La politique de cyberdéfense peut-elle être a-politique?

Daniel Ventre

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à monsieur **Daniel Ventre** cette consultance sur "la politique de cyberdéfense peut-elle être a-politique?", sous le numéro de marché 1504119643.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique
75700 PARIS SP 07

I - Problématiques

1.1. La politique de défense est-elle a-politique?

Bastien Irondelle dans un article publié en 2007 et intitulé "La politique de défense est-elle a-politique?" [1], cherchait à mettre en évidence les relations qui s'établissent entre considérations d'ordre politique (*politics*, en anglais) et politiques de défense (au sens de politique publique, *policy* en anglais). Il y soulignait le consensus qui semble prévaloir en France concernant la conduite de la politique de défense : « *Pas un discours officiel, qui ne comporte sa révérence à l'égard du consensus sur la défense, qui n'évoque la nécessité de préserver ou de refonder* »[2]. Mais il évoquait aussi l'importance de la dimension électorale (des considérations électoralistes), susceptible d'influer sur les politiques de défense.

Les politiques de défense peuvent être contraintes par de multiples facteurs : économique, politique intérieure, contexte international, ... Elles peuvent être l'enjeu des luttes entre les partis politiques: aux Etats-Unis, depuis 1948, la politique étrangère est ainsi "*l'un des principaux terrains de combat pour les deux grands partis*"[3]. Le passage d'une administration démocrate à une administration républicaine se traduit par de nouvelles formulations des enjeux stratégiques: ainsi l'arrivée de l'administration républicaine (gouvernement de G.W. Bush) est-elle marquée par un glissement sémantique en matière de défense anti-missile (passant de la *National Missile Defense* à la notion de *Missile Defense*), révélatrice d'un changement stratégique et de posture ("*d'une administration démocrate peu convaincue [...] à une administration républicaine résolue*")[4].

Nous formulons l'hypothèse que le traitement de la cyberdéfense, au sein des politiques de défense, peut varier en fonction de la "couleur politique" des gouvernements, des partis politiques au pouvoir, des luttes entre les partis. Nous pourrions reformuler la question centrale de ce rapport : quelle est l'importance de la variable partisane dans la formulation des enjeux, dans la définition des politiques (*policies*) de cyberdéfense ? Dans le contexte américain, objet de l'étude, cela reviendrait à considérer les éventuelles différences pouvant émerger entre des politiques de cyberdéfense formulées par des Républicains et par des Démocrates. Existe-t-il des marqueurs, des spécificités propres à chaque approche? Qu'est-ce qui pourrait différencier une politique Démocrate d'une politique Républicaine sur ce sujet ?

La place prise par la dimension cyber dans les politiques de défense peut dépendre de multiples facteurs[5] tels que :

- Le contexte international,

[1] Bastien Irondelle, *La politique de défense est-elle a-politique ?*, CERI, Paris, France, mars 2007, 19 pages, http://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_bi.pdf

[2] Bastien Irondelle, *La politique de défense est-elle a-politique ?*, CERI, Paris, France, mars 2007, 19 pages, http://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_bi.pdf, page 1

[3] Stanley Hoffman, *Les partis américains et la politique extérieure des Etats-Unis, Le 81° Congrès (1949-1950)*, Revue française de science politique, 1952, vol.2, n°4, pp. 702-724, Paris, France, http://www.persee.fr/articleAsPDF/rfsp_0035-2950_1952_num_2_4_392167/article_rfsp_0035-2950_1952_num_2_4_392167.pdf

[4] Camille Grand, La défense anti-missile: un nouveau paradigme stratégique?, Revue Politique Etrangère, 2001, vol.66, n°4, pp.811-826, http://www.persee.fr/articleAsPDF/polit_0032-342x_2001_num_66_4_5125/article_polit_0032-342x_2001_num_66_4_5125.pdf

[5] Daniel Ventre, *Japon : stratégies de cyberdéfense*, Multi-System and Internet-Security-Cookbook, MISC, n° 64, 2012, p. 65-73

- les attaques contre l'Estonie se sont traduites par une prise de conscience forte des enjeux pour les Etats qui s'est accompagnée de la création d'institutions dédiées à la cyberdéfense – CCDCOE de Tallinn),
- L'appartenance à des organisations internationales (OTAN par exemple) impose des orientations, des mesures, aux Etats membres.

- Le contexte national et international :
  - le Japon, pays high-tech, hyper connecté, dont la société est probablement l'une des plus « dépendantes » du cyberespace, a dû attendre 2010 pour se doter de politiques de cyberdéfense, après un changement de gouvernement (arrivée au pouvoir du DPJ – Democratic Party of Japan en 2009). Cette politique de cyberdéfense est l'un des éléments contribuant à la reformulation de la politique de Défense du Japon, certes toujours inscrite dans le prolongement de ses prédécesseurs, mais faisant rupture sur des points essentiels en proposant un nouveau concept de défense dynamique, pour adapter les forces japonaises à l'environnement géopolitique (montée en puissance des capacités militaires chinoises, menaces de la Corée du Nord…)
- Des facteurs internes
  - La crise financière que traversent les Etats peut être l'une des raisons de remise en question des budgets alloués à la défense. Sous la pression de l'opinion publique les budgets de la Défense peuvent être modulés à la baisse. Dans un contexte de crise, la cyberdéfense peut d'autre part être considérée comme un enjeu non prioritaire face aux contingences immédiates[6].
  - L'image dont bénéficie l'institution militaire auprès de la population peut influencer le pouvoir d'influence de celle-ci. Tel semblerait être le cas de l'armée en Grèce, dont l'image positive lui permettrait d'obtenir des financements et bénéficier d'un niveau élevé d'influence politique. Les décideurs politiques auraient ainsi été réceptifs aux points de vue des militaires sur les besoins en termes d'opérations d'information[7]. La réceptivité des décideurs politiques grecs aux problématiques de la cyberguerre dépend peut-être également du talent des conseillers et experts en questions de défense à replacer les enjeux du cyber dans le contexte des enjeux stratégiques internationaux du pays[8].

1.2. La place de la cybersécurité/cyberdéfense dans le débat politique aux Etats-Unis

Sous l'administration Obama on notera une absence de consensus au sein de la classe politique sur les politiques de cybersécurité qui doivent être menées: les blocages législatifs constatés en 2011-2012 (nés de l'opposition entre un président démocrate et une Chambre des représentants républicaine et résultant de l'attentisme propre à une période pré-électorale[9]) ont abouti à l'*Executive Order*[10] du 12 février 2013, "Improving Critical Infrastructure Cybersecurity".

---

[6] Gorazd Praprotnik, Iztok Podbregar, Igor Bernik and Bojan Ticar, *A Slovenian Perspective on cyber warfare*, in Daniel Ventre (Ed.), Cyber Conflict, Competing National Perspectives, Wiley-ISTE, 352 pages, avril 2012.

