BRENNUS 4.0

LETTRE D'INFORMATION DU CENTRE DE DOCTRINE ET D'ENSEIGNEMENT DU COMMANDEMENT

Mars 2020

La stratégie française de cyberdéfense

Par Madame Aude Géry [1] , chercheur associé au sein de GEODE, centre de recherche et de formation sur la géopolitique de la Datasphère, et officier de réserve à l'EMSST

L'expansion et l'interconnexion des systèmes d'information et de communication ont fait apparaître de nouveaux défis pour les États, tant en termes de développement que de sécurité. Pour y faire face, ces derniers, dont la France, ont adopté différentes stratégies, en fonction de leur histoire, de leur fonctionnement mais également de la façon dont le cyberespace a été appréhendé [2]. La stratégie française de cyberdéfense se distingue par plusieurs caractéristiques, au plan doctrinal et organisationnel, qui lui sont propres. Si ces deux dernières années ont été particulièrement prolifiques au plan doctrinal, on relève une continuité et une cohérence d'action visant à doter la France des moyens d'assurer sa sécurité, et celle de ses citoyens, dans le cyberespace mais également d'y projeter sa puissance.

La stratégie française en matière de cyberdéfense : le choix d'une approche globale

« A l'heure où les attaques informatiques sont susceptibles de porter à tout moment gravement atteinte aux intérêts de la Nation, notre pays doit adapter sa posture de cyberdéfense avec l'ambition de mieux faire respecter sa souveraineté numérique »[3]. C'est par ces mots que la *Revue stratégique de cyberdéfense*, présentée le 12 février 2018, introduit la stratégie française en matière de cyberdéfense. Elle entérine ainsi un changement d'approche amorcé dès la publication de la *Stratégie nationale pour la sécurité du numérique* en 2015[4]. Jusqu'en 2015, la France retenait une approche technico-militaire de la cybersécurité, c'est-à-dire fondée uniquement sur la protection et la résilience des systèmes d'information et de communication. Depuis 2015, elle a adopté une approche globale, c'est-à-dire reposant sur la sécurité du numérique, celui-ci ayant pénétré tous les champs économiques et sociétaux.

Une approche globale reposant sur un modèle organisationnel dominé par l'ANSSI et caractérisée par la séparation des missions offensives et défensives

Pour assurer sa souveraineté numérique, la France n'a cessé, depuis le *Livre blanc de la défense et de la sécurité nationale* de 2008, premier document stratégique mentionnant le cyberespace comme espace stratégique, de renforcer ses moyens organisationnels, capaci-

taires, humains et juridiques pour assurer sa cyberdéfense. Succédant à la Direction centrale de la sécurité des systèmes d'information, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée en 2009[5] et désignée autorité nationale en charge de la sécurité des systèmes d'information en 2013[6]. Placée sous l'autorité du Premier ministre, elle constitue la pierre angulaire de l'organisation de la cyberdéfense française. Chargée de la coordination de la stratégie française de cyberdéfense, ses missions ont progressivement été élargies par les lois de programmation militaire de 2013[7] et 2018[8]. Elle est ainsi en charge de la défense et de la sécurité des systèmes d'information de l'Etat. De plus, elle dispose d'un pouvoir réglementaire lui permettant de fixer les règles devant être mises en œuvre par les opérateurs d'importance vitale en matière de protection de leurs systèmes d'information d'importance vitale, d'un pouvoir de certification et qualification des produits et services, et enfin du pouvoir, en cas de crise majeure, d'imposer des mesures à ces opérateurs. L'élargissement de ses missions ainsi que de l'approche retenue par la *Stratégie* de 2015, puis la *Revue stratégique de cyberdéfense,* vont nécessiter l'implication d'autres acteurs, tels que le ministère de l'Intérieur, le ministère de la Justice ou le ministère de l'Europe et des affaires étrangères. Il en résulte alors une stratégie profondément interministérielle, qui se traduit dans les chaînes opérationnelles et la gouvernance de la cyberdéfense, créées et modernisée en 2018[9], dont la coordination est assurée par l'ANSSI.

