LES VA-T-EN-CYBERGUERRE DÉBARQUENT

LE 6 OCTOBRE 2010 ***OLIVIER TESQUET***

A en croire le Pentagone, les États-Unis seraient menacés par une guerre informatique qui nécessite d'investir à fonds perdus dans des systèmes de défense. OWNI démonte les rouages de cette machine bien huilée.

"Le ministre de la guerre a donné sa démission, la guerre est supprimée" . La phrase est de Jules Renard mais elle pourrait tout aussi bien être la conclusion du point presse brumeux d'un gouvernement occidental. Nous sommes en 2010, et la notion de belligérant n'a plus grand chose à voir avec les préceptes millénaires de Sun Tzu. L'armée américaine s'est officiellement retirée d'Irak, mais elle s'est officieusement embourbée en Afghanistan. Le Pentagone a taillé des croupières aux entreprises d'armement en rabotant certains programmes, et les généraux 5-étoiles se sont fait la guerre **autour du vocable contre-insurrectionnel**. On a donné toutes sortes de noms aux conflits, singuliers ou pluriels, asymétriques, irréguliers, hybrides. Robert Gates, le secrétaire à la Défense, un *maverick* rescapé de l'administration Bush, a dépecé le mythe de ***Top Gun*** en **sacrifiant le chasseur F22**, cette rune avionique symbole de puissance dans la culture populaire. Il a aussi suivi les directives de Barack Obama en paraphant l'accord pour un envoi de **30 000 soldats supplémentaires** dans les faubourgs de Kaboul et les montagnes de Kandahar. On appelle ça les paradoxes de la guerre.

Nous sommes en 2010, et l'économie américaine reste liée jusque dans l'intimité à son complexe militaro-industrialo-congressionnel, qui fortifie tout à la fois son maillage économique local et son rayonnement international. Après avoir prôné depuis trois ans un retour à la raison autour des besoins immédiats de l'armée, le Pentagone a voté pour l'année fiscale 2011 le **budget de la Défense le plus élevé depuis 1945**, au-delà du seuil symbolique des 700 milliards de dollars. Après avoir fait l'aggiornamento de leur doctrine, momentanément débarrassée du concept de guerre traditionnelle, les États-Unis devaient se réunir autour d'un nouveau mot d'ordre: la cybersécurité. Un commandement dédié, le Cyber Command, est **sur le point d'être opérationnel**, et les hiérarques de l'administration se chargent d'assurer le service après-vente de cette menace flambant neuve, matérialisée après dix bonnes années de manœuvres en sous-main. William J. Lynn III, le second de Gates, s'est répandu dans la presse pour expliquer la nécessité de "défendre un nouveau domaine", particulièrement dangereux.

La cyberguerre est la nouvelle norme

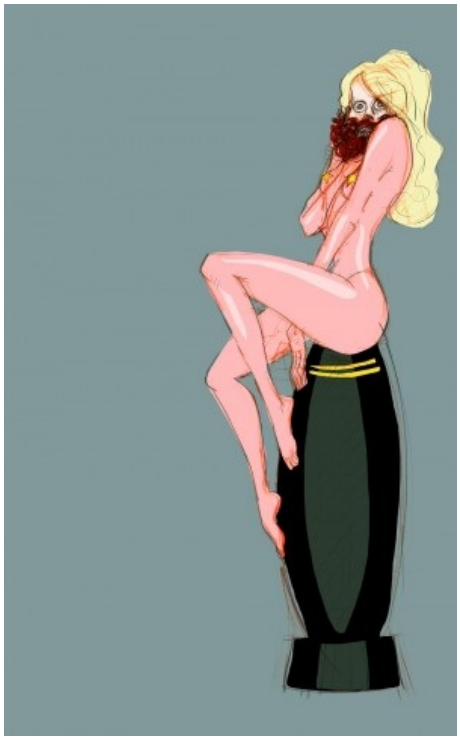
Certains poids lourds de la Défense, comme **Raytheon**, **Lockheed Martin** ou **Northtrop Grumman**, spécialisés dans l'aviation de pointe, les missiles ou les radars de haute technologie, ont senti cette évolution structurelle et développent des stratégies dédiées pour attirer à eux de nouveaux contrats particulièrement lucratifs dans le domaine de la sécurité des systèmes. Aujourd'hui, **selon Jane's**, la très sérieuse lettre d'information militaire, l'aviation concentrerait environ 800 programmes répartis en 120 contrats, pour une somme engagée de 1000 milliards de dollars. Sans atteindre les mêmes proportions (elle ne représente "que" 102 milliards de dollars), **la cyberguerre agrège** plus de 1200 projets et 100 contrats. Parmi les entreprises sollicitées, on ne retrouve aucune entreprise dédiée, mais tous les grands noms. Après avoir vendu du matériel pendant des décennies, les entreprises de Défense adossées au Département de la Défense vendent désormais **du service et du conseil**.

