# LA CYBERSTRATÉGIE FRANÇAISE

**Olivier Kempf ***

Depuis 2008, la France a pris la mesure des défis posés par le cyberespace. Ils sont divers et touchent à de nombreux domaines : vie quotidienne des citoyens et libertés publiques, défis économiques, défense et sécurité. Ce dernier aspect, celui qu'on désigne couramment par la notion de cyberdéfense, est l'objet de cet article qui vise à décrire et analyser la cyberstratégie française : on n'évoquera pas ainsi les questions civiles et économiques qui mériteraient, à elles seules, des articles particuliers.

Sans entrer dans un discours belliqueux, très souvent employé par de nombreux auteurs, notamment anglo-saxons, il vise à comprendre comment la France a articulé en quelques années une posture générale de cyberdéfense, lui permettant de combler une partie de son retard initial pour présenter un dispositif assez complet, même s'il compte encore quelques lacunes. Ainsi, le cyberespace doit être perçu comme un nouveau domaine de souveraineté dont la France ne pouvait être absente. De ce point de vue, la cyberdéfense constitue, à n'en pas douter, une des vraies priorités stratégiques de la France.

Pour le saisir, il convient tout d'abord de décrire le dispositif qui a été élaboré, avant de proposer quelques clefs d'interprétation démontrant toute l'importance qui est porté à cette cyberdéfense.

---

* politologue, chercheur associé à l'iris
Auteur d'*Alliances et mésalliances dans le cyberspace*, 2014, Économica.

*Recherches internationales*, n° 100, juillet-septembre 2014, pp. 135-151

## État des lieux

Le cyber français n'est pas une nouveauté qui aurait été découverte il y a seulement quelques années. Il est l'héritier d'une longue tradition du chiffre et de la cryptographie, datant de la Deuxième Guerre mondiale. Ainsi, la Direction technique du chiffre est créée en 1943 à Alger. Elle évolue jusqu'à devenir la Direction centrale de la sécurité des systèmes d'information (DCSSI) en 2001. L'an 2000 constitue par ailleurs le passage du chiffrement au cyberespace, c'est-à-dire à l'« interconnexion généralisée des réseaux ». Avec le cyber, il n'est plus simplement question du chiffrage de transmission (alors principalement par ondes) mais de quelquechose de nouveaux.

Ainsi, après les premières initiatives datant de 2008, l'effort a été poursuivi et accentué depuis 2012.

### *Des premières initiatives au tournant de 2008*



La prise de conscience par les autorités publiques des questions de sécurité informatique a débuté dans les années 2000. Parmi les premières initiatives, comptons le plan de renforcement de la sécurité des systèmes d'information de l'État, décidé par Jean-Pierre Raffarin (alors Premier ministre) en 2004. En 2005, le député Pierre Lasbordes rédige un rapport sur « *La sécurité des systèmes d'information – Un enjeu majeur pour la France* », rendu public en janvier 2006. Pour la première fois, l'approche dépasse le seul périmètre des systèmes d'information de l'État pour évaluer aussi la question des infrastructures vitales nécessaires au pays et inclut le monde de l'entreprise dans son ensemble. Le rapport conclut déjà à un retard français en la matière et note plusieurs points : la dispersion et l'autonomie des différents acteurs au sein des services de l'État, des moyens insuffisants et des entreprises vulnérables.

#### *La prise de conscience de l'année 2008*



L'attaque informatique contre l'Estonie en 2007 ainsi que l'agression de plusieurs services étatiques français (notamment des diplomates en poste en ambassade) provoquent une prise de conscience généralisée qui suscite l'intérêt du Sénat : le sénateur Roger Romani publie ainsi en juillet 2008 un rapport sur la

cyberdéfense[1], qui est le premier document officiel à aborder le sujet en profondeur[2]. Quasi simultanément, en juin 2008, le *Livre blanc sur la défense et la sécurité nationale* évoque la question. Il mentionne « le cyberespace », constitué par « le maillage de l'ensemble des réseaux, [qui] est radicalement différent de l'espace physique », et conclut à la certitude, dans les années à venir, de la multiplication d'attaques informatiques. Elles sont considérées comme un des risques majeurs pesant sur le pays.