[7] Joseph Fitsanakis, Digital Sparta: Information Operations and Cyber-warfare in Greece, in Daniel Ventre (Ed.), Cyber Conflict, Competing National Perspectives, Wiley-ISTE, 352 pages, avril 2012.

[8] Joseph Fitsanakis, Digital Sparta: Information Operations and Cyber-warfare in Greece, in Daniel Ventre (Ed.), Cyber Conflict, Competing National Perspectives, Wiley-ISTE, 352 pages, avril 2012.

[9] « *No resolution is expected during an election year".* Sandra I. Erwin, *Cybersecurity Legislation: solution or distraction?*, NDIA's Business and Technology Magazine, août 2012, http://www.nationaldefensemagazine.org/archive/2012/August/Pages/CybersecurityLegislationSolutionorDistraction.aspx

[10] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Il semblerait[11] cependant que quel que soit le parti au pouvoir, la cybersécurité fasse partie des priorités des gouvernements. L'on s'interroge alors sur le traitement marginal accordé au thème "cybersécurité/cyberdéfense" dans les programmes des candidats à l'élection présidentielle de 2012. Cela veut-il dire que le sujet de la cybersécurité et de la cyberdéfense ne peut pas être intégré dans les thèmes de campagne électorale? Les allusions au sujet sont brèves: lors d'un débat télévisé le candidat M. Romney fait allusion aux opérations chinoises dans le cyberespace (vols de données, piratage informatique, contrefaçon). Le candidat B. Obama dit pour sa part simplement qu'il faut penser à la cybersécurité[12]. Mais il n'y a pas de débats et échanges plus approfondis sur la question. De fait, il apparaît difficile de cerner les différences fondamentales entre les deux candidats en matière de cybersécurité[13].

Les programmes des partis républicain et démocrate (*Republican Platform* et *Democratic National Platform*) accordent une place relativement réduite à la problématique.

La plateforme républicaine[14] :

- Le parti **Républicain** est ouvertement **hostile à davantage de régulation:** la régulation fait peser sur le budget de l'Etat des contraintes lourdes et pénalise l'innovation en matière de cybersécurité[15].
- Les cyberattaques n'ont cessé de croître et le phénomène ira grandissant jusqu'à ce que les Etats-Unis ne le tolèrent plus. Tirant parti de ce constat, le document veut **démontrer l'incapacité de l'administration Obama** à gérer la menace des cyberattaques[16] et à proposer une véritable politique de dissuasion, la stratégie d'Obama ne s'appuyant que sur des pratiques défensives. Poursuivre avec B. Obama c'est donc prendre le risque de subir un cyber Pearl Harbor[17]. Le discours alarmiste est instrumentalisé **à des fins électoralistes**.
- La politique de cybersécurité républicaine (celle du président) mettrait l'accent sur le développement de capacités offensives.
- les menaces sont identifiées: Chine, Russie, terrorisme, cybermenaces...
- Le gouvernement doit **améliorer la sécurité de ses propres systèmes**. Le candidat Romney propose le renforcement du Federal Information Security Management Act pour améliorer la sécurité des systèmes d'information du gouvernement.
- Les républicains critiquent la réduction du budget de la défense sous l'administration Obama, signe de faiblesse envoyé aux adversaires
- Il faut développer la **coopération public-privé** pour faire face aux cybermenaces. Le gouvernement doit pouvoir **partager l'information** qu'il collecte sur la cybermenace avec le secteur privé, sans pour autant compromettre la sécurité nationale, et inversement.
- Le parti républicain est **partisan de dérégulation**. Pour autant, cela n'est pas nécessairement la position du candidat M. Romney. Ses conseillers ne sont pas totalement hostiles à des formes de régulation étatique, notamment le général Michael Hayden, qui fut

[11] Eric Chabrow, *Cybersecurity : Obama vs Romney*, 5 novembre 2012, http://www.bankinfosecurity.com/cybersecurity-obama-vs-romney-a-5264/op-1

[12] Eric Chabrow, *Cybersecurity : Obama vs Romney*, 5 novembre 2012, http://www.bankinfosecurity.com/cybersecurity-obama-vs-romney-a-5264/op-1

[13] Eric Chabrow, *Cybersecurity : Obama vs Romney*, 5 novembre 2012, http://www.bankinfosecurity.com/cybersecurity-obama-vs-romney-a-5264/op-1: "What remains uncertain is how a President Romney would differ from a second-term President Obama on his approach to IT security over the next four years"

[14] http://www.gop.com/2012-republican-platform_Exceptionalism/#Item7 Voir le chapitre *Twenty-First Century Threat: The Cybersecurity Danger.* Site consulté le 29 mars 2013

[15] "The costly and heavy-handed regulatory approach by the current administration will increase the size and cost of the federal bureaucracy and harm innovation in cybersecurity"

[16] « *The current Administration's cyber security policies have failed to curb malicious actions by our adversaries »*),

[17] « *The U.S. cannot afford to risk the cyber-equivalent of Pearl Harbor* »

directeur de la NSA (qui exprime des points de vue en ce sens dans une lettre en date du 6 juin 2012)[18].

La plate-forme Démocrate[19]:

La plateforme internet du parti Démocrate rappelle les actions menées par B. Obama durant son mandat.

- La cybermenace y est qualifiée de **menace émergente**. Elle est aussi l'une des plus **importantes** qui pèse sur la sécurité nationale
- Les outils que l'Amérique utilise pour devenir plus puissante sont aussi utilisés par des criminels terroristes et des Etats pour tenter de perturber, détruire les infrastructures critiques, vitales pour l'économie, le commerce, la sécurité, l'armée.
- Les **solutions proposées** consistent en la **mise en place de réseaux sécurisés**, résilients, la création du premier cyber commandement dédié à la cybersécurité, des mesures de dissuasion, prévention, détection, défense du pays contre les cyber-intrusions.
- Tout cela passe par des **investissements en R&D** et le développement d'une **culture de cybersécurité**, le **renforcement du partenariat avec le privé et des acteurs internationaux.**
- La **régulation** a toujours été soucieuse de renforcer les capacités de cybersécurité **tout en respectant les droits des citoyens**. A cet égard l'administration Obama a fait veto contre le projet de loi CISPA jugé trop menaçant pour la vie privée.
- Les démocrates défendent l'idée de la **neutralité du net,** d'un internet ouvert, libre, lieu favorisant l'innovation, la création, la consommation, la liberté de parole, libéré de toute forme de censure et de violation **des droits privés**.
- L'administration Obama veut donner **plus de pouvoirs au DHS** dans sa mission de protection des agences civiles du gouvernement.

Où sont alors les convergences et différences majeures entre les deux partis?