A cela, rien de très étonnant. Plus qu'aucune autre forme de conflit, la cyberguerre formule une équation basée sur l'expertise, et non sur la capacité industrielle à usiner des milliers de pièces. Avec l'irruption de cette composante, certains politiques n'hésitent plus à placer leur mise sur le tapis de jeu. Ainsi, Mike McConnell, l'ancien directeur du renseignement de George W. Bush, expliquait **dans une tribune pour le Washington Post** *"comment gagner la cyberguerre que nous sommes en train de perdre"*. Six semaines plus tard, le Pentagone allouait un **juteux contrat de 34 millions de dollars** au géant du consulting en sécurité Booz Allen Hamilton, pour répondre à cette carence. Qui est le P-DG de Booz Allen Hamilton? Mike McConnell.

Ron Schwenn, assistant director des acquisitions au Government Accountability Office (GAO, la Cour des Comptes américaine), passe l'année à compulser des rapports sans marge et à éplucher des cahiers des charges fantaisistes, où le dépassement de frais devient la norme. S'il se drape d'ordinaire dans les atours du discours officiel pour ne pas froisser sa hiérarchie, il nous exprime au téléphone sa méfiance envers ce glissement stratégique:

> ***Nous sommes indépendants, mais notre rôle est purement consultatif. Avec le durcissement budgétaire imposé par Gates, on aurait pu penser que le Département de la Défense allait enfin suivre nos recommandations, mais il n'en est rien. Quand ils ont réalisé qu'ils ne pourraient pas sauver certains programmes, obsolètes ou trop coûteux, ils ont décidé de réinjecter des fonds dans des projets aux alias futuristes, avec pour mot d'ordre la prévention contre les cyberattaques. Non seulement le DoD fait preuve d'une mansuétude surprenante dans ce domaine, mais c'est une main tendue à toutes les entreprises frappées par la politique de rigueur.***

La cyberguerre permet de vendre la guerre en temps de paix



Dans l'âge post-nucléaire, où la polarité n'est plus aussi simple qu'un commutateur guerre/paix, la cyberguerre en tant que nouvelle menace répond paradoxalement à un besoin d'apaisement: c'est une réponse au débat tendu sur la contre-insurrection, aux attaques de drones, aux dommages collatéraux que celles-ci entraînent, aux errements opérationnels, aux tensions entre Barack Obama et le général Stanley McChrystal, l'ex-commandant de la coalition en Afghanistan, congédié par le président après une **interview un peu trop libérée** dans Rolling Stone.

Si le principe séculaire de dissuasion et la capacité de projection restent les deux mamelles de la pensée militaire américaine (le **Quadriennal Defense Review**, qui fixe tous les quatre ans la stratégie à moyen terme de l'armée, a reconduit cette double idée), l'impopularité des conflits irakien et afghan au sein de l'opinion publique pousse législateurs, chefs d'état-major et capitaines d'industrie à agiter le chiffon rouge d'une menace encore volatile. Des spots de publicité commencent à débarquer sur CNN aux heures de grande écoute, tout comme dans la presse. Dans ***The Atlantic*** du mois d'août, on pouvait voir cette réclame pour Lockheed Martin, sur fond de moniteurs et d'uniformes kakis: *"Lorsqu'il s'agit de se défendre contre les cyberattaques et d'assurer la résistance, il y a un mot important, COMMENT"*. Pour une entreprise de cette taille, frappée au cœur par la réorganisation des programmes, ne nous leurrons pas, il s'agit d'un formidable relais de croissance

