Intervention du Général de division Eric Bonnemaison,

directeur adjoint de la Délégation aux affaires stratégiques
au Forum International de la Cybersécurité – FIC 2013

LE CONTINUUM DÉFENSE-SÉCURITE DANS LE CYBERESPACE

28 janvier 2013

- seul le prononcé fait foi -

Le continuum sécurité défense est une idée assez ancienne. On pourrait remonter au moins au début du XXème siècle avec l'instauration de l'ancêtre du SGDSN qui assurait déjà une coordination civilo-militaire de la défense nationale. Dès la naissance de la Vème république, il a été clair que la sécurité et la stabilité de la France ne dépendaient pas seulement des forces armées mais également de ses forces de police et de sa structure sociale, politique, économique et éducative. L'ordonnance de 1959 a donné une définition assez large de la **défense nationale**, dite **"globale",** qui regroupait la défense armée, la défense civile, chargée de la protection de la population, de l'ordre public et des institutions, de la défense économique, et de la défense culturelle pour maintenir l'esprit civique et les valeurs républicaines.
Le Livre Blanc de 2008 a quant à lui distingué le concept de sécurité nationale de celui de défense, peut-être pour permettre de mieux discuter ensuite les termes de leurs rapprochements. On a ainsi vu émerger une "stratégie de sécurité nationale" assez novatrice car visant à mettre en cohérence les différentes politiques publiques (dont la politique de défense) au service de la "résilience" de la Nation et des pouvoirs publics, mais aussi de ses intérêts à long terme.
Le Livre Blanc de 2013, en cours de rédaction et qui reste à approuver par le Président de la République, pourrait remettre en avant ce concept de stratégie de sécurité nationale qui modernise le concept de défense globale, sans véritablement remettre en cause ses fondements.
Parfois les différences entre sécurité et défense peuvent être claires: tout le monde voit bien à quel registre appartiennent la police de la route et la dissuasion nucléaire. Parfois, la frontière est plus floue et c'est typiquement le cas du cyber.
Plus encore que pour les autres domaines, pour les forces armées, **le cyber représente pour la défense un défi stratégique qui doit être pensé dans un cadre plus englobant que les seules opérations militaires**.

En effet, le cyber introduit des nouvelles vulnérabilités pour les forces armées

Les évolutions des forces armées modernes ont conduit à accélérer la boucle OODA: Observation, Orientation, Décision, Action de John Boyd. L'idée est qu'une armée efficace doit décider vite et bien pour appliquer le bon effet au bon endroit. Elle frappe les capteurs de l'adversaire, ses centres de décision ou ses moyens d'action. Elle le rend ainsi de plus en plus lent à décider et agir et, finalement, le conduit à la paralysie et à la défaite. Les armées ont ainsi été conduites à développer des systèmes de commandement et de contrôle (C2) de plus en plus sophistiqués pour lever autant que possible le brouillard de guerre, décider et agir en quasi temps réel. Au final, il s'agit de substituer aux stratégies d'attrition des frappes précises aux endroits qui font vraiment mal.
Ces systèmes C2 vont maintenant jusqu'aux plus bas niveaux tactiques: par exemple jusqu'aux fantassins avec le système Felin qui les transforme en soldats-capteurs communicants. Ils nécessitent

des réseaux haut-débit en métropole et sur chaque théâtre d'opération. Ils nécessitent de puissants systèmes de traitement de l'information.

Or, il faut admettre que les forces armées utilisent pour ces systèmes des versions plus ou moins améliorées des systèmes qu'on peut trouver dans le civil. Les protocoles sont basés sur l'IP, les postes de travail sont massivement des PC, beaucoup de logiciels sont grand public. Bien sûr, les systèmes les plus critiques, en particulier les plus nécessaires à la dissuasion et aux opérations, sont spécifiquement protégés. Mais la défense peut être victime de toutes ces attaques pas forcément ciblées qui arrivent par internet et qui pourraient affecter la périphérie des systèmes de défense voire un peu plus.
Le cas typique est le virus *Conficker* en 2008: transféré depuis internet sur l'intranet de la défense par une clé USB, il a obligé à arrêter le réseau pour le dépolluer. Or ce réseau d'usage général supporte les applications de soutien des forces armées: la gestion des ressources humaines, la solde, la messagerie générale, la logistique… Il aurait donc pu y avoir des conséquences importantes.

