybersécurité d'excellente qualité.

L'ANSSI n'est pas à l'abri de ces enfermements. Ainsi, il aura fallu sept ans et la détermination de ses deux directeurs généraux successifs pour que les experts de l'agence se dotent d'un conseil scientifique. Longtemps le cloud computing n'a été considéré par l'agence que comme un simple retour du client-serveur. Il aura fallu plusieurs réunions avec un équipementier télécoms non européen qui demandait à l'ANSSI ce qu'il faudrait ajouter aux standards en discussion finale pour améliorer la cybersécurité de la 5G pour que l'agence s'investisse sur ce nouveau protocole.

Les premiers actes et le style adopté par le nouveau Premier ministre, la nomination au poste clé de Secrétaire Générale du Gouvernement de Claire LANDAIS qui a suivi l'activité de l'ANSSI ces deux dernières années, sont un signe que l'humilité succède à l'arrogance.

La volonté ensuite.

Une fois la prise de conscience effectuée, l'arrogance tempérée par un peu d'humilité, forts des capacités françaises en matière de recherche et des grands acteurs du secteur - opérateurs télécoms, sociétés de service, startups et licornes potentielles - il est possible de doter la France d'une stratégie en matière de numérique, au-delà des stratégies de niche actuelles. Les idées existent, les acteurs du secteur en proposent régulièrement[30], de multiples rapports parlementaires en développent, notamment sur les trois leviers communs au numérique et à la cybersécurité que sont l'identité numérique[31] - des arbitrages sur ce sujet étaient déjà prêts en 2016 -, la ville et les territoires intelligents[32] - les collectivités sont livrées à elles-mêmes sur ce sujet pour lequel se posent pourtant des questions de souveraineté, d'égalité, de libertés et de protection des données. Pour la 5G, levier essentiel, le gouvernement ayant choisi dans les faits d'écarter les équipementiers non européens de la construction des futurs réseaux 5G, l'optimisme pousse à croire qu'existe déjà, partagée avec d'autres membres de l'Union, une stratégie de soutien des équipementiers européens qui procure une alternative d'équipements maîtrisés de même niveau technique et permette d'envisager les générations suivantes.

L'élaboration et le suivi d'une telle stratégie du numérique pourrait être confiée au Commissariat destiné à remplacer le Commissariat général à la stratégie et à la prospective créé en 2013[33], « France-Stratégie », dont les travaux n'ont pas été de nature à inspirer administrations et décideurs politiques. Il

[30] Par exemple les idées synthétisées par Syntec numérique en mai dernier https://syntec-numerique.fr/actu-informatique/75-propositions-secteur-numerique-pour-relance-economique

[31] Rapport des députés Marietta KARAMANLI, Christine HENNION et Jean-Michel MIS http://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information

[32] Rapport du député en mission Luc BELOT (2017) https://www.vie-publique.fr/rapport/36551-de-la-smart-city-au-territoire-dintelligences-lavenir-de-la-smart

[33] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027343503&categorieLien=id

appartiendra au nouveau Haut-Commissaire de veiller à ce que cette stratégie survive aux gouvernements. En matière de cybersécurité comme dans d'autres domaines, la Nouvelle France Industrielle du précédent quinquennat comportait des « feuilles de route » qui auraient mérité un peu de continuité. La quête d'éléments de communication susceptibles de montrer que les gouvernements agissent d'une part et l'appétence de quelques grandes entreprises pour les subventions qui accompagnent les programmes repeints d'autre part ont généralement raison de la continuité des politiques.

Enfin une stratégie du numérique devrait adopter une ambition claire et les moyens nécessaires, à l'instar de nos voisins allemands. En juin dernier, le gouvernement allemand a en effet décidé d'investir 9 des 130 milliards d'euros de leur plan de relance dans la filière hydrogène afin de devenir le numéro un mondial dans dix ans[34]. En 2018, le plan hydrogène de la France était doté de 100 millions d'euros, près de cent fois moins. Le plan de relance annoncé cet automne fixera sans doute une perspective plus réaliste.

Le courage enfin.

À l'international, être fidèle à ce que nous sommes. En choisissant un modèle de cybersécurité interministériel, dans lequel les pratiques défensives et offensives ne sont pas confiées aux mêmes acteurs, même s'ils travaillent ensemble, la France a choisi le seul choix qui permette le développement d'un numérique durable. Sous l'impulsion de la France, l'Union européenne a choisi une approche similaire. Un peu de courage pourrait peut-être aider à limiter les actions offensives néfaste de certains états dans le numérique. Lancé en 2018, l'« Appel de Paris pour la confiance et la sécurité dans le cyberespace[35] », conçu à l'origine par le Quai d'Orsay pour reprendre la main après la conférence organisée par le SGDSN à l'Unesco et répondre aux initiatives privées[36], a permis, grâce aux talents des diplomates, d'engager sur un même document près de 80 états dont certains s'opposent sur ces sujets dans les instances multilatérales et 650 entreprises. Devant l'impasse dans laquelle se trouvent les discussions du groupe d'experts de l'ONU face aux deux résolutions présentées par deux blocs d'états, l'Appel de Paris pourrait être enrichi, par exemple par la recherche des éléments communs à toutes les initiatives, et mieux exploité pour favoriser le désarmement dans l'espace numérique.

De la même manière, la décision récente de la Cour de Justice Européenne à propos du *privacy shield*, la volonté de l'ONU d'élaborer un texte sur la cybercriminalité, le projet de loi américain Earn it[37] sont autant de sujets sur lesquels la France pourrait s'exprimer et peser avec ses alliés européens pour conforter ses choix et promouvoir ses valeurs. Certaines organisations internationales[38] évoquent la cybersécurité comme un droit humain : la marge de manœuvre à l'international est donc importante.