- Les deux convergent sur la reconnaissance d'une menace majeure, de nature cybernétique, pesant sur la sécurité nationale; sur la nécessité d'une coopération public-privé et du partage d'information[20].
- Les divergences se font jour sur le **rôle que devrait jouer le gouvernement fédéral dans la définition de normes de sécurité**[21]. Les républicains sembleraient plus réticents à de nouvelles régulations s'imposant au secteur privé (jugeant que la coopération public-privé doit être volontaire) quand les démocrates seraient quant à eux plus sensibles à la défense des droits de la vie privée.
- Les divergences s'exprimeraient également dans la **posture: défensive pour les Démocrates, offensive pour les Républicains?** Tel est le point de vue critique des républicains. Les informations sur l'opération Stuxnet sont peut-être arrivées à point nommé dans un contexte électoral, venant démentir les accusations émises par les parti républicain, d'inefficacité et de maintien dans une posture strictement défensive de la part du gouvernement Obama. D'autre part, le gouvernement Obama ne peut pas être taxé d'immobilisme en matière de politique de cyberdéfense: création du Cyber Command en 2010, nomination de Howard Schmidt comme coordinateur de la cybersécurité à la Maison Blanche fin 2009, affichage d'une politique conjointe DHS – DoD en matière de

[18] http://www.hsgac.senate.gov/imo/media/doc/CYBER%20letter%20from%20top%20security%20guys.pdf
[19] Moving America Forward, 2012 Democratic National Platform, 32 pages, http://assets.dstatic.org/dnc-platform/2012-National-Platform.pdf
[20] http://www.hsgac.senate.gov/imo/media/doc/CYBER%20letter%20from%20top%20security%20guys.pdf
[21] Eric Chabrow, *Cybersecurity : Obama vs Romney*, 5 novembre 2012, http://www.bankinfosecurity.com/cybersecurity-obama-vs-romney-a-5264/op-1

cyberdéfense[22], programme de renforcement du potentiel (ressources humaines, moyens financiers) dédié à la cyberdéfense nationale, etc.

- Selon Melissa Hathaway qui a mené sous la présidence Obama la Cyberspace Policy Review, mais qui avait aussi exercé un poste à responsabilité dans la cybersécurité sous l'administration Bush, la mise en pratique d'une politique de cybersécurité par **M. Romney consisterait en une approche managériale** : considération coûts-bénéfices, une gestion des problèmes par objectifs[23]. Approche qui ne caractériserait pas la démarche de B. Obama.

On retrouve donc des clivages traditionnels: plus ou moins d'Etat, plus ou moins de régulation, plus ou moins de pouvoirs au DHS (le candidat républicain John McCain se positionnait contre le renforcement des pouvoirs de l'agence), plus ou moins d'atteintes aux droits à la vie privée des citoyens, etc.
Mais les positions ne sont pas toujours bien tranchées:

- Comme le souligne Eric Chabrow[24], M. Romney n'a pas exprimé clairement sa position sur la question des pouvoirs du DHS et dans la pratique, son choix pourrait ne pas dépendre de contraintes purement managériales, d'opinions politiques conformes à celles de son parti (hostile au développement des pouvoirs du DHS) mais simplement du besoin de maintenir des alliés (clientélisme ?) à des postes clefs du DHS.
- Les républicains voudraient plus d'investissements; on constate que sous l'administration démocrate les budgets dédiés au cyber n'ont cessé de croître.
- Les républicains veulent une posture cyber offensive, l'administration Obama n'a jamais masqué ses intentions de durcissement de la posture de cyberdéfense, en développant des capacités militaires

Si consensus il y a, au-delà de la simple reconnaissance de l'enjeu majeur, c'est dans la volonté partagée de ne pas en faire un véritable sujet de débat de campagne électorale, attitude qui interroge[25].

II - Analyse des discours

2.1. Le corpus

Pour essayer d'aborder cette problématique nous avons analysé l'ensemble des discours[26] des Secrétaires à la défense américains sur la période 1° janvier 1995- 31 décembre 2012.

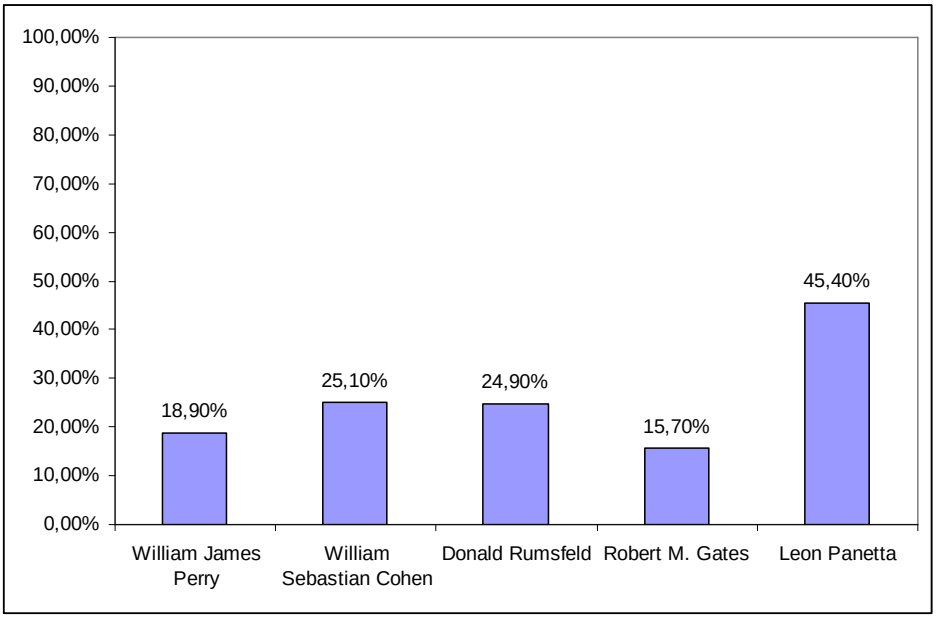
Les discours des secrétaires à la défense sont analysés en procédant à une lecture des objets suivants:

- Les références à la dimension, politique, partisane. Ont été indexés dans l'ensemble des discours les termes suivants: républicains (*Republicans*), démocrates (*Democrats*).
- La question du rôle de la technologie (pas spécifiquement cyber) dans les affaires militaires.
- Le traitement de la dimension « cyber ». Ont été indexés l'ensemble des termes suivants: cyberguerre (*cyberwar, cyber warfare*), guerre de l'information (information warfare), cyberterrorisme (*cyber terrorism, cyber terrorist*), cybersécurité (*cyber security*), cyberdéfense (*cyber defense*), cyber attaques (cyber attacks), internet, informatique (*computer*).

