Le Ministère de la défense a présenté récemment son « Pacte Défense Cyber », un plan d'action en 50 points pour cadrer ses actions en matière de cyberdéfense. Jusqu'ici, rien de plus normal, il s'agit évidemment d'un enjeu d'importance cruciale. Toutefois, ce qui retient immédiatement l'attention, c'est la tension (voire contradiction) entre d'une part l'impératif de souveraineté dans ce domaine hautement stratégique et, de l'autre, l'insistance du Pacte sur des cadres de coopération internationale où, c'est le moins que l'on puisse dire, les partenaires de la France ne partagent pas forcément ce souci.

Un sujet de souveraineté par excellence

Le dernier **Livre blanc** reconnaît *« la sécurité des systèmes d'information »* comme *« composante essentielle de la souveraineté nationale »*. Une vision exprimée aussi par le ministre de la défense Jean-Yves Le Drian, dans son **discours à Rennes** en juin dernier, en ouverture d'un colloque sur la cyberdéfense. Le risque *« c'est désormais l'atteinte aux intérêts stratégiques de l'Etat et à notre autonomie d'appréciation, de décision et d'action, par la menace cyber. C'est un enjeu majeur de défense et de souveraineté de la Nation »*.

Patrick Pailloux*, ancien directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), parle même de la *« souveraineté de la souveraineté »*. Pour lui, *« Si nous ne sommes pas capables de protéger nos propres données, le reste ne sert à rien. À quoi servirait de concevoir entièrement par nous-mêmes des systèmes de défense placés sous notre contrôle exclusif si nous sommes impuissants pas ailleurs à assurer leur protection ? (...) Il s'agit de conserver la capacité – que la France avait par le passé – de protéger ses informations de manière autonome. »*

Compte tenu des enjeux de souveraineté, la question des coopérations est un sujet délicat d'emblée. En faire l'un des six « Axes » du Pacte, en précisant qu'au premier rang des partenaires potentiels *« se trouvent* naturellement *les Etats membres de l'Union européenne et les Etats alliés de l'OTAN »* a de quoi étonner, en particulier à la lumière des révélations de **l'affaire Snowden/NSA**. Mais même si on fait abstraction de cet énorme « éléphant dans la salle », l'idée de trop miser sur l'une ou l'autre enceinte serait au mieux naïve, au pire carrément néfaste.

Coopération cyberdéfense dans l'OTAN ?

Le Pacte prévoit de *« s'engager à l'OTAN pour garantir la résilience de l'organisation en cas de crise cyber et les capacités des forces alliées en opération »*. Mais cette approche pragmatique et restrictive de la France se heurte, du côté de l'OTAN, à un véritable projet politique. Lequel projet voit dans le cyber un nouveau domaine où il convient d'asseoir le droit de regard de l'organisation au plus vite possible. C'est écrit noir sur blanc dans **le rapport annuel 2013 du Secrétaire général** de l'Alliance : *« Bien que le rôle principal de l'OTAN dans le domaine cybernétique soit de défendre ses propres réseaux, en 2013, l'Alliance a élargi ses activités à la lutte contre les cybermenaces »*.

Ce qui implique d'être *« mieux préparée à prêter assistance à des pays membres ou partenaires de l'Alliance lorsqu'il s'agit de détecter une cyberattaque, d'assurer la défense contre une telle attaque ou de rétablir le fonctionnement normal des réseaux »*. L'OTAN se porte donc volontaire pour reprendre à son compte, en principe, une large part du fardeau que constitue, pour les Etats membres, leur propre cyberdéfense. Dans cet esprit, les références au fameux Article 5 (de « défense collective ») dans le contexte d'éventuelles cyberattaques se font de plus en plus fréquentes. Reste à définir quel type d'interférence OTAN/US on tente de justifier cette fois-ci derrière ce paravent.

Le Pacte semble confirmer que la France souhaite s'en tenir à ce que l'Article 5 prévoit *stricto sensu* en cas d'agression armée : une assistance volontaire sur décision nationale (*« en cas de crise cyber particulièrement grave qui affecterait un de nos alliés, nous [la France] assumerions naturellement nos responsabilités en l'assistant de notre mieux »*). Ce qui limiterait fort heureusement le droit de regard de l'Alliance. Et serait donc plus conforme à la position traditionnelle de Paris, laquelle s'efforce de cantonner l'OTAN à la protection de ses propres réseaux et des forces en déploiement. C'est déjà assez de pain sur la planche, manifestement.

