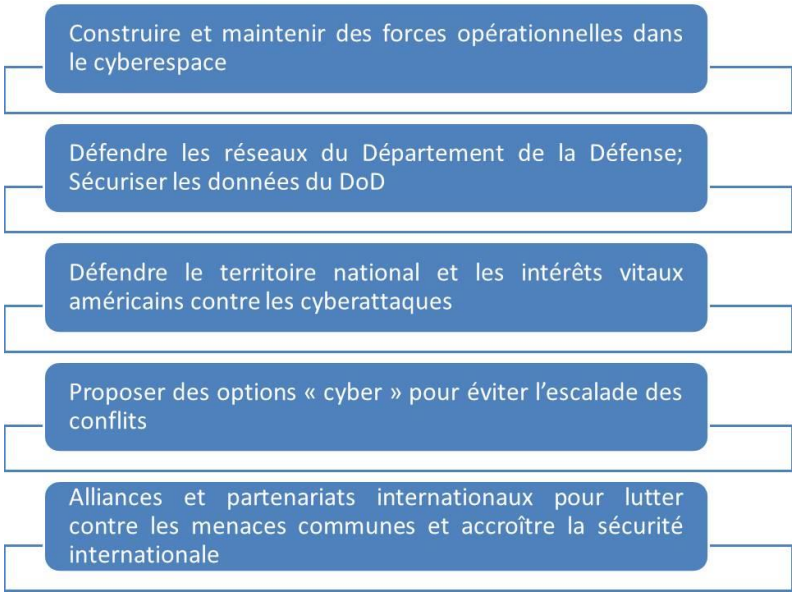
Les défis pour la défense à l'horizon 2035 : le point de vue américain

Daniel Ventre, CNRS (CESDIP), Titulaire de la Chaire Cybersécurité & Cyberdéfense

26 Juillet 2016, article III - 26

Le Département de la Défense américain vient de publier le 14 juillet 2016 un document intitulé « *Joint Operating Environment – JOE 2035. The Joint Force in a Contested and Disordered World* »[1]. Ce document traduit la vision de la Défense américaine à l'horizon 2035 : sa vision du monde, des défis et la manière d'y faire face. Il s'inscrit dans le droit prolongement, pour sa dimension cyber, de la cyberstratégie du Département de la Défense, dont nous rappelons les principes :



Liste reconstituée à l'aide du document de synthèse « Fact Sheet : The Department of Defense (DOD) Cyber Strategy. April 2015 »[2]

[1] Joint Chiefs of Staff, *Joint Operating Environment – JOE 2035. The Joint Force in a Contested and Disordered World*, Etats-Unis, 14 juillet 2016, 57 pages, http://www.dtic.mil/doctrine/concepts/joe/joe_2035_july16.pdf

[2] *Fact Sheet : The Department of Defense (DOD) Cyber Strategy. April 2015, Etats-Unis, 2 pages,* http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf

L'article que nous proposons résume les principales lignes et argumentaires développés dans le document JOE 2035.

I - Les grands principes

Cette prospective se décline en quelques points clefs : mes relations entre les USA et leurs adversaires, actuels et futurs, prendront la forme de conflits ouverts, violents ; l'environnement et la forme de la guerre subiront des transformations qu'ils convient de préparer, accompagner, anticiper, tant sur les plans capacitaires qu'opérationnels. Les conflits auront pour cause et terreau des sociétés désorganisées, des Etats désireux d'en découdre pour imposer leurs normes aux autres nations (remettre en cause l'ordre du système international et s'y affirmer), les évolutions de la géographie humaine (« Human Geography »), ou le rattrapage technologique de certains acteurs qui leur permettra de défier les Etats-Unis (« Science, Technology and Engineering »). Les guerres seront plus complexes car leurs causes et enjeux interagiront, en rendant la lecture, la compréhension et la résolution plus complexes. Dans un tel contexte la Défense a pour mission de protéger les intérêts nationaux, d'éviter les conflits, de punir les agressions, de vaincre les adversaires. La guerre en 2035 dépendra de 6 contextes majeurs :