[22] http://www.bankinfosecurity.com/dhs-dod-to-tackle-jointly-cyber-defense-a-3010
[23] Eric Chabrow, *Cybersecurity : Obama vs Romney*, 5 novembre 2012, http://www.bankinfosecurity.com/cybersecurity-obama-vs-romney-a-5264/op-1
[24] Eric Chabrow, *Cybersecurity : Obama vs Romney*, 5 novembre 2012, http://www.bankinfosecurity.com/cybersecurity-obama-vs-romney-a-5264/op-1
[25] Anonyme, *Third presidential debate: Both candidates flunk cybersecurity*, 23 octobre 2012, Blog CSO Online, http://blogs.csoonline.com/security-leadership/2420/third-presidential-debate-both-candidates-flunk-cybersecurity
[26] Tels qu'ils sont proposés en téléchargement sur le site du Département de la défense http://www.defense.gov/speeches/SecDefArchive.aspx

Nom du secrétaire à la défense	Nombre de discours disponibles	Nombre de discours évoquant la question « cyber »
William James Perry	53	10
William Sebastian Cohen	167	42
Donald Rumsfeld	269	67
Robert M. Gates	255	40
Leon Panetta	97	44
Total	**841**	**203**

Statistiques sur la place du cyber dans les discours étudiés



Part, en %, des discours évoquant la dimension "cyber"

2.2. Sur l'approche partisane (Républicains et Démocrates)

William James Perry (discours étudiés: 1995-1997):

- Il est des sujets sur lesquels républicains et démocrates suivent la même ligne. Ainsi les présidents américains ont-ils su entretenir et développer des relations avec la Chine depuis 20 ans, et ce quelle que soir leur appartenance politique[27]. Il y a ainsi consensus sur l'importance des relations avec la Chine, consensus sur l'importance du maintien des positions en Europe après la fin de la guerre froide[28], etc.
- Mais démocrates et républicains divergent sur les moyens budgétaires qui doivent être accordés au financement de la Défense[29].

William Sebastian Cohen (discours étudiés: 1997- 2001):

[27] Ever Vigilant in the Asia-Pacific Region. Remarks by Secretary of Defense William J. Perry , the Japan Society, New York City, Tuesday, September 12, 1995

[28] U.S. Involvement Underwrites Bosnian Peace Bid. Prepared statement of Secretary of Defense William J. Perry and Gen. John M. Shalikashvili, USA, chairman of the Joint Chi, Senate Armed Services Committee, Tuesday, October 17, 1995

[29] Ten Things I Never Imagined Doing Five Years Ago, Remarks by Secretary of Defense William J. Perry at the Business Week Forum, Washington, D.C, Thursday, January 18, 1996

- Durant la seconde guerre mondiale, le fait de savoir si un général était démocrate ou républicain n'avait aucune importance. Il était patriote, se battait pour la nation[30]. Il n'y a pas de républicains, pas de démocrates, pas d'indépendants, il n'y a qu'une seule Amérique[31].
- La tradition de non partisanisme s'est effacée. Ce que Cohen regrette[32].
- Le plus haut niveau politique (président) souhaite qu'il n'y ait pas d'approche partisane en ce qui concerne la politique de sécurité[33]. Il ne doit pas y avoir de division politique quand il s'agit de politique de sécurité/défense[34]. Politique de défense mais aussi politique étrangère, ne doivent pas souffrir de divisions partisanes[35]. Lorsque Clinton nomme Cohen, c'est pour donner un signal fort de la nécessité d'une approche bipartisane, d'un partage, sur les sujets de sécurité/défense[36]. Cohen insiste d'ailleurs sur le fait qu'il est un républicain servant dans une administration démocrate[37]. Cohen véhicule ce message : il ne vient pas parler en tant que républicain ou en tant que démocrate, mais de sécurité et de défense de la nation américaine[38].

<u>Donald Rumsfeld (discours étudiés: 2001-2006):</u>

- Que le Congrès soit Républicain ou Démocrate, peu importe pour D. Rumsfeld[39]. Il y a des sujets de sécurité, et c'est là le plus important[40]. Tous les partis politiques doivent se retrouver derrière la bannière américaine. Cette fusion de la nation américaine est présente dans les discours concernant l'Iraq, lorsque des membres du Congrès viennent témoigner de ce qu'ils ont vu en Iraq, des menaces que représente S. Hussein. Derrière l'enjeu, il ne peut y avoir que consensus. Et ce consensus est bien sûr indispensable à l'atteinte de l'objectif poursuivi[41].
- Présidents républicains et démocrates ont géré les menaces pesant sur les Etats-Unis et le monde non pas en lançant de nouvelles guerres, des attaques préemptives, mais au contraire en renforçant

[30] Marshall's Legacy: A Guide for Tomorrow, Prepared Remarks of Secretary of Defense William S. Cohen , Virginia Military Institute, Marshall ROTC Seminar, Lexington, Va., , Wednesday, April 16, 1997
[31] National D-Day Museum Opening, Public Celebration, Remarks as Delivered by Secretary of Defense William S. Cohen, New Orleans Arena, New Orleans, Louisiana, Tuesday, June 06, 2000
[32] Marshall's Legacy: A Guide for Tomorrow, Prepared Remarks of Secretary of Defense William S. Cohen , Virginia Military Institute, Marshall ROTC Seminar, Lexington, Va., , Wednesday, April 16, 1997
[33] Coalition to Advance Sustainable Technology (CAST), As Delivered by Secretary of Defense William S. Cohen, Denver, Colo., Friday, June 26, 1998
[34] Mississippi Tribute to Armed Forces, Remarks by Secretary of Defense William S. Cohen, Biloxi, Miss. , Monday, October 19, 1998
[35] New England Council, Public Sector New Englander of the Year Award, Remarks as Delivered by Secretary of Defense William S. Cohen, Westin-Hotel Copley Place, Boston, Massachusetts , Thursday, September 28, 2000
[36] Ceremony Presenting Secretary William S. Cohen with the Nixon Center "Architect of the New Century" Award, As Delivered by Secretary of Defense William S. Cohen , The Mayflower Hotel Washington DC , Tuesday, December 08, 1998
[37] Distinguished Civilian Service Awards, Remarks as Delivered by Secretary of Defense William S. Cohen, The Pentagon, Washington, DC, Thursday, November 04, 1999
[38] National Convention of the Veterans of Foreign Wars and The Ladies Auxiliary, Remarks as Delivered by Secretary of Defense William S. Cohen, Midwest Express Center, Milwaukee, Wisconsin, Monday, August 21, 2000
[39] Testimony Before the Senate Armed Services Committee: Defense Strategy Review, As Delivered by Secretary of Defense Donald H. Rumsfeld and Chairman of the Joint Chiefs of Staff General Hugh Shelt, Hart Senate Office Building, Washington, DC, Thursday, June 21, 2001
[40] Testimony Before the Senate Armed Services Committee: Defense Strategy Review, As Delivered by Secretary of Defense Donald H. Rumsfeld and Chairman of the Joint Chiefs of Staff General Hugh Shelt, Hart Senate Office Building, Washington, DC, Thursday, June 21, 2001
[41] Fifth Anniversary of the September 11th Attacks, As Delivered by Secretary of Defense Donald H. Rumsfeld, Pentagon Mall, The Pentagon, Monday, September 11, 2006

les protections, en privilégiant la paix[42]. Une même ligne de conduite est assurée, quelle que soit la couleur politique.