A côté de ce bruit de fond cyber, la défense est bien entendu spécifiquement visée par des attaques ciblées. Il s'agit par exemple d'espionnage, de tentative de paralysie voire de destruction.
Le problème se pose avec acuité non seulement pour nos systèmes C2 mais aussi pour nos systèmes d'armes. En effet, toutes les plateformes de combat, que ce soient des bateaux, avions ou chars, embarquent massivement de l'électronique et de l'informatique. Certains systèmes sont assez spécifiques, comme le radar à balayage électronique, mais comportent des composants achetés sur étagère. D'autres sont quasiment identiques aux systèmes civils. Par exemple, quelle différence entre la chaufferie nucléaire d'un sous-marin et une centrale d'EDF? Quelle différence entre le SCADA qui pilote la propulsion d'une frégate et un SCADA utilisé dans l'industrie? Malheureusement pas assez…
La force des armées modernes, leur technologie, est donc également devenue une vulnérabilité. La cyberdéfense militaire s'intéresse donc à l'ensemble des systèmes utilisés depuis leur conception, leur réalisation, leur fabrication, leur exploitation opérationnelle mais aussi leur maintenance. Tous ces systèmes sont fortement dépendants de technologies et de prestataires civils voire étrangers.
Le routeur espionné par un industriel étranger, le SCADA attaqué par un hacker, le virus introduit, volontairement ou non, par un sous-traitant dans un sous-marin nucléaire, le ransomware paralysant le logiciel de paiement des soldes, toutes ces attaques qui pourraient ne relever que la cybercriminalité peuvent avoir un impact important, stratégique voire politique sur notre défense. Quel serait par exemple la crédibilité d'une dissuasion qui utiliserait des composants non maîtrisés ?

Le cyber est ainsi devenu un domaine stratégique où l'asymétrie est reine

En effet, pour le général Beaufre, le but de la stratégie est *"d'atteindre la décision en créant et en exploitant une situation entrainant une désintégration morale de l'adversaire, suffisante pour lui faire accepter les conditions qu'on va lui imposer."* **Puisqu'il s'agit de peser sur la volonté de l'adversaire, le cyber se révèle être un moyen de choix**. Il permet d'influencer directement la population de l'adversaire grâce à l'internet. Le cyber permet également de paralyser ou de désorganiser les secteurs clés, dans des proportions ajustables. Cela peut aller de la simple gêne, avec le déni de service par exemple. Mais cela peut aller jusqu'à une désorganisation brutale et durable de la société en frappant ses infrastructures critiques.
Tout ceci se prête magnifiquement au dialogue stratégique entre les Etats: ils peuvent gérer l'escalade et choisir d'éviter ou non "la montée aux extrêmes" clausewitzienne. Les Etats peuvent aussi décider d'avancer masqués, ce qui est plus facile dans le cyberespace que dans le monde conventionnel, et qui laisse place à toutes les manipulations imaginables.
Le cyber, en frappant des cibles civiles, par des moyens relativement limités, est ainsi une option stratégique qui intéresse tous les Etats.
Les Etats les moins avancés sont du reste les moins vulnérables aux cyberattaques et les plus intéressés par ce moyen d'un relatif faible coût. Une clé USB infectée peut faire plus de dégâts à un centre de commandement et de contrôle qu'une bombe de 250kg à précision métrique, sans compter les coûts cumulés de la frappe aérienne…
Ce pouvoir égalisateur du cyber permet ainsi au faible de frapper le fort là où il est faible et d'éviter de se confronter à lui sur son terrain conventionnel. Les Etats les plus puissants trouvent également dans le cyber un outil de basse intensité qui complète le spectre des effets. Le cyber ouvre même des possibilités d'actions subtiles contre des alliés.

Mais le cyber est surtout le domaine de lutte idéal pour des groupes non étatiques. Ces groupes peuvent manifester des motivations politiques ou être purement mafieux. Ils peuvent affronter à distance un Etat avec un rapport coût efficacité particulièrement avantageux. Mieux, tout l'ordre

international qui fixe les frontières et les rapports entres les Etats est à leur avantage puisqu'il gêne les poursuites en multipliant les obstacles juridiques et politiques.
Finalement, chaque individu peut se servir du cyberespace pour servir une cause et éventuellement porter atteinte à un Etat, le sien ou un autre. On a par exemple vu le glissement d'Anonymous: en défendant la liberté de l'internet, il s'est attaqué à des Etats pratiquant la censure. Mais il a aussi assumé son engagement contre Israël pour des raisons politiques. La France n'est pas épargnée par ce phénomène comme le montre actuellement les attaques informatiques liées au Mali.
La conception westphalienne des relations internationales, déjà battue en brèche par le terrorisme international, est fondamentalement remise en cause par le cyber. Avec cet outil, n'importe quel groupe déterminé peut contester la politique d'un Etat et tenter lui en faire changer sous peine d'atteinte grave à son fonctionnement.

Du point de vue du ministère de la défense, quelles sont les conséquences de multiplication des agresseurs potentiels ?