D'après le contre-amiral Coustillière, en charge de la cyberdéfense à l'état-major des armées, alors même que l'Alliance se dit prête et compétente pour relever le défi de la cyberdéfense dans son ensemble, la seule protection des propres réseaux de l'Alliance *« est toujours une question en suspens »*. *« Les effets d'annonce [de l'OTAN] masquent en réalité des capacités réduites »*. Telle cette fameuse équipe d'intervention rapide, dotée de seulement 6 personnes au moment où le Secrétaire général Rasmussen la présenta comme le signe d'une Alliance en phase avec les « nouveaux défis ».

Toujours est-il que ces capacités-mirages ne sont pas sans danger. Pour les uns, elles servent d'alibi pour se reposer sur leurs lauriers, pour les autres elles permettent de bloquer toute initiative européenne en la matière, sous prétexte de « duplications inutiles ». Or si les Etats européens se rechignent à faire les efforts nécessaires pour mettre en place leurs propres capacités nationales et que l'Union européenne est écartée du jeu soi-disant pour éviter une compétition stérile, l'OTAN finira par rester effectivement seule sur la piste. Et elle pourra alors se présenter réellement comme unique recours possible, avec toutes les conséquences que cela implique.

La coordination cyber sur les théâtres d'opération est un autre casse-tête pour l'OTAN. Comme en témoigne les premières initiatives, très peu probantes, en Afghanistan. Pour l'exemple, le système permettant l'échange des emails entre les forces US et alliés en Afghanistan fut tellement lourd que quand il est tombé en panne personne ne s'en est aperçu pendant 35 jours. Vinrent alors les Britanniques avec leur idée géniale de faire des enclaves individuelles à l'intérieur d'un seul et même système sous contrôle central. Laquelle idée résolut certes les problèmes d'interopérabilité, mais n'aurait laissé quasiment plus de place aux systèmes sous contrôle national.

Finalement, en 2010, l'OTAN opte pour une démarche pragmatique. D'après Jean-François Ripoche, « architecte Commandement et maîtrise de l'information » à la DGA, *« L'Afghan Mission Network, en Afghanistan, avait assez bien réussi à cantonner les problèmes de sécurité*

de l'information à certaines interfaces, avec des passerelles d'accès à des réseaux, l'OTAN défendant ses réseaux pendant que les nations défendaient les leurs ». De l'avis général, c'est ce modèle qui devra servir de base pour les opérations futures. Reste à voir si la recherche de toujours plus d'interopérabilité ne devienne pas un prétexte pour s'ouvrir, s'aligner, voire se soumettre aux systèmes (et aux concepts) américains au final.

D'autant plus que, pour les Etats-Unis (et leurs acolytes euro-atlantistes), l'Alliance est un levier d'influence trop bien rôdé pour ne pas la mettre au profit en matière de cyberdéfense aussi. D'où leur intérêt pour **le centre d'excellence de Tallin**. Le Pacte du Ministère peut toujours rêver à *« forger une pensée stratégique et opérationnelle française en cyberdéfense »*, qui s'enrichisse *« des échanges avec nos alliés proches »*. Vu que la France est désormais membre à part entière de l'OTAN (elle a même rejoint le Centre l'an dernier), le risque de *« phagocytage conceptuel et théorique »* (pour reprendre les mots du **dernier Rapport Védrine**) est devenu bien trop flagrant.

Contre-amiral Arnaud Coustillière. Crédit photo : Stéphane Gaudin

Le contre-amiral Coustillière ne cache pas que, par exemple, *« le centre de Tallin subit une forte influence des conceptions juridiques américaines sur la défense préemptive »*. Dont il conclut qu'*« y apporter un peu de droit européen serait des plus souhaitables »*. Idem pour tout ce qui touche aux scénarios, à la planification, à l'analyse des menaces. Certes, l'idéal serait, comme l'avait écrit Védrine, *« d'influencer utilement la pensée de l'OTAN, sans se fondre dans celle-ci »*. N'empêche qu'il s'agit là d'un numéro d'équilibriste que nul n'a réussi jusqu'ici (à part, bien sûr, les Etats-Unis…).