Robert M. Gates (discours étudiés: 2006-2011):

- Les allusions au parti républicain ou démocrate renvoient à l'histoire des Etats-Unis, aux fondements mêmes de la politique de la nation américaine[43].
- Le Secrétaire souligne la continuité de la démarche politique des présidences successives, républicaines et démocrates, dans l'établissement de relations avec la Chine[44].

Léon Panetta (discours étudiés: 2011-2013):

- Le **Congrès doit jouer un rôle majeur** dans la préservation des capacités de défense des Etats-Unis, et il ne peut y avoir pour cela qu'une coopération pleine et entière entre le Congrès et l'exécutif, Républicains et Démocrates doivent suivre la même ligne, **éviter que des coupes budgétaires importantes ne produisent des effets désastreux**[45].
- Les distinctions Républicain/démocrate, libéral/conservateur, semblent s'effacer devant les enjeux supérieurs de la nation[46].
- Pour L. Panetta, l'époque où Républicains et Démocrates travaillaient en bonne intelligence est révolue[47], en tous cas éloignée. Il regrette les querelles politiciennes et l'époque où républicains et démocrates savaient travailler de concert[48]. Panetta rappelle que lorsqu'il était membre du Congrès, républicains et démocrates savaient défendre ensemble des projets. Il loue ces hommes qui savaient travailler ensemble[49]. Il s'inquiète de la situation politique actuelle, où il est difficile de trouver un consensus sur des questions de sécurité nationale, cela ayant pour effet une forme d'immobilisme au sein des affaires de défense, une situation préjudiciable à la sécurité qui a besoin quant à elle de dynamisme, d'action[50].
- Discours que l'on peut qualifier à la fois de critique et nostalgique de la part de L. Panetta, qui regrette l'époque des grandes figures politiques qui, au-delà de leurs différences, de leurs convictions, savaient faire corps face aux impératifs des enjeux nationaux[51].
- La sécurité et la défense ont besoin d'hommes et de femmes Républicains et Démocrates. Le discours se veut rassembleur. La défense n'aurait pas de couleur politique, car il s'agit de la défense de la nation.[52] Le consensus vers lequel doivent aller républicains et démocrates consiste à convenir du maintien d'un important budget pour la défense américaine car il faut que les Etats-

[42] Testimony of U.S. Secretary of Defense Donald H. Rumsfeld before the Senate Armed Services Committee regarding Iraq (Transcript), *Testimony as Delivered by Secretary of Defense Donald H. Rumsfeld, Dirksen Senate Office Building, Thursday, September 19, 2002*

[43] National Library for the Study of George Washington Groundbreaking Ceremony, As Delivered by Secretary of Defense Robert M. Gates, Mt. Vernon, VA, Thursday, April 14, 2011

[44] International Institute for Security Studies (Shangri-La Dialogue), As Delivered by Secretary of Defense Robert M. Gates, Shangri-La Hotel, Singapore, Saturday, June 04, 2011

[45] Lee H. Hamilton Lecture, As Delivered by Secretary of Defense Leon E. Panetta, Woodrow Wilson Center, Washington, DC, Tuesday, October 11, 2011

[46] Remarks by Secretary Panetta at Welcoming Ceremony for Deputy Secretary Carter, As Delivered by Secretary of Defense Leon E. Panetta, The Pentagon, Wednesday, November 09, 2011

[47] Center for National Policy Edmund S. Muskie Distinguished Public Service Award. As Delivered by Secretary of Defense Leon E. Panetta, Washington, D.C., Thursday, June 21, 2012

[48] Center for the Study of the Presidency and Congress (Eisenhower Award). As Delivered by Secretary of Defense Leon E. Panetta, Washington, D.C., Thursday, March 29, 2012

[49] Dean Acheson Lecture: "Building Partnership in the 21st Century". As Delivered by Secretary of Defense Leon E. Panetta, U.S. Institute of Peace, Washington, DC, Thursday, June 28, 2012

[50] Dean Acheson Lecture: "Building Partnership in the 21st Century". As Delivered by Secretary of Defense Leon E. Panetta, U.S. Institute of Peace, Washington, DC, Thursday, June 28, 2012

[51] Center for National Policy Edmund S. Muskie Distinguished Public Service Award. As Delivered by Secretary of Defense Leon E. Panetta, Washington, D.C., Thursday, June 21, 2012

[52] Center for National Policy Edmund S. Muskie Distinguished Public Service Award. As Delivered by Secretary of Defense Leon E. Panetta, Washington, D.C., Thursday, June 21, 2012

Unis conservent la plus grande armée du monde. Or Républicains et Démocrates assument conjointement la responsabilité de la baisse du budget de la défense (que déplore L. Panetta, même s'il reconnait que la société américaine connaît une grave crise budgétaire et économique).[53]

2.3. Le rôle de la technologie, discours moderniste

William James Perry (discours étudiés: 1995-1997):

- La **technologie a joué un rôle majeur** dans la victoire écrasante remportée lors de la campagne Tempête du Désert: "*Notre victoire dans Tempête du Désert fut le démonstration éclatante de l'avantage conféré dans le combat par l'avance technologique*". Les ordinateurs, logiciels, systèmes de communication sont des éléments clefs de cette nouvelle supériorité[54]. "*Tempête du Désert nous a montré que la technologie peut procurer non seulement la supériorité sur le champ de bataille, mais de plus réduit les pertes de façon spectaculaire*"[55].
- La technologie permet d'avoir une vision et une **maîtrise** de la globalité du champ d'affrontement, tout en interdisant à l'adversaire cet accès et cette maîtrise[56].
- L'avantage conféré est d'une évidence telle que les **réticences des chefs militaires** à l'introduction des nouvelles technologies ont été **levées**[57]. Politiques et militaires sont conscients de la nouvelle ère qui s'ouvre, la troisième vague de guerres et son champ de bataille numérique.
- Le **processus** de modernisation, **d'informatisation est engagé**. On enregistre de nouveaux succès: informatisation des systèmes militaires, des systèmes de C2, en Bosnie.[58] L'on met en évidence que des frappes aériennes détruisant des systèmes de contrôle et de défense aérienne ont des impacts à plus large échelle au niveau d'un pays, car les systèmes sont interconnectés[59].
- Désormais **le processus de modernisation/informatisation engagé devra être maintenu**: "... nous continuerons à maintenir une supériorité technologique sur le champ de bataille, en particulier en sachant tirer profit de l'avantage spectaculaire conférée par les technologies de l'information"[60]. La supériorité technologique est essentiellement fondée sur l'exploitation des NTIC[61].