En France, adopter des voies nouvelles. Vouloir que des startups innovantes deviennent des licornes au rayonnement mondial implique de s'exposer aux marchés et aux capitaux. Limiter les investissements étrangers dans les startups revient à les condamner au marché français ou, au mieux, européen.

Certains leviers restent à notre disposition. Celui de la commande publique par exemple qui représente 90 milliards d'euros annuels[39]. Une potentielle licorne française qui a décidé d'attaquer le marché américain a vu son principal concurrent local bénéficier d'un contrat public de 50 millions de dollars, lui procurant ainsi un avantage concurrentiel et la certitude d'une

[34] https://www.lemonde.fr/economie/article/2020/06/13/l-allemagne-veut-devenir-le-pays-de-l-hydrogene_6042722_3234.html

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

[36] Comme celle du techaccord initié par Microsoft https://cybertechaccord.org

[37] https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

[38] https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue

[39] 31 milliards pour les achats de l'Etat, 16 milliards pour les achats de défense et de sécurité, 23 milliards pour les hôpitaux publics, 20 milliards pour les collectivités territoriales.

valorisation conséquente. En France, « *L'innovation reste un ovni, mal appréhendé dans la communauté de la commande publique*[40] ». Pourtant, un décret de décembre 2018, sous-utilisé, autorise la conclusion de marchés sans mise en concurrence pour des achats innovants en dessous de 100 000 euros (un début !). De la même manière, on pourrait dans certains cas exclure de certains marchés publics les entreprises dépendantes d'un droit extra-européen.

À plusieurs reprises, le Président de la République a proposé des idées qui pourraient favoriser le développement du numérique et conforter le modèle français[41]. Ainsi en est-il du projet de Campus Cyber voulu par le Président de la République, inspiré des modèles israélien, américain, russe ou chinois mais fondé sur la création de communs opérationnels. Confié au seul entrepreneur capable de réunir tous les acteurs utiles, ce projet pourrait faire passer un cap d'efficacité à la cybersécurité française pour peu qu'administrations compétentes - dont l'ANSSI - aient le courage d'y investir des équipes opérationnelles en effectifs suffisants.

Conclusion

« *La barbarie d'aujourd'hui discourt et pose. Elle est vision du monde autant que pulsion. Elle érige sa violence en justice, sa vision du monde en vérité, son idéologie en absolu, l'irruption du réel en subversion. Elle précipite le lien pour le réduire à une relation univoque : dominer ou être dominé, appartenir à la race des seigneurs ou mériter sa place d'esclave. Au niveau des Etats, elle réactive la menace de la guerre*. »[42]

Dans tous les pays où il s'est développé, le numérique est rendu possible par la recherche et l'investissement essentiellement portés par le secteur privé. De leur côté les états fondent sur le numérique une part de plus en plus importante de leur croissance, de leur fonctionnement et de celui de la société.

Pourtant, ce sont les pratiques des états donnant la priorité à l'offensif qui mettent en danger un numérique qui soutient désormais l'essentiel des services critiques fournis à leurs populations. Il y a un peu plus de dix ans, un gouvernement français a choisi à contre-courant un modèle de cybersécurité privilégiant la prévention et la défense, seul moyen d'éviter l'escalade de l'affrontement entre états dans le numérique et la guerre dans le monde matériel.

Dans un cyberespace où les armes se retournent contre leurs créateurs et ou les preuves se fabriquent en quelques clics, des voix se font entendre qui déforment les positions françaises et en appellent à l'intervention de l'armée pour protéger les réseaux civils[43]. Si des sanctions à l'encontre d'entités étrangères comme celles prises sur la base de preuves par l'Union européenne ce 30 juillet sont proportionnées, si la caractérisation de la menace et la neutralisation des effets doit être élargie à la pose d'implants comme l'ont proposé des députés au printemps dernier[44], les discours autour d'une mal nommée « cyberdissuasion » doivent être tenus avec circonspection.

Dans le numérique, « Si vis pacem, para pacem ».

Par son histoire, sa culture, ses valeurs et ses choix, la France a une responsabilité dans le devenir du numérique. Avec de l'humilité, de la volonté et du courage, notamment de la part du gouvernement et des administrations, elle pourra, comme par le passé, peser en faveur d'une approche favorable au

[40] Samira BOUSSETTA, "Appuyons la transformation sur l'achat public !"in acteurs publics n°141, septembre 2019

[41] Notamment à l'occasion du discours annuel prononcé lors de la conférence des ambassadeurs.

[42] Céline PINA, "Nous nous vivions puissance, nous nous sommes réveillés nus… et barbares." in Front Populaire, n°1, Juin 2020.

[43] Dans l'actuel code de la défense, il n'est pas question de riposte face à une attaque informatique mais de caractérisation de la menace et de neutralisation de ses effets.
https://www.lemonde.fr/idees/article/2020/01/28/cybercoercition-un-nouveau-defi-strategique_6027444_3232.html

[44] http://www.assemblee-nationale.fr/dyn/15/textes/l15b2778_proposition-loi

développement du numérique et respectueuse de la souveraineté des états pour peu qu'elle conserve l'approche pluridisciplinaire déjà identifiée comme une nécessité il y a soixante-dix ans : « *Il ne serait peut-être pas mauvais que les équipes présentement créatrices de la cybernétique adjoignent à leurs techniciens venus de tous les horizons de la science quelques anthropologues sérieux et peut-être un philosophe curieux de ces matières* [45]. »

[45]Père Dominique DUBARLE, à propos de la publication de "Cybernetics, or control and communication in the animal and the machine," de Norbert WIENER, journal Le Monde, 28 décembre 1948.