II – Défense et cyberespace

2.1. Cyberespace souverain et non souverain : une frontière floue source de conflits

La distinction entre parties souveraines et non-souveraines du cyberespace est une problématique propre aux acteurs étatiques ; les acteurs non-étatiques quant à eux ne s'en soucient guère. Les Etats-Unis doivent défendre leur **cyberespace souverain**, et protéger l'utilisation du **cyberespace non-souverain,** en sa qualité de Global Commons. La frontière entre souveraineté et non-souveraineté pose problème dans le réel, ayant entraîné dans l'histoire de nombreuses guerres. La reconnaissance de la souveraineté des Etats s'inscrit dans un très long processus, nombreux étant les acteurs étatiques et non-étatiques à remettre en cause les souverainetés. Dans le cyberespace la

problématique n'en est pas moins sensible. Il y manque des règles, des normes, et des conflits pour la définition et la reconnaissance des espaces souverains sont fortement probables. La Défense estime donc essentielle **la définition des espaces souverains et communs, et leur distinction**.

Le rapport précise que les Etats-Unis doivent « contrôler **les parties essentielles** du cyberespace (à la fois souveraines et non-souveraines) ». Il y aurait donc 3 niveaux à considérer :

- la partie souveraine
- la partie non-souveraine
- et une partie à l'intersection des deux premières (ou les recoupant intégralement ?) qualifiée d'essentielle (« key parts »)

	Cyberespace souverain	**Cyberespace non-souverain (global commons)**	**Parties essentielles (key parts)**
Modalité d'action étatique sur chaque partie	Défense	Protection	Contrôle
Implication du militaire	Oui	Oui	Oui
Moyens employés	Cyber et non cyber	Cyber et non cyber	Cyber et non cyber

La **guerre** pourrait à l'avenir résulter de la lutte que se livrent les Etats pour protéger leur souveraineté dans le cyberespace. Les probabilités de conflits seront d'autant plus élevées que le nombre d'Etats disposant de capacités militaires cyber ne cessera de croître.

2.2. Les intentions étatiques et les capacités militaires

Le **cyberespace** est un lieu de compétition, d'affrontement, au même titre que les autres « global commons », où les adversaires tentent d'accroître leur espace d'action. L'élargissement de l'espace d'action des Etats est visible sur mer et dans les airs (établissement de nouvelles zones d'identification de défense aérienne – « *Air Defense Identification Zones », ADIZ*), ainsi que dans l'espace (où de nouveaux Etats peuvent projeter leur puissance, ne laissant plus cette prérogative aux Etats majeurs, en exploitant des produits commerciaux tels que moyens d'observation, moyens de communication).

Le monde ne cesse d'évoluer, et ce qui semble le plus inquiéter les Etats-Unis ici, ce sont les nouvelles puissances qui veulent s'imposer dans le monde, déployant pour cela ne nouveaux arrangements politiques, économiques et sécuritaires. Les tensions viennent des **divergences fondamentales** sur des sujets essentiels comme la gestion des ressources naturelles, les droits de l'homme, les responsabilités dans les Global Commons (mer, espace, cyberespace). Les projets de puissance de nombre d'Etats qui veulent s'imposer dans le système international risquent de mener à des conflits (ces Etats seront tentés de recourir à la force pour s'imposer). Les luttes idéologiques violentes, par les réseaux identitaires construits dans le cyberespace, défieront à l'horizon 2035 l'autorité des Etats, les fondements (institutionnels, sociaux, culturels) pacifiques de l'ordre mondial.

La prochaine décennie, toujours selon ce rapport, devrait voir se **multiplier les capacités et forces cyber étatiques**, que les adversaires emploieront pour essayer de contourner la puissance militaire conventionnelle américaine et influencer les calculs politiques et militaires. Les Etats seront ainsi de plus en plus nombreux à disposer de capacités cyber ; ces capacités seront offensives ; permettront de perturber le fonctionnement de tout système connecté, ou celui des sites pour provoquer des désordres sociaux, saper la confiance et l'intégrité des données, mettre en place de la surveillance