[53] Association of Defense Communities. As Delivered by Secretary of Defense Leon E. Panetta, Monterey, California, Monday, August 06, 2012
[54] Nontraditional Programs Are Critical to Future Defense. Prepared remarks of Secretary of Defense William J. Perry, The U.S. Conference of Mayors, Washington, Thursday, January 26, 1995
[55] Linking Technology and National Security. Prepared remarks of Secretary of Defense William J. Perry , The Economics Engineering Systems Department Graduation, Stanford University, Stanford, Calif., Friday, June 16, 1995
[56] Squaring DoD's "Circle", Prepared Remarks of Secretary of Defense William J. Perry , Military Communications Conference, McLean, Va, Wednesday, October 23, 1996
[57] Linking Technology and National Security. Prepared remarks of Secretary of Defense William J. Perry , The Economics Engineering Systems Department Graduation, Stanford University, Stanford, Calif., Friday, June 16, 1995
[58] U.S. Policy on Bosnia Remains Consistent. Prepared statement by Secretary of Defense William J. Perry , the Senate Armed Services Committee and House National Security Committee, Wednesday, June 07, 1995
[59] Curbing Saddam's Military Adventures, Briefing As Delivered By Secretary of Defense William J. Perry and Gen. Joseph Ralston, USAF, vice chairman of the Joint Chie, Pentagon, Tuesday, September 03, 1996
[60] Building a Ready, Flexible, Responsive Force. Remarks by Secretary of Defense William J. Perry , the Regional Commerce and Growth Association, St. Louis, Friday, September 29, 1995
[61] Managing Danger: Prevent, Deter, Defeat, United States Department of Defense Secretary of Defense William J. Perry, Annual Report to the President and the Congress, Monday, March 04, 1996

- Les technologies nécessaires doivent être acquises auprès de **l'industrie privée**. Le défi consiste à pouvoir suivre le rythme de l'évolution technologique, car il est impératif de disposer des dernières technologies[62].
- Les **industriels** n'ont plus besoin de faire d'efforts pour convaincre les militaires et les hommes politiques des avantages à tirer de ces nouvelles technologies[63].
- Mais la modernisation de l'armée ne dépend pas uniquement de la volonté des chefs militaires ni des moyens technologiques disponibles sur le marché. La **politique d'acquisition** (règlementation) décide de la vitesse de la modernisation[64]. Des règles inadaptées pénaliseraient le fonctionnement de la défense (et par delà, seraient un risque pour la défense nationale).De nouvelles procédures d'acquisition ont donc été mises en place[65]. Cette évolution réglementaire des procédures d'acquisition apparaît comme un changement radical.

Dans ce discours on voit ainsi poindre d'autres problématiques: celle de la course au développement capacitaire et celle des budgets alloués à la défense, point de tension entre républicains et démocrates.

William Sebastian Cohen (discours étudiés: 1997- 2001):

- Il est **impératif de développer et acquérir**, intégrer les technologies qui exploitent pleinement la puissance de l'ère numérique[66]. Il faut pour cela assouplir, moderniser, rendre plus dynamique le système d'acquisition des technologies, notamment en informatisant le processus[67].
- L'image d'une armée moderne, informatisée, qui peut impressionner par son niveau technologique, l'avantage technologique **n'est jamais un acquis définitif.** Celles utilisées durant la campagne Tempête du Désert paraitraient aujourd'hui (1998) dépassées. Il faut donc **maintenir les budgets d'acquisition.** Or ce sont au contraire des réductions budgétaires qui sont à déplorer[68]. Seule l'augmentation du budget de la défense accélèrera la modernisation, l'acquisition de nouvelles technologies et systèmes C4ISR[69].
- **L'armée utilise et utilisera de plus en plus internet pour ses activités**[70]. L'armée diffuse des documents sur le « web », elle effectue des achats sur le « web », tout ceci ayant pour effet de faire des économies[71]. La modernisation de l'armée (les soldats des forces armées modernes doivent être aussi bons en informatique qu'ils le sont au combat[72]; on est entré dans l'ère des cyber soldats, des

[62] Protecting the Nation Through Ballistic Missile Defense, Prepared Remarks Defense Secretary William J. Perry, George Washington University, Washington, Thursday, April 18, 1996
[63] Linking Technology and National Security. Prepared remarks of Secretary of Defense William J. Perry , The Economics Engineering Systems Department Graduation, Stanford University, Stanford, Calif., Friday, June 16, 1995
[64] Squaring DoD's "Circle", Prepared Remarks of Secretary of Defense William J. Perry , Military Communications Conference, McLean, Va, Wednesday, October 23, 1996
[65] Building a Ready, Flexible, Responsive Force. Remarks by Secretary of Defense William J. Perry , the Regional Commerce and Growth Association, St. Louis, Friday, September 29, 1995
[66] Presentation to the Annual Bernard Brodie Lecture, As Delivered by Secretary of Defense William S. Cohen, University of California at Los Angeles, Wednesday, October 28, 1998
[67] Time Has Come to Leap Into the Future, Prepared Remarks of Secretary of Defense William S. Cohen , Brookings Institution Board of Trustees, Washington,, Monday, May 12, 1997
[68] *Base Closure Pain Today can mean profits tomorrow, Prepared remarks by Secretary of Defense William S. Cohen , Washington, Thursday, January 29, 1998*
[69] New Defense Strategy: Shape, Respond, Prepare; *Prepared statement of Secretary of Defense William S. Cohen , Tuesday, February 03, 1998*
[70] Remarks as Prepared for Secretary Cohen to the National Defense Transportation Association, Remarks as Prepared for Secretary of Defense William S. Cohen, Houston, Texas, Monday, October 26, 1998
[71] Remarks as Prepared for Secretary Cohen to the Fortune 500 Forum Dinner Keynote Address, As Delivered by Secretary of Defense William S. Cohen, Pittsburgh, Pennsylvania, Friday, October 16, 1998
[72] Greater Tampa Chamber of Commerce, Remarks as Delivered by Secretary of Defense William S. Cohen, Tampa, Florida , Wednesday, December 08, 1999

cyber espions, un âge orwellien[73]) passe par l'intégration des technologies civiles dans les systèmes d'armes, l'intégration de puces d'ordinateurs grand public dans des systèmes d'armes[74]. Avec plus de 2 millions d'ordinateurs et 100 000 réseaux, le Département de la défense est plus efficace mais aussi totalement dépendant et donc plus vulnérable[75]. Dans les 4 prochaines années le département de la défense dépensera 3.6 milliards de $ dans la sécurité informatique[76]. Une transformation s'opère au sein du fonctionnement des armées, la logistique, la modernisation, les processus d'acquisition. Il s'agit de marier à la fois économies budgétaires et acquisition, modernisation[77].