Le *Livre blanc* de 2008 donne les grandes orientations : il identifie la sécurité des systèmes d'information comme un des attributs majeurs de la souveraineté nationale : « La France doit garder un domaine de souveraineté, concentré sur les capacités nécessaires au maintien de l'autonomie stratégique et politique de la nation : la dissuasion nucléaire, le secteur des missiles balistiques, les sous-marins nucléaires d'attaque, la sécurité des systèmes d'information font partie de ce premier cercle. »[3]

Il définit brièvement le cyberespace comme « le maillage de l'ensemble des réseaux » et précise que « dans la mesure où le cyberespace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace. Des règles d'engagement appropriées, tenant compte des considérations juridiques liées à ce nouveau milieu, devront être élaborées » (p. 53).

Le *Livre blanc* juge indispensable de renforcer la « coopération opérationnelle » en Europe, mais aussi d'imposer « des règles de durcissement des réseaux » (p. 96). Enfin, un long développement est consacré à la lutte informatique offensive (LIO) : « Dans le domaine informatique plus que dans tout autre milieu, il faudra, pour se défendre, savoir attaquer. Il faut donc connaître les formes et les techniques, multiples et diversifiées, de ces attaques potentielles (saturation, fichiers piégés, codes malveillants…), et savoir engager l'adversaire à la source même de l'agression, au travers de modes d'action offensifs. »





[1] Roger Romani, *Rapport sur la cyberdéfense*, Sénat, commission des Affaires étrangères, 8 juillet 2008, 59 p.

[2] Il précise ainsi la nature et les formes de la menace, constate que la France est insuffisamment préparée et organisée, et détaille les orientations positives du *Livre blanc* en appelant à des mesures supplémentaires.

[3] *Livre blanc sur la défense et la sécurité nationale*, p. 318.

Le *Livre blanc* préconise ensuite la définition d'un cadre d'emploi, le développement d'outils spécialisés, la formulation d'une doctrine d'emploi pour les capacités de LIO, la mise en œuvre d'une formation adaptée et régulièrement actualisée. Il ajoute que « ce cadre d'emploi devra respecter le principe de riposte proportionnelle à l'attaque, visant en priorité les moyens opérationnels de l'adversaire » (p. 207 et 208). Enfin, dans le droit fil des recommandations du *Livre blanc*, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a modifié l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, notamment au sein du titre V qui décrit les « mesures de sécurité relatives aux systèmes d'information » (articles 83 à 92).

*Premières mesures : création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et nomination d'un officier cyber*



L'État crée en 2009 l'ANSSI. C'est un service à compétence nationale rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN).

Il permet de se doter d'une capacité de prévention et de réaction face aux attaques informatiques, afin de mettre en place une politique de prévention et de disposer d'un réservoir de compétences. L'ANSSI « a pour principales missions d'assurer la sécurité des systèmes d'information de l'État et de veiller à celle des opérateurs nationaux d'importance vitale, de coordonner les actions de défense des systèmes d'information, de concevoir et déployer les réseaux sécurisés répondant aux besoins des plus hautes autorités de l'État et aux besoins interministériels, et de créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information en France et en Europe »[4]. Selon un décret de 2011, l'ANSSI est de plus « autorité nationale de défense des systèmes d'information ». À ce titre, elle décide les mesures que l'État met en œuvre pour répondre aux « crises affectant ou menaçant la sécurité des



[4] Voir « Présentation de l'ANSSI » sur le site de l'agence, http://www.ssi.gouv.fr/fr/anssi/presentation/

systèmes d'information des autorités publiques et des opérateurs d'importance vitale et elle coordonne l'action gouvernementale ».

En juillet 2011, un officier général de la cyberdéfense (« OG cyber ») est désigné par l'état-major des armées au sein du ministère de la Défense. Le ministère conserve en effet un rôle particulier dans le domaine cyber, tout d'abord parce que les militaires mènent des actions qui ne se limitent pas au territoire national. De plus, il y a nécessité de protéger particulièrement les systèmes d'information du ministère, puisque les armées doivent assurer la sécurité du pays en tout temps et toutes circonstances. Les services de l'OG cyber travaillent en étroite collaboration avec ceux de l'ANSSI.

*L'ANSSI*

La stratégie de la France en matière de « Défense et sécurité des systèmes d'information » a été publiée le 15 février 2011. Ce document de 24 pages décrit quatre objectifs stratégiques :
– être une puissance mondiale de cyberdéfense ;
– garantir la liberté de décision de la France par la protection de l'information de souveraineté ;
– renforcer la cybersécurité des infrastructures vitales nationales ;
– assurer la sécurité dans le cyberespace.

