« Cyber Operations in DOD Policy and Plans: Issues for Congress ». CRS Report. Note de lecture.

Daniel Ventre, CNRS, Titulaire de la Chaire Cybersécurité & Cyberdéfense

22 janvier 2015, Article III.20

Catherine A. Theohary et Anne I. Harrington viennent de rédiger un court rapport (33 pages) publié par le Congressional Research Service (CRS) américain, intitulé "*Cyber Operations in DOD Policy and Plans: issues for Congress*"[1]. Le rapport est daté du 5 janvier 2015.

Ce document peut être divisé en deux parties: la première, d'intérêt très relatif, revient sur le contexte et les éléments de la cybersécurité, en abordant de manière rapide (et donc superficielle) les notions de cyberespace, cyberarmes (malware, botnets, attaques DDoS), systèmes automatisés de défense, cibles (réseaux du gouvernement et des armées, infrastructures critiques), acteurs (Etats, hacktivistes, terroristes et criminalité organisée), APT, problématique de l'attribution, environnement de la menace (avec rappel des faits marquants récents que sont les attaques contre l'Estonie, le conflit russo-géorgien, les cyberattaques contre l'Iran), le tout en une petite dizaine de pages, et sans apporter d'éléments d'information nouveaux. Nous retenons toutefois de cette première partie les quelques lignes dédiées aux moyens de réponse aux cyberattaques automatisés. Ce hacking de représailles (*retaliatory hacking*) semble être pratiqué davantage dans le secteur privé qu'au sein des forces étatiques. L'Etat peut être cependant engagé dans de telles cyberattaques réactives dans des situations spécifiques de crise et de combat. Mais l'Etat peut-il encourager cette pratique dans le privé, alors que le cadre légal prohibe la diffusion de malware et l'intrusion dans des systèmes ? Doit-on interdire ces contre-attaques lorsqu'elles permettent de faire cesser les atteintes préjudiciables à la sécurité nationale ? La DARPA finance un programme important pour le développement de systèmes de sécurité automatisés capables de répondre à des cyberattaques et de les neutraliser. Rappelons aussi que d'autres Etats financent de telles initiatives (le Japon par exemple).

La seconde partie nous semble plus intéressante : elle traite des institutions de la cybersécurité/défense américaine, des partages des rôles entre elles, des missions attribuées, des

[1] http://www.fas.org/sgp/crs/natsec/R43848.pdf

responsabilités, des moyens alloués, et de toute cette dynamique d'institutionnalisation de la cyberdéfense initiée aux Etats-Unis depuis plusieurs années désormais.

I - La répartition des rôles et la définition des règles

1- La cybersécurité est prise en charge au niveau national par une institution placée au sein même de la Maison Blanche, dirigée par le Coordinateur de la Cybersécurité (Cybersecurity Coordinator) souvent désigné *Cyber Czar* (fonction créée en 2009 par l'administration Obama).

2- Le Cyber Commandement combine capacités et missions défensives et offensives. Il a la charge de la défense des réseaux de l'armée (domaine .mil). Ses missions sont définies dans le cadre de l'U.S.C. Title 10. Le cyber commandement réunit trois types de forces cyber :
   - Des forces nationales (national mission forces): dont le rôle est de protéger les infrastructures critiques essentielles à la sécurité nationale et économique
   - Des forces de combat (combat mission forces): dont le rôle est d'aider les commandements militaires à mettre leurs plans en œuvre
   - Des forces de cyber-protection (cyber protection forces) : dont la fonction est de sécuriser, protéger les réseaux du DoD.

3- La NSA assure les activités de renseignement sigint, et la sécurité de l'information des systèmes de sécurité nationale. A l'intérieur de la NSA se trouve le Central Security Service, service de cryptographie des armées. Ses fonctions sont définies dans le cadre de l'U.S.C. Title 50.

4- Un programme de partage d'informations sur les cybermenaces a été lancé en mai 2011 (DIB Cyber Pilot) pour faciliter les échanges entre armée, renseignement et industriels.

5- Le cadre juridique de la cybersécurité et des cyber-opérations est contenu dans plusieurs documents :
   - *USC Title 10*
   - *USC Title 50*
   - *Executive Order 13636 pour renforcer la cybersécurité des infrastructures critiques (12 février 2013)*
   - *Presidential Policy Directive 21 : pour renforcer la sécurité et la résilience des infrastructures critiques (PPD 21) (février 2013)*
   - *National Infrastructure Protection Plan (NIPP) 2013 (DHS) (en phase avec la PPD 21)*
   - *National Security Presidential Directive 54*
   - *Homeland Security Presidential Directive 23*
   - *Section 941 of the National Defense Authorization Act (FY 2013)* : attribue la responsabilité des cyberopérations au Secrétaire de la Défense. Ce dernier est l'autorité qui conduit les opérations militaires dans le cyberespace, y compris les opérations clandestines. Les auteurs introduisent ici une réflexion sur la distinction entre « covert operations » et « clandestine operations ». Dans une opération clandestine, qui relève bien des missions de l'armée, on cherche à dissimuler l'opération elle-même mais pas celle de leur commanditaire. Une opération clandestine est réalisée par une agence de l'Etat. Dans une opération secrète (covert) l'accent est mis sur la dissimulation de l'identité de l'acteur opérant/commanditaire. Une telle action est soumise à l'aval présidentiel, conformément à l'USC Title 50. Les opérations cyber peuvent relever dans les faits de ces deux catégories (covert ; clandestine). La question qui se pose est celle du nécessaire aval présidentiel, du reporting trimestriel au Comité Défense du Congrès (congressional defense committee), ou au contraire de la possibilité pour les cyberopérations de se passer

du circuit strict qui s'impose aux actions secrètes (covert). De quel cadre doit relever la computer network exploitation (CNE) menée par l'armée ?