- Le discours moderniste peut être tempéré. les avantages de la technologie peuvent se retourner contre celui qui les utilise[78]: l'internet, par la mise en accès des connaissances (science, technologie) ne va qu'accentuer le processus d'acquisition de moyens de destruction par les adversaires[79]. Apparaît le **discours sur la menace** qui pèse sur les systèmes informatiques, et sur la société toute entière dépendante de ces systèmes d'information: menace de l'incident technique, menace de l'attaque de hackers contre ces systèmes essentiels[80]. Si les hackers parviennent à attaquer les systèmes critiques, cela aura un impact sur nos vies[81]. Les systèmes de l'armée américaine ont subi des cyberattaque lorsqu'elle était présente dans le Golfe persique[82].
- Le passage à l'an 2000 fut un problème sérieux de sécurité: l'exemple donné évoque la possible réaction d'un Etat comme la Russie qui constaterait que ses systèmes d'information ne fonctionnent plus le 31 décembre 1999. Le pays pourrait penser qu'il est victime d'une opération de l'Amérique ou d'un autre Etat. Le passage à l'an 2000 devait donc bien être géré[83] comme un problème de sécurité[84].

<u>Donald Rumsfeld (discours étudiés: 2001-2006):</u>

- Il est important d'assurer la domination dans le cyberspace, comme cela est fait dans l'espace de bataille traditionnel. La RAM a transformé les forces, en exploitant la force de la technologie et la

[73] Economic Strategy Institute Global Forum, Remarks as Delivered by Secretary of Defense William S. Cohen , Ronald Reagan International Trade Center, Washington, D.C. , Monday, May 15, 2000
[74] Remarks as Prepared for Secretary Cohen to the Fortune 500 Forum Dinner Keynote Address, As Delivered by Secretary of Defense William S. Cohen, Pittsburgh, Pennsylvania, Friday, October 16, 1998
[75] Microsoft Corporation, Remarks as Prepared for Delivery by Secretary of Defense William S. Cohen , Washington, Thursday, February 18, 1999
[76] Microsoft Corporation, Remarks as Prepared for Delivery by Secretary of Defense William S. Cohen , Washington, Thursday, February 18, 1999
[77] Remarks to the Department of Defense Conference on Base Reuse "Recognizing a Decade of Community Redevelopment", Remarks as Delivered by Secretary of Defense William S. Cohen , Crystal City Arlington, Virginia, Monday, March 22, 1999
[78] Chicago Council on Foreign Relations/Chicagoland Chamber of Commerce Mid-America Club, Remarks as Delivered by Secretary Of Defense William S. Cohen, Chicago, Illinois, Tuesday, September 26, 2000
[79] Secretary Cohen's speech addresses R&D, threats to national security, As Delivered by Secretary of Defense William S. Cohen, Boston Marriott Copley Place, Boston, Mass., Thursday, September 17, 1998
[80] Presentation to the Annual Bernard Brodie Lecture, As Delivered by Secretary of Defense William S. Cohen, University of California at Los Angeles, Wednesday, October 28, 1998
[81] Presentation to the Annual Bernard Brodie Lecture, As Delivered by Secretary of Defense William S. Cohen, University of California at Los Angeles, Wednesday, October 28, 1998
[82] Microsoft Corporation, Remarks as Prepared for Delivery by Secretary of Defense William S. Cohen , Washington, Thursday, February 18, 1999
[83] Air Mobility Museum, Dover Air Force Base, Remarks as Delivered by Secretary of Defense William S. Cohen , Dover, Delaware , Wednesday, December 15, 1999
[84] Remarks to the Boston Chamber of Commerce, Remarks as prepared Secretary of Defense Willaim S. Cohen, Boston Marriot Copley Place, Boston, Mass., Monday, November 09, 1998

mettant au service de la force des idées[85]. Sur le champ de bataille numérisé, réseau centrique, l'objectif est d'exploiter la dominance de l'information[86].

- Les ordinateurs et les communications ont permis la résurgence de la suprématie économique américaine[87]. Mais les Etats-Unis sont aussi vulnérables que n'importe quel Etat du monde en raison de leur dépendance aux réseaux[88]. Les défis pour la défense sont donc immenses. L'environnement international est totalement nouveau : couverture satellites 24/24, attaques terroristes, catastrophes, opérations de combat, téléphones cellulaires, caméras numériques, internet, emails, journalistes embarqués, sensibilité pour la protection des documents et de l'information classifiée, et un gouvernement qui est toujours organisé pour la période industrielle, pas pour l'ère de l'information. Qui plus est, l'armée est engagée dans un conflit non conventionnel, asymétrique, forme d'affrontement pour lequel elle n'est pas organisée, entraînée, équipée. Elle doit affronter des adversaires qui ne sont pas étouffés par les contraintes bureaucratiques et légales. La tâche est dantesque[89].

Robert M. Gates (discours étudiés: 2006-2011):

- Tout le spectre des capacités militaires sur terre, air, mer dépend des communications numériques et des réseaux de données[90].

Léon Panetta (discours étudiés: 2011-2013):

- Il faut retenir les leçons des conflits récents, et poursuivre les développements technologiques, les cyber capacités, renforcer les capacités de projection des forces dans des zones hostiles, mener des opérations spéciales. Il faut également protéger les programmes de science et de technologie[91].
- Les évolutions permanentes doivent permettre de développer une armée capable de vaincre sur tous les terrains, y compris le cyberespace[92].
- Le budget de la cyberdéfense est de l'ordre de 3.4 milliards de $ et permet de développer des cybercapacités pour affronter toutes les nouvelles formes de menaces actuelles et futures[93].

2.4. Guerre de l'information et opérations d'information

William James Perry (discours étudiés: 1995-1997):

- *Pas de référence*

[85] White House Swearing-In of the Secretary of Defense, Remarks as Delivered by Secretary of Defense Donald Rumsfeld , The Oval Office, The White House Washington, DC , Friday, January 26, 2001

[86] Testimony by Secretary of Defense Donald H. Rumsfeld on Crusader Artillery System before Senate Armed Services Committee (transcript), *As Delivered by Secretary of Defense Donald H. Rumsfeld, Dirksen Senate office building, Washington, D.C. , Thursday, May 16, 2002*

[87] Armed Forces Farewell to President William Jefferson Clinton, Remarks as Delivered by Secretary of Defense Williams S. Cohen, Conmy Hall, Fort Myer Arlington, Virginia, Friday, January 05, 2001

[88] Transcript of Testimony by Secretary of Defense Donald H. Rumsfeld on Homeland Security before Senate Appropriations Committee, *As Delivered by Secretary of Defense Donald H. Rumsfeld, Senate Dirksen Office Building, Tuesday, May 07, 2002*

[89] Secretary Rumsfeld-Budget Testimony-Senate House Armed Services Committee, As Prepared for Delivery by Secretary of Defense Donald H. Rumsfeld, Washington, DC, Thursday, February 17, 2005