Pour cela, sept axes d'effort ont été identifiés :
– anticiper et analyser ;
– détecter, alerter et réagir ;
– accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines ;
– protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales ;
– adapter notre droit ;
– développer nos collaborations internationales ;
– communiquer pour informer et convaincre.

Cette stratégie illustre la difficulté de l'exercice, puisqu'il s'agit d'assurer la sécurité à la fois de l'État (donc des administrations), mais aussi des entreprises et des citoyens. Elle mentionne la notion « d'information de souveraineté » (qui doit d'ailleurs être protégée jusqu'au niveau territorial) : cela reste à préciser, mais suggère que la cyberdéfense ne se limite pas seulement aux contenants (matériels et logiciels) mais touche aussi à ce qu'ils transportent, c'est-à-dire à la qualité des informations.

## *Doctrine militaire*

Une doctrine militaire de cyberdéfense a été développée sous la direction du Centre interarmées de concept, doctrines et expérimentations (CICDE, organisme sous la tutelle de l'État-major des armées, EMA). Un concept de cyberdéfense (CIA 6.3) a été publié à l'automne 2011, avant de devenir une RDIA 6.3. Une doctrine interarmées de cyberdéfense (DIA 6.3) a été publiée en janvier 2012. Une nouvelle mouture a été publiée en avril 2014 (DIA 3.40).

Ces deux documents sont protégés en « diffusion restreinte » : on ne peut donc pas en parler en détail sinon pour signaler qu'ils décrivent les objectifs et les principes d'organisation mis en œuvre par le ministère de la Défense pour cette cyberdéfense[5].

## *Un effort prolongé depuis 2012*

### *Le rapport Bockel*



En 2012, le sénateur Bockel publie un rapport dans le contexte de la campagne présidentielle. Il a pour objet de faire le point en prévision du nouveau *Livre blanc* à venir et de sensibiliser les esprits. Il propose de « faire de la cyberdéfense une priorité nationale », constatant des lacunes lors de la comparaison effectuée avec nos voisins similaires (Allemagne, Grande-Bretagne). Le rapport propose notamment de renforcer les effectifs et moyens consacrés à la cyberdéfense, de créer un pôle juridictionnel spécialisé, de rendre obligatoire la déclaration d'incident, de renforcer la protection des opérateurs d'importance vitale (OIV), de conduire une politique industrielle, de développer la formation, d'augmenter la coopération européenne, et de se méfier de certaines entreprises chinoises (Huawei et ZTE) mesure qui retiendra l'attention d'un document plus riche que cette simple idée.

### *Le* Livre blanc *sur la défense et la sécurité nationale de 2013*

Le *Livre blanc sur la défense et la sécurité nationale* de 2013 (ci-après désigné par LB) répond un an plus tard au rapport Bockel. Le



[5] On pourra cependant lire S. Gourtay, « Travaux de concept et de doctrine de cyberdéfense », *Revue Défense nationale,* juin 2012.

préfixe « cyber » apparaît 36 fois (hors sommaire) pour 160 pages, quand il apparaissait, en 2008, seulement 6 fois pour 350 pages. Il constate : « Le cyberespace est donc désormais un champ de confrontation à part entière ». Il marque incontestablement la vraie priorité donnée au sujet.

Il énonce le développement par la France de capacités *défensives et offensives* (ce qui n'est qu'un rappel des principes déjà évoqués dans le LB 2008). Le cyberespace intègre logiquement la posture permanente de sécurité (PPS) selon une « posture de cybersécurité ». Il décrit une chaîne opérationnelle de cyberdéfense « centralisée à partir du centre de planification et de conduite des opérations de l'état-major des armées ». La DGA se voit confier le volet technique de la cyberstratégie française. Les efforts humains ne sont pas négligés puisque le LB décide la mise en place d'une nouvelle réserve opérationnelle, quand un recrutement est prévu « à la hauteur des efforts consentis par nos partenaires britannique et allemand ». Les opérateurs d'importance vitale verront leur standard de sécurité informatique fixé par un dispositif législatif et réglementaire. Le LB expose une doctrine de réponse aux agressions informatiques majeures, fondée sur deux manœuvres : celle de la *prévention* qui sera coordonnée sous l'autorité du Premier ministre, et celle de l'intervention qui se veut être une *réponse globale* et ajustée faisant appel à divers moyens diplomatiques, juridiques et policiers. En fonction des circonstances, les moyens de la défense seraient utilisés de façon graduée.