Ce qui caractérise la stratégie française de cyberdéfense depuis ses débuts est son modèle d'organisation et de gouvernance. Il repose sur un principe fondamental : la séparation des missions et capacités offensives (renseignement et opérations offensives) et défensives (protection et défense des réseaux), se distinguant ainsi des modèles anglo-saxons[10]. Cette séparation vise à *« garantir une meilleure coordination entre l'ANSSI et la cyberdéfense militaire »* et à *« faciliter un travail de confiance entre l'ANSSI et les entreprises »*[11]. L'ANSSI ne dispose ainsi pas du pouvoir de mener des opérations offensives. Cette séparation contient cependant des ambiguïtés. En effet, l'ANSSI, pour répondre à une attaque informatique affectant la sécurité de la Nation, peut *« procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque »*[12]. Or, dans la mesure où elles consistent à pénétrer des systèmes tiers sans autorisation du propriétaire ou de l'administrateur, ces opérations techniques peuvent être qualifiées d'opérations offensives. Pour autant, ce modèle, confirmé dans la *Revue stratégique de cyberdéfense*, offre de nombreux avantages à même de renforcer la résilience de la Nation face aux menaces informatiques.

Une approche globale qui a pour objectif d'assurer la souveraineté numérique de la France

La *Revue stratégique de cyberdéfense* est claire : *« [l]a cyberdéfense de la France, au-delà de celle de l'État lui-même et des opérateurs d'importance vitale, passe par une élévation du niveau global de cybersécurité dans la société. Pour être efficace, il s'agit bien d'envisager, dans une logique de souveraineté numérique, une défense cyber dans la profondeur de notre pays intégrant celle des citoyens, des entreprises et des collectivités territoriales »*[13].

Elle contient cependant une ambiguité sémantique liée au

concept de souveraineté numérique. En effet, la souveraineté numérique y est définie comme *« la capacité de la France d'une part, d'agir de manière souveraine dans l'espace numérique, en y conservant une capacité autonome d'appréciation, de décision et d'action et d'autre part, de préserver les composantes les plus traditionnelles de sa souveraineté vis-à-vis de menaces nouvelles tirant partie de la numérisation croissante de la société »*[14]. On comprend dès lors que le concept de souveraineté numérique renvoie à celui d'autonomie stratégique numérique. Comme le relève Alix Desforges, cela fait écho à *« un concept très lié à la notion d'autonomie de décision développée par le théoricien de la dissuasion nucléaire, le général Poirier »*[15]. L'autonomie de la décision se traduit par la capacité à identifier et caractériser les menaces afin de pouvoir y répondre. Elle suppose préalablement une identification des activités souveraines et impose de disposer de technologies propres permettant de les exercer. Tirant les conséquences de cet objectif, la *Revue stratégique de cyberdéfense* identifie alors des technologies dont la maîtrise est essentielle

à l'exercice de cette autonomie de décision : le chiffrement des communications, la détections d'attaques informatiques, les radios mobiles professionnelles, le cloud et l'intelligence artificielle[16].

Cette confusion sémantique n'obère cependant pas totalement les aspects traditionnels de la souveraineté. En tant qu'État, la France est par nature souveraine et exerce donc ses prérogatives dans l'espace numérique. Si cet exercice peut être rendu difficile par la nature transfrontière des réseaux et la multiplication des conflits de juridiction, le principe même de sa souveraineté ne saurait être remis en cause. Par ailleurs, l'autonomie stratégique numérique, évoquée en filigrane de la souveraineté numérique, participe à l'exercice de cette souveraineté en visant à doter la France des moyens d'exercer ses compétences, et notamment d'appliquer son droit national, sur son territoire et ses citoyens.

La place des Armées dans l'organisation française de cyberdéfense

On ne saurait présenter la stratégie française de cyberdéfense sans mentionner le rôle et la place particuliers du ministère des Armées dans le modèle français de cyberdéfense. En 2008, le cyberespace est identifié dans le *Livre blanc de la défense et de la sécurité nationale* comme *« un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires »*[17]. C'est cette représentation du cyberespace comme champ de confrontation qui confèrera au ministère des Armées une place à part dans le dispositif français de cyberdéfense[18]. La nomination d'un officier général cyberdéfense, rattaché au sous-chef opérations de l'Etat-major des Armées en 2011 marquera alors le début de la montée en puissance des Armées dans ce domaine. En effet, si l'ANSSI est l'autorité nationale en charge de la défense et de la sécurité des systèmes d'information, ce qui est depuis devenu le COMCYBER a une place particulière : il a en charge la sécurité des réseaux du ministère des Armées ainsi que la conduite des opérations militaires dans le cyberespace. La loi de programmation militaire de 2013 marque un changement d'échelle en organisant une véritable chaîne opérationnelle de cyberdéfense. L'évolution va se poursuivre avec la constitution, en 2017, du commandement de la cyberdéfense (COMCYBER) qui est directement placé sous l'autorité du Chef d'État-major des Armées puis la présentation, le 18 janvier 2019, de la *Stratégie cyber des Armées*.