Le premier problème de la défense est d'essayer de faire le tri entre les actes relevant simplement de la cybercriminalité et ceux portant atteinte aux capacités des forces armées ou aux intérêts vitaux. Les malwares divers, les défaçages, les spams génèrent un bruit de fond cyber qui occupe inutilement des spécialistes et rendent plus difficile la détection des vraies attaques ciblées et dangereuses. Une coopération très étroite avec l'ANSSI est donc nécessaire pour mieux classifier la menace et choisir d'apporter la réponse appropriée: traitement judiciaire, diplomatique ou politique.
La défense profite donc de tous les efforts faits pour faire baisser la cybercriminalité: moins de citoyens tentés, moins d'outils disponibles en ligne, plus de dissuasion par la politique pénale.
La défense est aussi intéressée par la diminution des menaces qui pèsent sur les infrastructures critiques. Nul doute qu'une attaque réussie sur ces systèmes fragiliserait la société, obligerait probablement les forces armées à intervenir auprès des populations, obérerait une partie des capacités militaires, voire pourrait conduire à une escalade stratégique. Après tout, les Etats-Unis ont déjà annoncé qu'ils n'hésiteraient pas à riposter par tout moyen, y compris conventionnel, à une attaque cyber contre leurs intérêts vitaux. En France, la doctrine n'est pas aussi clairement établie mais le président de la République aurait toute autorité pour apprécier la réponse adaptée dans un tel cas.
Au niveau national, beaucoup a été fait, que ce soit au ministère de l'intérieur ou à l'ANSSI. Beaucoup reste sans doute à faire et le Livre Blanc proposera des pistes.

En revanche, au niveau international, rien n'a pratiquement été fait. La convention de Budapest ratifiée par la France impose à la trentaine d'Etats parties de coopérer contre la cybercriminalité. Cela n'engage que les signataires, tous des Etats occidentaux, et cela ne repose que sur la bonne volonté.
Des négociations sont conduites dans différentes enceintes pour améliorer la sécurité du cyberespace en essayant de prendre en compte cette confusion des acteurs. Mais les conceptions très différentes des Etats ne facilitent pas les choses: la définition d'un terroriste n'est pas exactement la même à Washington, Paris, Moscou ou Pékin. Alors si on cumule terrorisme et cyber…
Tous les Etats conviennent tout de même que c'est le manque de contrôle qui crée des opportunités pour les groupes non étatiques. Certains Etats n'ont pas encore introduit dans leur législation les cyber-infractions. D'autres ne peuvent pas les poursuivre par manque de moyens. D'autres ne veulent pas les poursuivre quand elles servent leurs intérêts. Pour mémoire, les attaques contre l'Estonie en 2007 avaient une vraie dimension stratégique: toute une société bloquée en signe de désaccord politique. Au final, la Russie a condamné un unique étudiant à une peine symbolique.

Tous les Etats conviennent également qu'il faut faire entrer le cyber dans le cadre classique des relations internationales, sous peine d'augmenter dramatiquement les comportements conflictuels.
Le cyber révolutionne en effet **le *jus ad bellum***, c'est-à-dire le droit qui détermine si on est en guerre ou non. Quelle attaque cyber pourrait être considérée comme une attaque armée? Faut-il des morts ou des destructions physiques pour donner le droit à la légitime défense prévue par l'article 51 de la Charte des Nations Unies? Est-ce qu'une paralysie de services essentiels à la vie de la nation est suffisante? Au-delà des conséquences, comment s'assurer de l'identité de l'agresseur? Est ce que le temps de mener l'enquête, par des moyens techniques ou de renseignement, ne laisse pas une fenêtre de vulnérabilité encore plus importante qui donne une vraie prime à l'agresseur?
Le *jus in bello*, c'est-à-dire le droit dans la guerre, est également à préciser. Qu'est ce qu'une riposte proportionnée? Comment d'ailleurs évaluer les dommages subis ou les dommages infligés? Qu'est ce qu'un dommage collatéral quand tous les systèmes sont interconnectés et peuvent servir à lancer une attaque cyber? Qu'est ce que le respect des Etats neutres quand le réseau mondial est interconnecté ? Qu'est ce qu'un combattant ou un non combattant à l'heure du cyber, quand n'importe

qui depuis chez lui peut participer à des cyberattaques contre les intérêts des Etats? Est-ce que la mère de famille et le retraité qui s'impliquent dans un conflit à l'étranger, comme on l'a vu en Libye ou en Syrie, qui lèvent des fonds, qui diffusent des renseignements classifiés, lancent des attaques en déni de service sont des cibles légitimes de l'Etat attaqué? Est-ce qu'ils pourraient être poursuivis si leurs actions participent à des crimes de guerre?

Le cyber est donc l'illustration du concept de continuum sécurité défense

De l'acte criminel aux opérations stratégiques, de la gêne à la destruction, de l'Etat au simple individu, le cyber embrasse tout le spectre des actions, des intentions et des conséquences. Il exige donc une réponse qui couvre tout le spectre et qui nécessite la mobilisation et la coordination de tous les acteurs de la société.
La défense y prend sa place, qui n'est pas hégémonique mais qui doit assumer son rôle particulier. En effet, selon le mot du général Georgelin, ancien chef d'Etat-major des armées: *"les armées doivent pouvoir encore fonctionner quand tout le reste s'est effondré".* Et cela est valable malgré le cyberespace et ces menaces, mais aussi grâce au cyberespace et à ses opportunités.