L'activisme de l'OTAN en matière de cyberdéfense engendre donc des risques sur tous les plans : qu'il s'agisse de rassurances factices (qui encouragent les Européens à encore plus de déresponsabilisation), d'engrenages pratiques (lesquels feraient de l'exigence d'interopérabilité un prétexte pour pousser vers des solutions de plus en plus centralisées, sous l'égide de Washington) ou de « phagocytage » conceptuel (sans doute le plus pernicieux de tous, puisqu'il nous priverait, à terme, de toute analyse et de réflexion autonomes) ; la plus grande vigilance est donc de mise quant à l'Alliance atlantique. Un constat qui devrait normalement revaloriser le rôle de l'UE, comme enceinte de coopération véritablement européenne en matière cyber. Sauf que c'est loin, très loin, d'être acquis.

Coopération cybersécurité dans l'UE ?

S'agissant de l'Union européenne, la France cherche à *« soutenir la prise en compte de la cybersécurité comme priorité européenne d'abord pour les institutions elles-mêmes et également pour les Etats membres »*. Le Pacte déclare aussi que *« l'Union européenne reste quant à elle le cadre naturel du développement de la cybersécurité collective de nos infrastructures critiques »*. Paris tient aussi à *« promouvoir les solutions européennes de cybersécurité »,* de même que *« la cyberdéfense militaire »* au sein de l'UE. Une fois de plus, on se retrouvera donc vite face à la concurrence OTAN-Union européenne. Et la France semble toujours y privilégier, si possible, les solutions proprement européennes.

Hélas, force est de constater que même la protection des propres réseaux de l'UE soulève des questionnements. Pour rappel : le journaliste Jean Quatremer sonna l'alarme dès 2001 (dans une **série d'articles**), en pointant du doigt les propos du responsable du cryptage à la Commission de Bruxelles. Notamment la fameuse phrase : *« J'ai toujours eu de très bons contacts avec la NSA à Washington. Elle vérifie régulièrement nos systèmes (de cryptage) pour voir s'ils sont bien verrouillés et s'ils sont correctement utilisés. »* Et la NSA s'y emploie, sans aucun doute, dans un esprit tout à fait amical… Surtout qu'il s'agit, pour les Etats-Unis, des communications confidentielles d'une organisation qui est, sur de nombreux dossiers, leur plus formidable rival commercial.

Il n'est pas non plus tout à fait anodin que le responsable en question, M. Perkins est de nationalité britannique. Si le Royaume-Uni est un Etat membre de l'UE (jusqu'aux dernières nouvelles), il fait aussi partie intégrante du club des « Cinq yeux » (ou *Five Eyes* UK, USA, Canada, la Nouvelle Zélande et l'Australie) au sein duquel il espionne ses partenaires européens depuis des décennies pour le compte des cousins anglo-saxons. Comme en témoignent les nombreuses enquêtes et révélations autour du réseau Echelon.

Les responsables US sont par ailleurs régulièrement invités à participer aux réunions du Joint Intelligence Committee britannique, organe coordinateur des services de renseignement de Sa Majesté. Normal. Les Etats-Unis **financent en partie lesdits services**, en même temps qu'ils **fixent une partie de leurs priorités**. Par contre, les « partenaires » européens de Londres sont tous tenus strictement à l'écart de ce saint des saints du partage des informations entre initiés. Normal aussi. Ils en sont en partie les cibles.

Rien n'est plus illustratif de l'atmosphère surréaliste en Europe, résultant du double jeu britannique, que le sommet « cybersécurité » en octobre dernier où se sont réunis les chefs d'Etat et de gouvernement des 28. Parmi eux, le Premier ministre britannique a pris sa place comme à l'accoutumée, alors même que **les grands titres de la presse** faisaient état de la coopération entre la NSA et son gouvernement pour espionner l'Italie, et que la **Chancelière Merkel** ne s'est pas encore remise du choc d'apprendre que son portable personnel était également surveillé par des oreilles amies. C'est dire les limites de l'exercice.

Ceci étant, l'UE aurait tout de même du potentiel en matière cyber. De par sa compétence normative, l'Union européenne se fait déjà active, avec **sa stratégie de cybersécurité** publiée en février 2013, suivie d'une proposition de directive. Celle-ci prévoit des mesures concrètes pour assurer un niveau élevé de sécurité pour des réseaux informatiques dans l'Union, y compris l'obligation pour les opérateurs critiques et pour les administrations de signaler les incidents (un pas indispensable, mais difficile à franchir de peur de perdre la face et/ou des clients).