### *Discours de M. Le Drian de juin 2013*

À l'issue de la publication du LB 2013, le ministre de la Défense, Jean-Yves Le Drian, a tenu à Rennes le 3 juin 2013 un discours important d'affirmation de la posture française de cyberdéfense[6]. Il constitue une parole « politique » qui vient en appui du LB et en détaille certains aspects. Ainsi, le ministre rappelle que « Le LB de 2013 élabore une doctrine nationale de réponse aux agressions informatiques majeures. Une politique

[6] Accessible à http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/discours-du-ministre-de-la-defense-au-colloque-sur-la-cyberdefense (consulté le 31 mai 2014).

de sécurité ambitieuse sera ainsi mise en œuvre, afin d'identifier l'origine des attaques, d'évaluer les capacités offensives des adversaires potentiels et l'architecture de leurs systèmes, et de pouvoir ainsi les contrer ». Cette politique comprend deux volets : « la montée en puissance d'une posture robuste et résiliente pour protéger les systèmes d'information de l'État, les opérateurs d'importance vitale et les industries stratégiques. [Et] une capacité de réponse gouvernementale devant des agressions qui sont de nature et d'ampleur variées ». Il ajoute que « La capacité informatique offensive, associée à des capacités de renseignement, concourt de façon significative à notre posture de cybersécurité. Elle contribue notamment à caractériser la menace et à identifier son origine. Elle permet, en outre, d'anticiper certaines attaques et de configurer nos moyens de défense en conséquence. La capacité offensive enrichit la palette des options qui sont à la disposition de l'État. Elle comporte elle-même différents stades, qui sont plus ou moins réversibles, plus ou moins discrets, mais toujours proportionnés à l'ampleur et à la gravité de la situation. »



*La LPM et ses suites*

La loi de programmation militaire (LPM) 2014-2019, adoptée en 2013, apporte quelques précisions en matière de cyberdéfense et sécurité. Ainsi, le Premier ministre pourra imposer aux opérateurs d'importance vitale des obligations en matière de sécurisation de leur réseau, de qualification de leurs systèmes de détection, d'information sur les attaques qu'ils peuvent subir et de soumission à des contrôles de leur niveau de sécurité informatique ou de l'application des règles édictées. De même, l'effort de développement des capacités de cyberdéfense militaires est poursuivi avec la mise en place d'un dispositif de cyberdéfense militaire, étroitement intégrée aux forces et en relation avec le domaine du renseignement, des capacités défensives et offensives pour préparer ou accompagner les opérations militaires, une chaîne opérationnelle de cyberdéfense (centralisée à partir du centre de planification et de conduite des opérations de l'état-major des armées), une composante technique confiée à la DGA et chargée de connaître et d'anticiper la menace, de développer la recherche amont et d'apporter son expertise en cas de crise informatique. Les moyens humains consacrés à la cyberdéfense

seront renforcés avec le recrutement de centaines de spécialistes et la mise en place d'une réserve opérationnelle de cyberdéfense.

Il reste que l'article 20 de la loi a suscité une grande polémique puisqu'il autorise un grand nombre d'administrations à se faire communiquer par tous les opérateurs les « documents » qu'ils ont transmis ou stockés, sous réserve de la recherche de renseignements intéressant par exemple la sécurité nationale, la prévention du terrorisme, la criminalité, la délinquance organisée ou surtout « la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ». Même la CNIL s'en était émue.

Pour prolonger cette loi, en février 2014, le ministre de la Défense, Jean-Yves Le Drian, présentait un pacte de cyberdéfense sur lequel nous reviendrons plus en détail.

*

Ainsi, le discours français de cyberdéfense s'est progressivement enrichi depuis les premières conclusions du rapport Laborde en 2006. Il témoigne d'une prise de conscience incontestable. Huit ans plus tard, la France dispose d'un corpus doctrinal riche et globalement cohérent. Au fond, il manifeste la prise en compte de la dimension cyber de la souveraineté qui est en phase de durcissement car elle démontre une position géopolitique qui s'affirme à mesure que le cyberespace prend de l'ampleur.



## Une cybersouveraineté en phase de durcissement

Décrire un dispositif est peut-être ce qu'il y a de plus aisé. Plus délicate est l'interprétation de cette évolution : que signifie-t-elle vraiment ? Or, il ne s'agit pas simplement de suivre un discours à la mode mais bien de répondre aux défis posés non seulement par le cyberespace mais par la dimension géopolitique de celui-ci.