Présentée par Florence Parly, ministre des Armées, et par le général Lecointre, Chef d'État-major des Armées, la *Stratégie cyber des Armées* est le premier document stratégique des Armées portant exclusivement sur la cyberdéfense dont certains éléments sont rendus publics. En effet, deux documents, les *Éléments publics de doctrine militaire de lutte informatique offensive* et la *Politique ministérielle de lutte informatique défensive*, ont été publiés suite au discours de la ministre[19]. S'ils ont été particulièrement remarqués en raison d'éléments portant sur la lutte informatique offensive, il faut cependant relever qu'ils ne constituent en rien une rupture dans la stratégie française de cyberdéfense militaire. *A contrario*, ils s'inscrivent dans la lignée de la *Revue de la défense et de la sécurité nationale* et de la *Revue stratégique de cyberdéfense* en visant à doter les Armées d'une stratégie leur permettant d'assurer leur supériorité dans cet espace et ainsi d'assurer la sécurité de la Nation et d'exercer pleinement sa souveraineté. Par ailleurs, le fait d'assumer développer, détenir et utiliser des capacités offensives n'est pas une nouveauté. En effet, dès 2008, le *Livre blanc* reconnaissait la nécessité pour la France de se doter de telles capacités[20]. Ces deux documents marquent néanmoins une étape importante dans la construction de la stratégie militaire française de cyberdéfense, non seulement en organisant une normalisation de l'offensif, mais également en participant ainsi au renforcement de la posture de puissance cyber dont la France entend se prévaloir[21].

Une stratégie internationale volontariste de la France en matière de cyberdéfense

Le dernier élément marquant de la stratégie française de cyberdéfense porte sur sa stratégie internationale. Si la nomination du premier ambassadeur en charge des questions de cyberdéfense ne date que de 2014, la France a participé à tous

les cycles de négociations des Nations unies relatifs aux technologies de l'information et de la communication dans le contexte de la sécurité nationale à partir de 2004. Elle a également participé activement à l'élaboration de la Convention sur la cybercriminalité, adoptée par le Conseil de l'Europe en 2001, et a notamment été à l'initiative de l'inscription sur la Liste des biens et technologies à double usage de l'Arrangement de Wassenaar des logiciels d'intrusion. La nomination d'un ambassadeur du numérique au mandat extrêmement large, en 2017, suivi quelques semaines plus tard de la publication de Stratégie internationale de la France pour le numérique, entérinèrent le rôle clé du ministère de l'Europe et des affaires étrangères dans l'élaboration et la mise en œuvre de la stratégie française de cyberdéfense. Elles marquent également le choix de la France d'être un acteur de premier plan dans la sécurité et la stabilité internationales du cyberespace.

La *Revue stratégique de cyberdéfense* consacre ainsi de longs développements aux objectifs de la France en proposant d'aller plus loin dans l'élaboration du cadre juridique international, à travers la promotion des normes de comportement responsable des États. De plus, elle détaille, pour la première fois, sa vision de l'application du droit international dans le cyberespace[22]. Enfin, elle propose de nouvelles règles et normes concernant la responsabilité des acteurs non-étatiques en matière d'usage d'outils offensifs, et la responsabilité des entreprises pour la conception et la maintenance des produits numériques. Le lancement de l'*Appel de Paris pour la sécurité et la stabilité du cyberespace*[23], avec le soutien extrêmement actif de Microsoft[24], en novembre 2018, constitue la dernière initiative internationale de la France. Signé par plus de 60 États et 500 acteurs non-étatiques, ce document liste des engagements politiques, pour certains nouveaux, visant à renforcer la sécurité et la stabilité du cyberespace. Marqué par son caractère multiacteurs, il s'inscrit dans la continuité de la reconnaissance des responsabilités partagées mais différenciées de tous les acteurs, étatiques ou non, dans la stabilité du cyberespace, et démontre la volonté, également illustrée par le soutien de la France à la Global Commission on the Stability of Cyberspace, d'avancer dans ce domaine.