D'une manière plus générale, l'Union pourrait, et devrait en principe, explorer de nombreuses pistes afin de lutter contre l'espionnage informatique (identifié comme l'une des menaces principales par les experts cyber, et largement médiatisé à la suite de l'affaire Snowden). D'après Mark Leonard, directeur du think-tank *European Council on Foreign Relations*, **ces pistes pourraient comprendre** des mesures pour faire payer des amendes record à n'importe quelle société de l'informatique qui transmettrait des données sur les citoyens européens à une agence de renseignement étranger ; de même que (à l'instar de Galieo, le

système de navigation par satellites) la prise en charge financière d'une partie du développement de centres de données « cloud » (nuage) européens.

Ce qui nous amène aux aspects technologico-industriels. Dès son préambule, le Pacte du Ministère affiche son plein *« soutien au développement d'une industrie nationale et européenne de cybersécurité »*. Ce qui est fort heureux. A condition, toutefois, de bien faire la distinction entre les deux. Si, au prime abord, la dimension européenne s'impose comme une évidence pour échapper aux dépendances extérieures, ce serait sans compter avec les partenaires européens de la France et leurs politique à courte vue.

Pour eux, l'idée même d'une quelconque préférence européenne reste un tabou, et taxée d'anti-américanisme primaire, dans toute discussion relative à la base technologique et industrielle. Ce qui rend **le schéma des trois cercles** en grande partie illusoire. La frontière entre le cercle européen et le cercle mondial n'a pas vraiment de sens, dès lors que les Européens se refusent à protéger leurs atouts vis-à-vis d'autres puissances. Or s'engager dans des rapports d'interdépendance avec des partenaires dépendants et ouverts à tous les vents revient au même que d'accepter soi-même une position de vulnérabilité et de dépendance.

Le problème, c'est que l'Europe est le seul moyen pour empêcher que la défense cyber ne devienne un nouveau « parapluie » fictif USA/OTAN pour légitimer leur mainmise. Comme l'a fait remarquer Guillaume Poupard, responsable du pôle de sécurité des systèmes d'information à la DGA, beaucoup de pays européens *« ont déjà renoncé, et veulent être protégés plus qu'ils ne veulent prendre en main leur propre cybersécurité. C'est contre cette attitude qu'il faut aller en leur faisant prendre conscience que beaucoup peut être fait au niveau européen »*. Par opposition, entendons-nous bien, à des structures américano-otaniennes. A la condition que cela ne soit pas finalement du pareil au même.

* Patrick Pailloux a été nommé directeur technique de la DGSE à compter du 1er mars 2014

Lectures annexes :

- **Audition du contre-amiral Arnaud Coustillière** à la Commission de défense nationale et des forces armées de l'Assemblée nationale (12 juin 2013)
- **Rapport d'information** du Sénat sur la cyberdéfense (juillet 2012)
- **Cybernétique : sortir du piège américain**, de Véronique TRUONG *(avocate, spécialiste du droit de la propriété intellectuelle),* article paru dans la Revue Défense Nationale n°768 de mars 2014
- **Le contrat « open bar » entre Microsoft et la Défense sous le prisme du Sénat** (PC INpact, 27 février 2014)
- **Alcatel-Lucent : un allié très écouté de la NSA**, d'Emmanuel PAQUETTE paru sur le site de l'Express le 30 octobre 2013)
- **Les câbles sous-marins : clés de voute de la cybersurveillance**, de Maxime VAUDANO (Le Monde, 6 septembre 2013)
- Cyber : la guerre a commencé (Revue Sécurité Globale n°**23** et **24**, printemps-été 2013)
- **Au coeur de la cyberdéfense** : Magazine DSI Hors-Série n°32
- **L'Observatoire du FIC** (Forum International de la Cybersécurité)
- **Les actes** du colloque FIC 2013

- **Attention : Cyber ! Vers le combat cyber-électronique**, Aymeric Bonnemaison et Stéphane Dossé (Editions Economica
- **Le cyberespace – Nouveau domaine de la pensée stratégique**, Stéphane Dossé, Olivier Kempf, Christian Malis (Editions Economica)
- **Cybertactique : conduire la guerre numérique**, Bertrand Boyer (Editions Nuvis)