Ainsi, la position française affirme que le cyberespace appartient au cœur de souveraineté, ce qui entraîne une posture internationale qui répond aux défis posés par la cyberconflictualité et la guerre économique.

### *Le cyberespace appartient au cœur de souveraineté*

Les décisions prises au cours de la dernière décennie témoignent de la prise de conscience, par les autorités françaises,

du rôle crucial de la cyberdéfense. Ainsi, elle appartient au « cœur de souveraineté » avec d'autres fonctions comme par exemple la dissuasion nucléaire, la fonction renseignement, les forces spéciales. Ceci explique la dimension étatique de cette cyberdéfense, articulée autour d'un dispositif à deux étages.

*L'ANSSI, acteur central*

Ainsi, le rôle de l'ANSSI est central. Ce service dépend du Secrétariat général à la défense et la sécurité nationale (SGDSN) et à ce titre du Premier ministre. Il s'agit donc d'une fonction interministérielle. Alors que le SGDSN était responsable, au cours de la guerre froide, de l'animation interministérielle de la défense (défense civile, défense économique…), cette dimension s'est fortement atténuée depuis 1990. C'est pourquoi la cyberdéfense, qui constitue un domaine transversal par nature, entre très bien dans le champ de compétences du SGDSN qui a trouvé là une évolution à sa mesure.



L'ANSSI est responsable, on l'a vu, de la cyberdéfense de niveau étatique. Cela entraîne plusieurs responsabilités. La première consiste à animer les actions des ministères régaliens : celui de la Défense, sur lequel nous reviendrons, mais aussi celui de l'Intérieur (Direction générale de la sécurité intérieure, gendarmerie nationale) et celui de l'Économie (douanes). Il s'occupe ensuite de développer la protection des « opérateurs d'importance vitale » (OIV) qui sont fixés par décret. La France adopte en la matière une approche particulière. À l'étranger, on utilise fréquemment la notion d'« infrastructure critique », sous-entendant que l'essentiel repose sur les « infrastructures », certaines étant « critiques », d'autres pas. La France utilise quant à elle la notion d'OIV. On discerne là une double singularité. Peu importe au fond « l'infrastructure », ce qui compte est « l'importance vitale », c'est-à-dire le service rendu au fonctionnement quotidien de la notion. La deuxième est organique puisqu'elle repose sur l'identification d'opérateurs, quels que soient leurs statuts (administrations, secteur public, entreprises privées). Au fond, il s'agit de pointer les responsabilités. Cette double approche évite de vouloir décrire les « infrastructures critiques » : sont OIV les agents désignés comme tels par un décret. Celui-ci est classifié, mais on comprend aisément que le réseau d'énergie nucléaire, les réseaux d'énergie ou les services d'urgence

et de santé entrent dans la liste. Ainsi, la démarche française est-elle très pragmatique. L'ANSSI et ces OIV collaborent donc étroitement pour protéger l'ensemble des réseaux informatiques concernés (incluant évidemment les systèmes informatiques essentiels de l'État), ce qui recouvre une complexité extrême.

L'ANSSI est enfin responsable de la défense économique en lien avec les initiatives contemporaines de « défense économique » comme l'intelligence économique ou la protection des agents économiques de souveraineté.

*Le ministère de la Défense*

À côté de l'ANSSI, un acteur joue un rôle central, il s'agit du ministère de la Défense. Traditionnellement, les armées ont pour mission d'assurer en tout temps et toutes circonstances la défense du territoire et de la population, pour reprendre la vieille expression de l'ordonnance de 1959 (qui a malheureusement disparu du droit positif). Si les armées ont un rôle évidement prééminent, on ne peut réduire leur rôle en matière cyber à l'action du seul officier général cyberdéfense. Il faut en effet mentionner deux autres acteurs ou types d'acteurs dépendant du ministre de la Défense.

Le premier est la délégation générale à l'armement (DGA) qui est chargée, pour l'État, de prescrire et contrôler le déroulement des programmes d'armement. De ce point de vue, la DGA a une première mission de dialogue avec l'industrie spécialisée en la matière, mais elle développe aussi dans ses laboratoires un certain nombre d'outils de très haute facture technologique indispensables à la panoplie française.