- *La directive présidentielle PPD 20* (octobre 2012), dont le contenu est classifié, distingue défense des réseaux (*network defense*) et opérations offensives et défensives dans le cyberespace (*offensive and defensive cyberspace operations*).
  - Pour la défense des réseaux : Les missions entre les diverses acteurs responsables ne sont pas réparties en fonction de la nature des menaces (espionnage, terrorisme, criminalité, guerre…) mais en fonction des domaines (.mil pour le DoD; .gov pour le DHS ; etc.)
  - Pour les opérations offensives : elles relèvent d'un cadre défini dans un document classifié, Executive Order, émanant du DoD (chef des Etats-Majors – Chairman of the Joint Chiefs of Staff- à la direction du Secrétariat de la Défense). Ce document classifié définit les conditions de l'exercice cyber offensif pour le cyber commandement, et les forces cyber des diverses branches de l'armée américaine (Air Force, Navy, …)
  - Les militaires ne peuvent répondre à une cyberattaque terroriste ou de cyberguerre que sur autorisation et ordre du Président.

II - L'augmentation des ressources

- Le budget cybersécurité demandé par le DoD est de 5.1 milliards de $US en 2015 (pour un budget TIC de 36 milliards pour le seul DoD). Ce budget cybersécurité est en hausse de 1 milliard de $entre 2013 et 2014.
- L'accroissement des capacités s'accompagne de l'augmentation des ressources humaines, passant de 1000 hommes à 6200, entre 2013 et fin 2016. Les forces cyber sont composées à 80% de militaires, 20% de civils.

III - La prise en compte de l'environnement international

Les règles établies par les Etats-Unis pour assurer leur cyberdéfense disposent d'un cadre réglementaire national. Mais les décisions prises au sein de l'arène internationale (dans le cadre de la convention de Budapest, des résolutions des Nations Unies, du droit international des conflits armés, du droit des contremesures, de l'OTAN, de l'UIT, d'accords bilatéraux, mais encore d'institutions comme le G8, l'APEC, l'ASEAN, l'OAS (Organization of American States), la ligue des pays arabes, l'OCDE, l'OSCE…) pourraient avoir un impact sur les règles appliquées par le gouvernement américain pour l'action de ses propres forces de défense. Cette dimension internationale est prise en compte par les Etats-Unis dans sa stratégie internationale publiée en 2011, International Strategy for Cyberspace, qui appelle à une forte coopération bilatérale et multilatérale, ainsi qu'à une forte participation du secteur privé. Le gouvernement ne souhaite pas de nouvelle convention internationale, s'appuyant sur la convention de Budapest, jugée suffisante. Le droit international est également commenté : le Département d'Etat définit les conditions dans lesquelles une cyberattaque peut être qualifiée d'usage de la force (septembre 2012) : celles dont résultent des pertes en vies humaines ou des destructions significatives. Cette lecture insiste sur les effets, recherchés et produits, et non sur les moyens employés. Mais l'usage de cyberattaques sans effets cinétiques relève parfois aussi du conflit armé : les cyberattaques contre des réseaux pendant un conflit armé sont des actes de guerre et doivent être traitées comme tels (réponse proportionnée).

IV - L'étude formule pour conclure plusieurs questions

- Le droit en vigueur est-il suffisant ?

- Comment les responsabilités du cyber-commandement et du Département de la défense s'imbriquent-elles juridiquement avec les obligations et prérogatives du secteur privé en matière de cybersécurité ? Les auteurs rappellent l'existence du principe de *Posse Comitatus*[2], qui interdit le recours à l'armée pour des questions de politique intérieure. Or l'obligation faite au Cyber Command de contribuer à la protection des infrastructures critiques suppose de facto un soutien au secteur privé, qui est propriétaire de la majorité des infrastructures critiques du pays. La protection de biens privés par l'armée en temps de paix ne viole-t-elle pas ce P*osse Comitatus* ?
- Le cyber commandement doit-il être son propre commandement unifié ? La frontière entre opérations de renseignement et opérations militaires offensives est très étroite, en raison de la localisation du cyber commandement et de la NSA dans de mêmes enceintes, et de la direction des deux institutions par un même homme. Le renseignement cyber (computer network exploitation) est très proche des cyberattaques (computer network attacks). Ne faut-il pas, pour éviter les conflits entre USC Title 50 et USC Title 10, donner une contrôle civil à la NSA et faire du Cyber Command un commandement unifié, et non plus une structure placée sous le Stratcom ? Le problème essentiel semble résider dans l'attribution à un seul individu de la direction de la NSA et du Cyber Command, l'une relevant de l'USC Title 10 l'autre de l'USC Title 50, qui définissent des règles concurrentes ?
- Une cyber-force séparée est-elle nécessaire ? Si le cyberespace est bien une 5° dimension, pourquoi ne pas lui attribuer une force spécifique ? La question demeure, avec d'un côté les partisans d'une arme propre, de l'autre ceux qui défendent la particularité du cyberespace, à savoir sa transversalité.

[2] http://www.law.cornell.edu/uscode/text/18/1385