stratégique, de l'espionnage industriel et scientifique. Si le texte est écrit au futur (« *states will have… in the future, state military … will increasingly use… attacks will work…* »), les modalités décrites sont bien celles du présent, et **d'une situation appelée à s'inscrire dans la durée.**
Dans la société post-moderne, le pouvoir sera exercé via les réseaux, mobilisant des masses d'individus connectés et poursuivant des objectifs communs, capables de remettre en cause la bureaucratie verticale. Dans ce contexte le militaire doit savoir manipuler les perceptions, les comportements et les décisions de ses cibles (en combinant narrations, techniques de communication stratégique, propagande… et cyberattaques).
Le texte **déroule tous les scénarios possibles impliquant l'usage du cyberespace, des nouvelles technologies** (big data, biométrie, surveillance, etc.) : la lutte contre le terrorisme, la lutte contre des mouvements insurrectionnels, attaques et guerre sur le sol même des Etats-Unis, conflits internationaux contre des ennemis puissants pouvant se prolonger sur plusieurs années, actions de paix (« peace enforcement operations »).

Pour la défense américaine, les cyber-capacités sont donc une dimension incontournable. **Les efforts** que vont consentir les adversaires pour accroître les capacités nécessaires à leur domination, régionale ou globale, **iront en priorité aux cyber-capacités**. Car c'est par le biais du cyberespace que seront menées les attaques stratégiques (contre les infrastructures financières, énergétique, du pays), affirme la défense américaine. Ces capacités seront complétées, ou viendront compléter, les capacités exprimées en termes de missiles, navires, sous-marins, etc. Le cyber est le **complément des moyens physiques** de la force, de la puissance. Certains **Etats sont en mesure d'intégrer les capacités de cyberguerre aux niveaux tactiques et opérationnels de la guerre** (pour, par exemple, attaquer les réseaux militaires adverses pour gripper le fonctionnement des armées déployées sur les théâtres d'opération). La structure physique du cyberespace présente l'une des vulnérabilités essentielles des systèmes d'armes connectés, parce que cette structure peut être attaquée au moyen d'armes cinétiques, ou d'armes lasers, ou électromagnétique. Cet environnement de combat sera d'autant plus transformé et complexe que viennent s'ajouter des armes hypersoniques, des robots, des intelligences artificielles. Vulnérabilités structurelles du cyberespace, intelligence, tempo opérationnel et décisionnel accéléré, sont les ingrédients de ces modifications.

Les Etats n'auront pas tous la même approche du contrôle du cyberespace. La Chine continuera l'installation de barrières pour protéger les cyber-infrastructures critiques, mais aussi pour assurer un contrôle à l'intérieur (surveillance, contrôle des flux d'information, visant à limiter toute opposition). L'avenir devrait laisser place à plus de pratiques autoritaires (limitation d'accès, barrières vis-à-vis du reste du monde…) Le rôle des cyber-forces militaires consistera à assister les autorités nationales dans la délimitation et la défense des frontières nationales dans le cyberespace. Les cyber-forces de nombre de pays, notamment aux tendances autoritaires, tenteront de déstabiliser la cohésion sociale et politique de leurs adversaires. Les pays hostiles mèneront des opérations de propagande, d'influence des perceptions, des comportements, des décisions, à grande distance, et pour un coût peu élevé. Les pays étrangers pourront cibler leurs adversaires américains, en attaquant spécifiquement des responsables politiques, militaires, industriels, à l'aide d'opérations de guerre de l'information. Pour mener leurs attaques, les Etats disposent de nouveaux types d'armements que sont les **« cyber-armes »**, dépourvues du caractère cinétique des armes et qui sortent des critères traditionnels de la guerre interétatique. Ces armes ouvrent de nouvelles possibilités, de nouvelles modalités actions s'inscrivant entre la guerre et la paix.
Les **opérations offensives**, visant à préserver la souveraineté américaine, attaquée dans le cyberespace, recouvrent :

- des opérations d'identification, ciblage, capture voire élimination des cyberagresseurs ennemis (« kill adversary cyber operatives »)
- la destruction des capacités et infrastructures cyber adverses (via des frappes cinétiques combinées à des actions de guerre électronique et cyberguerre) Le rapport insiste à plusieurs

reprises sur cette facette de la lutte contre les capacités cyber ennemies : les actions physiques contre la dimension physique, matérielle du cyberespace.
- Des actions menées sur les prises de guerre, que recouvre la formule « captured adversary networks », et sur lesquelles l'armée américaine pourra alors imposer des règles et son droit (contrôle de noms de domaines, accès, administration de systèmes clefs).