Il faut également mentionner l'ensemble des services de renseignement. Il peut s'agir de la Direction du renseignement militaire (DRM) qui dépend du chef d'état-major des armées (CEMA) comme l'OG cyber ; il s'agit aussi des services spécialisés comme la Direction générale du renseignement extérieur (DGSE), responsable du contre-espionnage, ou la Direction de la protection sécurité de la défense (DPSD) et de la responsable de la contre-ingérence. Tous ces services sont évidemment très discrets et on peut difficilement décrire leur activité exacte en matière de cyberdéfense. La DGSE a été régulièrement mentionnée au moment de l'affaire Snowden[7].





[7] Voir Quentin Michaud, *Edward Snowden, une rupture stratégique*, Économica, à paraître en novembre 2014.

## *Une posture internationale*

Ce dispositif vise à construire la souveraineté cyber. Celle-ci s'exprime au travers d'une posture internationale. D'un mot, on peut la caractériser comme étant occidentale mais marquant une indépendance discrète.

### *Aux côtés des Occidentaux*

Le caractère occidental ne surprendra personne car il est conforme à la politique française depuis de nombreuses décennies. Cette position fut particulièrement visible lors du sommet de Dubaï, en décembre 2012, à l'occasion du sommet de l'Union internationale des télécommunications. Alors, deux visions s'affrontaient sous le prétexte de la révision ou non du vieux règlement international des télécommunications. Certains pays, conduits notamment par la Russie et la Chine, souhaitaient l'adoption d'un traité international de régulation du cyberespace. En plaçant le domaine sous la tutelle de l'ONU et donc en permettant à tout État d'agir comme bon lui semblait, un tel traité autorisait en fait une régulation nationale de l'Internet et officialisait par là la possibilité de contrôle et donc de censure de celui-ci. Un autre camp était conduit par les États-Unis et affirmait la pérennité du système actuel, en favorisant un Internet transparent et libre. Certes, la question s'était nouée symboliquement autour de la tutelle de l'ICANN, l'organisme qui est responsable de l'attribution des noms de domaine de l'Internet : comme il est placé sous la tutelle (distante, il faut bien le constater) du département américain du Commerce, les opposants avaient beau jeu de dénoncer une absence de « liberté ». La France, comme la plupart des pays européens, soutint Washington et cette solution fut celle finalement retenue par défaut.



L'affaire est significative, non pas tellement par l'importance de la décision de Dubaï (en effet, limiter la question de la gouvernance du cyberespace à la seule tutelle de l'ICANN est très réducteur), mais parce qu'elle manifesta les positions politiques en présence. De ce point de vue, la France se rangea sans hésiter dans le camp occidental.

### *L'Europe et l'Otan*

De même, la France adopte sans surprise une position européenne cherchant à collaborer avec certains de ses voisins ou

à développer un cadre européen de régulation. On peut toutefois discerner quelques nuances. En particulier, l'étude d'un des derniers documents publiés, le pacte de cyberdéfense présenté par Jean-Yves Le Drian, permet d'illustrer les dimensions de cette attitude.

L'axe 5 du pacte cyberdéfense s'intitule ainsi : « cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance Atlantique et dans les zones d'intérêt stratégique ». Il précise : « Pour assurer la cyberdéfense de son territoire et de ses forces face aux menaces mondiales et provenant d'acteurs étatiques ou non, elle doit bâtir des coopérations pour échanger des informations et éventuellement coordonner ses actions dans le cyberespace » : on le voit, la stratégie est minimale puisqu'on n'évoque qu'échange d'informations et coordination des actions, mais rien qui n'aille vraiment plus loin, du moins officiellement.

Les partenaires possibles sont décrits : « Au premier rang de ses partenaires se trouvent naturellement les États membres de l'Union européenne et les États alliés de l'Otan. Mais d'autres États des zones d'intérêt stratégique – notamment au Moyen-Orient ou dans le Pacifique – sont également des partenaires à rechercher. Toutefois, les coopérations les plus approfondies imposent un haut degré de confiance et des capacités techniques développées qui restreignent le cercle des partenaires potentiels. »



Le cadre multilatéral européen n'est évoqué en matière cyber qu'autour de la structuration d'une industrie européenne de cybersécurité. Par exemple, dans le pacte de cyberdéfense, l'action 26 ambitionne « de développer les solutions de souveraineté tout en mutualisant au niveau européen la R&D qui peut l'être, par exemple dans le domaine de la sécurité des systèmes industriels ». En fait, la France attend plus de l'Europe de définir un cadre de droit que de fournir réellement une cyberdéfense. Elle a ainsi soutenu l'adoption de la stratégie européenne de cybersécurité, en 2013, car elle y voit le moyen d'inciter nombre de partenaires à faire des efforts en la matière (ce qu'exprime l'action 39 du pacte qui vise à « soutenir la prise en compte de la cybersécurité comme priorité européenne d'abord pour les institutions elles-mêmes et également pour les États membres »). Ainsi, l'action 38 du pacte déclare que « L'Union européenne reste quant à elle le cadre naturel du développement de la cybersécurité collective de nos infrastructures critiques. Le ministère de la