Pour autant, la stratégie internationale de la France ne doit pas être limitée aux questions de paix et sécurité internationales et de gouvernance d'Internet. En effet, l'activité diplomatique de la France est également représentée par les coopérations techniques en matière de cybersécurité, principalement pilotées par l'ANSSI, ou encore la coopération dans le domaine militaire mise en œuvre par le COMCYBER, notamment dans le cadre de l'OTAN. Toutes ces initiatives participent ainsi à la projection de puissance numérique de la France et constituent un pilier important de sa stratégie

La stratégie française de cyberdéfense se caractérise par son approche globale, tant en termes de contenu que d'acteurs. Elle vise à permettre à la France d'assurer sa sécurité et celle de ses citoyens et de projeter sa puissance dans le cyberespace. Aymeric Bonnemaison et Stéphane Dossé écrivaient en 2014 qu'il *« apparaît [donc] nécessaire pour les États de « planter le drapeau » »*[25] dans le cyberespace. De ce point de vue, la France a assurément commencé à le faire en consacrant d'importants efforts à la montée en puissance de la cyberdéfense française, tant au plan défensif qu'offensif. En parallèle, son action se caractérise par une volonté de faire progresser la sécurité et la stabilité du cyberespace en participant activement aux négociations internationales dans ce domaine, et en promouvant une plus grande responsabilité de tous les acteurs concernés. Enfin, tant au niveau national qu'international, son action repose sur le principe de coopération, condition *sine qua non* pour assurer sa sécurité dans le cyberespace ainsi que la stabilité de l'environnement informatique mondial.

———————————

[1] Aude Géry est doctorante en droit international public à l'Université de Rouen. Sa thèse porte sur la prolifération des armes numériques. Elle est également chercheuse associée au sein de GEODE, centre de recherche et de formation sur la géopolitique de la Datasphère, et officier de réserve à l'EMSST.

[2] Frédérick Douzet (dir.), *Cyberespace : enjeux géopolitiques, Hérodote*, n°152-153, 1er-2ème trimestre 2014, 313 p.

[3] *Revue stratégique de cyberdéfense*, 2018, p. 7.

[4] Pour une analyse de l'évolution de la stratégie française de cyber-défense, voir Alix Desforges, *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France*, Thèse, Université Paris 8, 2018, 395 p.

[5] Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».

[6] Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, article 21.

[7] *Ibid.*, articles 21 et 22.

[8] Loi n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, article 34.

[9] *Revue stratégique de cyberdéfense, op. cit.*, pp. 52-55.

[10] À titre d'exemple, au Royaume-Uni, c'est le Government Communication Headquarters (GCHQ), service de renseignement technique, qui est chargé des opérations offensives et de la cybersécurité et cyberdéfense de l'Etat. Le National Cyber Security Centre, en charge de la protection des systèmes informatiques, est une division du GCHQ.

[11] Danilo D'Elia, *La cybersécurité des opérateurs d'importance vitale : analyse géopolitique des enjeux et des rivalités de la coopération pulbic-privé*, Thèse, Université Paris 8, 2017, pp. 116-117.

[12] Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, article 21.

[13] *Revue stratégique de cyberdéfense, op. cit.*, p. 93.

[14] *Ibid*.

[15] Amaëlle Guiton, « Internet : des États entre « souveraineté numérique » et « autonomie stratégique », *Libération*, 13 février 2019, disponible sur https://www.liberation.fr/planete/2019/02/13/internet-des-etats-entre-souverainete-numerique-et-autonomie-strategique_1709212.

[16] *Ibid*., p. 96 et suivantes.

[17] Livre Blanc de la défense et de la sécurité nationale, 2008, p. 53.

[18] Alix Desforges, *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France*, *op. cit.*, p. 120-156.

[19] On relèvera ici encore le choix de séparer distinctement les missions offensives des missions défensives même si, comme l'affirme les *Éléments publics*, la lutte informatique offensive peut être mise au service de la lutte informatique défensive.

[20] *Livre blanc de la défense et de la sécurité nationale, op. cit.*, p. 53.

[21] Pour une analyse de ces documents, voir François Delerue, Alix Desforges, Aude Géry, « A Close Look at France's New Military Cyber Strategy », *War on the Rocks*, 23 avril 2019, disponible sur https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/ ; Stéphane Taillat, « Signaling, Victory, and Strategy in France's Military Cyber Doctrine », *War on the Rocks*, 8 mai 2019, disponible sur https://warontherocks.com/2019/05/signaling-victory-and-strategy-in-frances-military-cyber-doctrine/.

[22] François Delerue, Aude Géry, « France's Cyberdefense Strategic Review and International Law », *Lawfare*, 23 mars 2018, disponible sur https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.

[23] https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la.

[24] Martin Untersinger, « La France veut relancer les négociations sur la paix dans le cyberespace », *Le Monde*, 8 novembre 2018, disponible sur https://www.lemonde.fr/pixels/article/2018/11/08/la-france-veut-relancer-les-negociations-sur-la-paix-dans-le-cyberespace_5380571_4408996.html.

[25] Aymeric Bonnemaison, Stéphane Dossé, *Attention : Cyber ! Vers le combat cyber-électronique*, Economica, 2014, p. 79