Il est proposé ou envisagé de créer un parapluie ou bouclier cyber pour le Département de la Défense, une patrouille des cyber-frontières nationales, conjointement à un renforcement du renseignement (une approche globale renforcée), à la contribution militaire à des cyber exercices nationaux, ou encore au développement de réseaux renforcés (« hardened networks »).

2.3. Les responsabilités de la Défense

La **responsabilité de la protection** des réseaux critiques, des infrastructures de communication, des serveurs, des systèmes financiers, sont **des composantes de l'espace souverain américain**. Les forces armées dans leur ensemble doivent contribuer à leur protection, pour faire face à des adversaires multiples. Cette responsabilité de la défense s'étend à la protection des partenaires et des alliés, notamment en vue de contribuer à la **cyber-résilience**. Pour atteindre cette dernière, l'effort doit être conjugué avec celui d'organisations civiles, d'Etats alliés, de partenaires internationaux, d'entreprises privées, voire de cyber activistes. L'armée ne doit pas réduire son action de support à la défense des intérêts souverains, mais le prolonger aux espaces communs. L'objectif est d'y défendre le principe de libre accès, et les intérêts nationaux. La difficulté dans ces *global commons* consiste à faire face à des acteurs asymétriques, non conventionnels, à des approches asymétriques.

Conclusion

Ce rapport décline tout un ensemble de termes et expressions dérivés du terme « cyber » (voir tableau ci-dessous). A l'aide de ce vocabulaire et de ces concepts, qui ne sont d'ailleurs pas définis dans le rapport, et ne le sont pas davantage pour la plupart dans le dictionnaire du département de la défense, il pose les bases de la place du cyberespace dans le conflit moderne, et de son rôle opérationnel et tactique.

Nous retiendrons de ce document que le militaire américain :
- conserve, pour penser l'avenir du conflit, le prisme de la pensée clausewitzienne. En attestent les citations insérées dans le document, en introduction de la Section I ("*The first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make is to establish… the kind of war on which they are embarking*"), ou encore dans la conclusion du rapport ("*The primary purpose of any theory is to clarify concepts and ideas that have become, as it were, confused and entangled*").
- insiste sur, ou rappelle l'importance de la matérialité du cyberespace, en s'attachant à désigner son infrastructure physique comme l'une de ses facettes les plus vulnérables.
- désigne la frontière entre cyber souverain (ce qui n'appartient qu'à nous) et commun (ce qui appartient à tous) comme l'un des points de friction clefs, car s'y retrouvent Etats et acteurs non-étatiques. Les conflits ne naissent donc pas de n'importe quelle part du cyberespace, de n'importe quelle action. Il est des lieux plus essentiels que d'autres. Mais dès l'instant où tous les Etats viendraient à définir des zones de cyberespace souverain, la conséquence n'en serait-elle pas, à terme et *de facto*, la disparition de toute zone commune ?

Cyber actions
Cyber activist
Cyber activities

Cyber advocates
Cyber border patrol
Cyber campaign
Cyber capabilities
Cyber coercion
Cyber commons
Cyber defenses
Cyber denial measures
Cyber deterrence
Cyber domain
Cyber effort
Cyber exercises
Cyber forces
Cyber infrastructure
Cyber law
Cyber operations
Cyber operatives
Cyber power
Cyber resiliency
Cyber revolution
Cyber rules
Cyber strategies
Cyber support
Cyber systems
Cyber techniques
Cyber umbrella
Cyber vulnerabilities
Cyber warfare
Cyber warfare capabilities
Cyber weapons
Cyberattacks
Cyber-attacks
Cyber-capable
Cyber-connected
Cyber-dependent
Cyber-enabled
Cyber-military
Cybersecurity
Cyber-security
Cyberspace
Cyberspace disruption
Cyberspace sovereignty
Cyberweapons

Tableau : Liste des mots clefs (termes, expressions) de ce rapport, déclinant le terme « cyber »

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18

La chaire remercie ses partenaires