Défense, en lien avec l'ANSSI et le ministère des Affaires étrangères, s'attachera à renforcer la prise en compte de la cyberdéfense de toutes les organisations militaires de l'Union européenne et des opérations militaires sous commandement européen ». L'action 40 affirme quant à elle qu'« une base industrielle européenne doit progressivement être élaborée afin d'assurer à terme la cybersécurité des programmes conduits par l'Union européenne, et en particulier par l'Agence européenne de défense ».

L'Otan constitue l'alliance militaire qui constitue un cadre naturel d'action. Le pacte précise toutefois : « S'agissant de l'Alliance Atlantique, le soutien de la France à la prise en compte de la cyberdéfense comme enjeu stratégique est total. La protection des infrastructures de l'Otan elle-même et la cyberdéfense des forces en opération sont les deux objectifs majeurs. En cas de crise cyber particulièrement grave qui affecterait un de nos alliés, nous assumerions naturellement nos responsabilités en l'assistant de notre mieux ». La cyberdéfense de l'alliance paraît, ce faisant, cantonnée à la protection des seuls réseaux alliés (donc pas ceux des États membres, responsabilité qui demeure nationale) et des réseaux déployés dans les opérations de l'alliance : la lecture est donc assez minimale puisqu'il s'agit de promouvoir l'interopérabilité des forces (action 42) et le partage d'informations sur les menaces (action 43).



*Coopérations bilatérales*

Ainsi, la France semble privilégier un cadre plutôt bilatéral qui lui semble plus pertinent, dans l'état actuel des choses, que le cadre multilatéral. Il s'agit bien d'« engager et approfondir des coopérations bilatérales mutuellement profitables avec nos alliés dans les domaines opérationnels, techniques et industriels », comme les décrivent les actions 36 à 38. L'action 41 précise par exemple que « le soutien de nos partenaires européens proches comme le Royaume-Uni et l'Allemagne sera recherché, mais aussi celui des nations comme l'Estonie et la Belgique ». Royaume-Uni et Allemagne avaient déjà été évoqués dans le *Livre blanc*. Cela semble indiquer que la France entend développer des relations avec ceux qui conduisent des efforts certains en matière de cyberdéfense, comme l'indique l'action 37 qui parle d'« approfondir les coopérations avec les alliés les plus présents

dans le cyberespace pour améliorer notre vision commune des menaces, anticiper les attaques et travailler en commun à leur solution ». L'ordre choisi, non alphabétique, n'est pas anodin : il traduit non une priorité politique mais semble plutôt indiquer une priorité technique.

Curieusement, les États-Unis ne sont pas cités comme tels dans le pacte cyberdéfense qui y fait une très discrète allusion en évoquant seulement les « États alliés de l'Otan ». Ce silence traduit une sorte de gêne, d'autant que l'on sait, depuis les révélations de l'affaire Snowden, que la France a développé des relations assez approfondies avec les États-Unis, sans pour autant entrer dans un système d'alliance quasi intégrée comme a pu choisir de le faire le Royaume-Uni. Plusieurs raisons expliquent cette attitude.

D'une part, on peut y retrouver l'écho de la traditionnelle posture française d'indépendance et de souveraineté, même si cela s'éloigne d'un anti-américanisme qui a pu motiver certaines attitudes du passé. En fait, la France partage aujourd'hui beaucoup avec les États-Unis et notamment une certaine vision de responsabilité mondiale (à la différence de nombreux États européens, la France ne se désintéresse pas stratégiquement du reste du monde), tout comme l'utilisation récurrente des outils de puissance, notamment militaires, pour contribuer à résoudre les crises. Ainsi, Américains et Français se sont-ils régulièrement retrouvés sur les théâtres d'opération, ce qui crée des liens. La France, qui est devenue la première puissance militaire du continent, est également devenue un allié très solide de Washington.