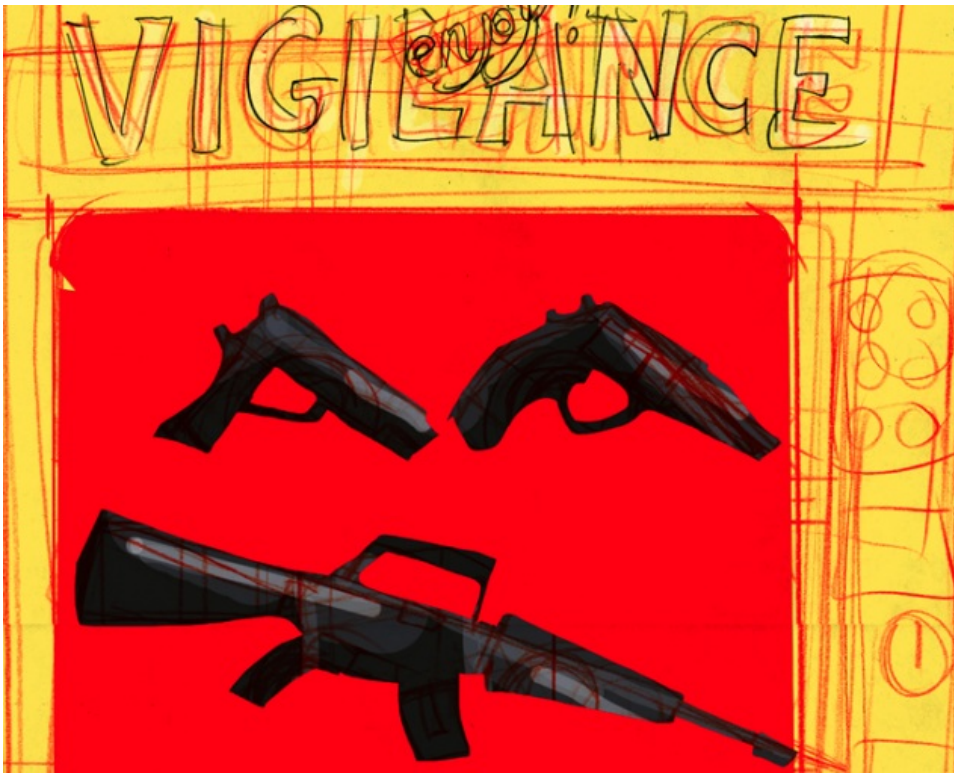
Au-delà du poids qu'est en train de prendre l'"industrie" de la cyberguerre dans l'économie de la Défense, c'est la gigantesque opération de marketing élaborée pour la promouvoir qui attire l'attention. Fin septembre, le Département de la Sécurité Intérieure a organisé pendant quatre jours un ***"cyber-blitz"*** , afin de tester les capacités de résistance des systèmes informatiques de l'Etat à une attaque-éclair. Mais contrairement aux annonces, ce n'est pas la première fois que l'administration joue à se faire peur. En février, le Bipartisan Policy Center, un think tank bipartisan (comme son nom l'indique) avait mis en place le **Cyber Shockwave**, autre exercice au nom ronflant qui montrait les *"failles des Etats-Unis"* .

Aux manettes de ce Risk numérique, on ne retrouvait que d'anciens cadres de l'administration, liés au renseignement ou à la sécurité nationale. Ce n'est pas non plus un hasard si parmi tous les théoriciens de la cyberguerre, on retrouve bon nombre d'anciens de la **RAND Corporation**, cet aïeul caritatif des think tanks qui existait 16 ans avant que Dwight Eisenhower ne verbalise la notion de complexe militaro-industriel. Parmi eux, on peut citer John Arquilla, le chantre de la cyberguerre offensive, qui redéfinit sans détours la notion de risque: *"CYBERWAR IS COMING!"* , écrivait-il l'année dernière dans un rapport de l'organisation (**PDF**), lettres capitales et point d'exclamation compris.

La cyberguerre est une guerre sans soldats

"La crainte de la guerre est pire que la guerre elle-même" , écrivait le stoïcien Sénèque. Avec l'avènement de la cyberguerre (qui existe dès lors qu'on l'énonce), les experts se sont substitués aux universitaires, ce qui a largement contribué à téléporter le discours général aux frontières de la peur panique. Les littérateurs du genre n'hésitent pas à manipuler les

représentations les plus grossières pour servir leur rhétorique ou monnayer leurs compétences. Sur la couverture de **Cyberwar**, l'ouvrage "de référence" de Richard Clarke, vieux routier du renseignement, on peut admirer une souris d'ordinateur au motif camouflage. L'image est un tantinet racoleuse, le propos aussi, mais il permet à son auteur de remonter en **première page de Google** quand vous tapez "cyberwar".