D'autre part, on peut y voir une sorte de pragmatisme face à la domination technique du cyberespace par les Américains. L'idée consiste à coopérer afin de progresser et donc d'augmenter ses propres capacités, partant sa propre indépendance. Autrement dit, il ne s'agit pas de s'aligner mais de progresser grâce à la concurrence technique. Le chemin est évidemment subtil et délicat à mettre en œuvre et justifie peut-être la discrétion retenue. Il n'est pas tout à fait nouveau si l'on se souvient que les recherches françaises en matière nucléaire bénéficièrent en leur temps d'un soutien scientifique indirect de la part des Américains, ce qui est peu connu.

## *Cyberconflictualité et guerre économique*

La France a depuis quelques années été victime d'un certain nombre d'agressions. Ainsi, le constructeur nucléaire Areva

a-t-il fait l'objet d'une attaque massive à l'automne 2011. On se souvient de même de l'attaque contre le ministère des Finances, en mars 2011, qui a suscité une véritable prise de conscience parmi les responsables de l'État. Citons également l'espionnage de l'Élysée, intervenu au moment de l'élection présidentielle de 2012.

*Cyberconflictualité et discrétion*

Il ne s'agit pas ici de faire l'inventaire de tous les cas de cyberagressions, simplement de constater que la France n'est pas épargnée, même si elle communique moins sur ces affaires.

Ainsi s'explique peut-être la discrétion adoptée au moment de la révélation de l'affaire Snowden. Le scandale initial retomba dans l'oubli, les autorités faisant quelques déclarations de fermeté sans vraiment prendre de décisions. On peut y voir deux raisons : d'une part, le fait que « tout le monde espionne tout le monde » et qu'il s'agit en fait d'une pratique déplaisante mais inévitable ; d'autre part, la collaboration américaine susmentionnée interdisait une dénonciation trop vigoureuse. Ces affaires étaient discrètes et la France n'avait nulle envie qu'on commence à trop s'intéresser à ces affaires secrètes. Les révélations sur Frenchelon (un dispositif d'espionnage électronique organisé par la DGSE), plus tard sur « Babar » et « Lustre » (qui seraient des dispositifs français d'espionnage), voire sur l'écoute d'un certain nombre de câbles gérés par l'opérateur Orange constituaient autant de fuites qu'il fallait éviter. Autrement dit, si cette interprétation est la bonne, le scandale était certes déplaisant, mais le réalisme politique commandait un profil bas, d'autant que l'opinion française ne semblait pas accorder une si grande importance à la chose, à la différence de ce qui se passait en Allemagne ou au Brésil.



*Cyber et guerre économique*

Une autre dimension paraît toutefois importante à souligner. À l'instar des grands acteurs du cyberespace (États-Unis bien sûr mais aussi Israël, Chine, Russie…), la France cherche à développer une autonomie technique et industrielle. Cela relève bien sûr de la guerre économique, mais participe aussi du développement d'une « base industrielle et technologique de cyberdéfense ». Un certain nombre d'acteurs jouent un rôle majeur comme Alcatel, Thalès, Bull, Airbus cyberdéfense, ST Microélectronics. Des initiatives

comme Vepsen ou le développement d'un antivirus français vont également dans ce sens avec le soutien discret de l'État.

## Conclusion

Même si la France disposait d'atouts préalables, elle a su les exploiter en bâtissant une véritable stratégie de cyberdéfense. Initiée en 2008, renforcée depuis 2012, elle vise à établir un dispositif assez complet qui permette de protéger un aspect désormais essentiel de la souveraineté nationale.

Les critiques pourraient lui reprocher d'être incomplet : mais ils se réfèrent pour cela à un modèle américain dont la domination du cyberespace est encore évidente. De ce point de vue, la France réussit à construire un dispositif cohérent et fiable bien qu'il soit encore perfectible. À tout le moins ne peut-on pas reprocher l'absence de conscience du problème ni les efforts réalisés, dans un contexte général de pénurie financière. Compte tenu de cet environnement, le résultat est satisfaisant et place la France dans le peloton des nations qui comptent dans le cyberespace.



***Résumé :***
À partir de 2008, la France a décidé de rattraper son retard initial en matière de cyberdéfense afin de maîtriser ce nouvel espace qui appartient désormais au premier cercle de la souveraineté au même titre que la dissuasion nucléaire, les missiles balistiques ou les sous-marins nucléaires. La France doit développer une capacité de lutte dans cet espace – maillage de l'ensemble des réseaux – tant offensive que défensive. La prise de conscience et les efforts sont certains.