Si la cyberguerre est une bataille d'experts, son application physique est inversement proportionnelle au bruit qu'elle génère. Loin des clivages politiques ou d'un schéma tracé sur un paperboard, cela tient à quatre raisons toute simples, inhérentes à l'arme informatique:

- La frontière entre le test de sécurité et l'attaque à proprement parler reste floue. Dans ces conditions, il est facile de plaider l'accident et d'invoquer la bonne foi, comme si le soft power se durcissait le temps d'un petit ver.
- Au contraire d'une ogive nucléaire ou de la conception d'un missile air-sol, une arme informatique ne nécessite ni matériaux complexes, ni compétences rares.
- Les armes conventionnelles laissent des impacts de balles, mais les attaques informatiques sont presque impossibles à tracer.
- Les armes informatiques ne réclament aucune infrastructure particulière pour les développer. Sans usine, bon courage aux satellites chargés de débusquer les lieux de fabrication…

Sans application de terrain, l'existence de la cyberguerre est conditionnée par son relais médiatique. C'est pour cette raison que Barack Obama a nommé Howard Schmidt au poste de cybertsar ("cyberczar" en anglais) en janvier 2009. Étonnamment, on ne l'entend pas beaucoup ce spécialiste reconnu de la sécurité. Pourquoi? Peut-être parce qu'il a soutenu dans Wired ***que "la cyberguerre n'existe pas"*** .

La cyberguerre ne laisse pas de traces de bottes, mais elle marque les esprits

Si elle n'a pas vraiment plus en haut lieu, la saillie de Schmidt n'est en réalité que l'affirmation brutale de la réalité. Puisque n'importe qui peut prétendre avoir lancé une attaque, puisque n'importe qui peut prétendre en avoir stoppé une, qui pourra mettre le doigt sur un virus en temps réel, en identifiant les tenants et les aboutissants? Personne.

Dans cet écosystème de la pensée magique, on peut identifier deux manières de faire la guerre en se salissant seulement le bout des doigts contre la poussière d'un clavier: d'un côté, la cyberguerre "à la russe", contre **l'Estonie** ou **la Géorgie**, afin d'entretenir sa zone d'influence traditionnelle et d'assurer le contrôle de son étranger proche; de l'autre, la cyberguerre "à l'américaine", ouverte, totale, **avec la Chine en point de mire** pour une nouvelle bataille du Pacifique. La première est crédible, parce qu'elle obéit à une géopolitique cohérente. La seconde est un fantasme destiné à attraper les journalistes, parce qu'elle ressemble à la quatrième de couverture d'un best-seller de Tom Clancy: un peu de technologie, un peu de diplomatie, un peu d'espionnage. Pour le référencement, on

appelle ça le nuage de mots-clés parfait.

–

Crédits: Illustrations de Loco *(trescherloco [at] yahoo [point] fr)*

Télécharger l'illustration de Une en haute définition

EMMANUEL
le 10 octobre 2010 - 14:45 • SIGNALER UN ABUS - PERMALINK

Vraiment pénible a lire votre style, épuisant de vous décrypter a chaque phrase… Oui donc la cyberguerre n'existe pas, merci.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER TESQUET
le 11 octobre 2010 - 0:35 • SIGNALER UN ABUS - PERMALINK

Merci pour cette sentence, Emmanuel. Sinon, vous pouvez expliciter votre point de vue?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CAR INSURANCE
le 7 novembre 2011 - 4:38 • SIGNALER UN ABUS - PERMALINK

How do I restore my computer to an earlier time?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

3 pings

SCADA, salades et escalades » Article » OWNI, Digital Journalism le 11 octobre 2010 - 17:58

[...] Ils ont d'ailleurs annoncé haut et clair leur capacité offensive en matière de cyberguerre, et ont déployé une doctrine stratégique de prééminence absolue en matière de contrôle [...]

Cyberwar is coming ! La vieille chouette le 17 octobre 2010 - 18:46

[...] complément, je vous recommande la lecture de « Les va-t-en cyberguerre débarquent« Post Published: 17 octobre 2010 Author: La vieille chouette Found in section: [...]

Bank of America se prépare à la prochaine fuite de WikiLeaks » Article » OWNI_Live ! le 3 janvier 2011 - 11:59

[...] du renseignement de George W. Bush, ce spécialiste de la sécurité avait signé en avril 2010 un très juteux contrat de 34 millions de dollars avec le Département de la Défense pour répondre aux menaces de [...]