[90] Submitted Statement on DoD Challenges to the Senate Armed Services Committee, As Submitted by Secretary of Defense Robert M. Gates, Room SD-106, Dirksen Senate Office Building, Washington, D.C., Tuesday, January 27, 2009

[91] Statement on Major Budget Decisions. As Delivered by Secretary of Defense Leon E. Panetta, Pentagon Briefing Room, Thursday, January 26, 2012

[92] Greater El Paso Chamber of Commerce. As Delivered by Secretary of Defense Leon E. Panetta, El Paso, Texas, Thursday, January 12, 2012

[93] Submitted Statement -- Senate Budget Committee (Budget Request). As Submitted by Secretary of Defense Leon E. Panetta, Capitol Hill, Washington D.C., Tuesday, February 28, 2012

William Sebastian Cohen (discours étudiés: 1997- 2001):

- La guerre de l'information fait partie, au même titre que le terrorisme et les armes de destruction massive, de moyens asymétriques ou non conventionnels utilisés par les acteurs des nouvelles menaces dans le monde[94].
- Pour se protéger des opérations de guerre de l'information, il faut des moyens technologiques à la hauteur: "Nous avons besoin de forces qui puissent s'engager plus efficacement; ce qui implique de disposer des dernières technologies de pointe, de stocks importants de munitions de précision, et de forces qui puissent survivre à des attaques chimiques, biologiques, nucléaire et à la guerre de l'information"[95].
- La guerre de l'information, ainsi que le terrorisme, la guerre chimique, bactériologique, sont des éléments du nouveau monde, qualifié de *Grave New World*[96].
- Le nombre d'armes, champs de bataille, menaces, dangers, se diversifie: armes chimiques, biologiques, guerre de l'information[97]. Si la notion de guerre de l'information" est utilisée à plusieurs reprises, elle n'est toutefois pas définie.

Donald Rumsfeld (discours étudiés: 2001-2006):

- Guerre de l'information (information warfare) et opérations d'information (information operations) sont deux notions qui demeurent non définies dans le discours.
- La guerre de l'information est une menace au même titre que la menace chimique, bactériologique[98]. Les réseaux civils critiques pour la vie de l'économie sont soumis à la guerre de l'information[99], qui joue un rôle de plus en plus important.
- Il faut savoir intégrer les opérations d'information dans les opérations militaires conventionnelles.
- Les projets et budgets dédiés au développement des capacités de guerre de l'information, d'opérations d'information, demeurent secrets[100].
- La guerre de l'information prenant de plus en plus de place dans les affaires militaires, de la capacité à assurer la sécurité des réseaux militaires dépendra le succès dans les combats[101].

Robert M. Gates (discours étudiés: 2006-2011):

- La place des opérations d'information s'est inversée : il s'agissait par le passé de mener des opérations militaires soutenues, accompagnées par des opérations d'information. Il s'agirait

[94] Partnerships Grow In Western Hemisphere, Prepared Remarks of Secretary of Defense William S. Cohen , The Western Hemisphere Symposium, Miami,, Tuesday, April 15, 1997
[95] International Institute for Strategic Studies, Remarks as Delivered by Secretary of Defense William S. Cohen , Hotel del Coronado, San Diego, California , Thursday, September 09, 1999
[96] National Women's Law Center 1999 Annual Dinner, Remarks as Delivered by Secretary of Defense William S. Cohen , Washington Hilton, Washington, DC, Wednesday, November 03, 1999
[97] George C. Marshall European Center for Strategic Studies, Remarks as Delivered by Secretary of Defense William S. Cohen, Garmisch, Germany, Wednesday, December 01, 1999
[98] White House Swearing-In of the Secretary of Defense, Remarks as Delivered by Secretary of Defense Donald Rumsfeld , The Oval Office, The White House Washington, DC , Friday, January 26, 2001
[99] Testimony before the House Appropriations Committee: Fiscal Year 2002 Defense Budget Request, As Delivered by Secretary of Defense Donald H. Rumsfeld, Chairman of the Joint Chiefs of Staff General Hugh Shelton,, Rayburn House Office Building, Washington, DC, Monday, July 16, 2001
[100] Transcript of Secretary Rumsfeld at Town hall Meeting at Nellis Air Force Base, Nevada, Remarks as Delivered by Secretary of Defense Donald Rumsfeld, Nellis Air Force Base, Wednesday, February 20, 2002
[101] Fiscal Year 2003 Defense Budget Testimony – Senate Armed Services Committee, Prepared Testimony of Secretary of Defense Donald H. Rumsfeld, Senate Armed Services Committee, Washington, D.C., Tuesday, February 05, 2002

aujourd'hui de mener des campagnes stratégiques de communication accompagnées d'opérations militaires[102].

Léon Panetta (discours étudiés: 2011-2013):

- *Pas de référence*

2.5. Cyberattaques

William James Perry (discours étudiés: 1995-1997):

- *Pas de référence*

William Sebastian Cohen (discours étudiés: 1997- 2001):

- Le monde a changé. Le quotidien est désormais fait de cyberattaques émanant d'individus agissant de chez eux ou d'acteurs étatiques, de cyber soldats, de l'étranger[103]. Des Etats sont en train de se doter de forces spécifiques pour mener des cyberattaques[104].

Donald Rumsfeld (discours étudiés: 2001-2006):

- La période actuelle sera sans doute plus tard perçue comme ayant été période de transition, passage d'un monde où les menaces étaient comprises à un monde de menaces mal comprises. Les cyberattaques sont l'une des marques de cette nouvelle période[105].
- Notre dépendance à l'informatique et aux réseaux fait de ceux-ci des cibles pour de nouvelles formes d'attaques[106]. Les cyberattaques, en augmentation constante[107], contre les systèmes critiques dans un monde hyper connecté peuvent avoir des effets comparables à ceux d'un conflit armé[108]. Les cyberattaques sont d'autant plus faciles à imaginer que tous les acteurs partagent les mêmes vulnérabilités[109].
- Aux yeux de Rumsfeld, arrivant au terme de son mandat, la plus grande des menaces réside dans les cyberattaques[110], en raison de la dépendance de toute la société au cyber. Les cyberattaques seront inévitables dans les prochaines années.

[102] National Defense University (Washington, D.C.), As Delivered by Secretary of Defense Robert M. Gates, Washington, D.C., Monday, September 29, 2008
[103] Groundbreaking for the World War II Memorial, Remarks as Delivered by Secretary of Defense William S. Cohen, The National Mall, Washington, DC, Saturday, November 11, 2000
[104] Center for Strategic and International Studies, Remarks as Delivered by Secretary of Defense William S. Cohen, Washington, DC, Monday, October 02, 2000
[105] Armed Forces Day, Joint Services Open House, Remarks as Delivered by Secretary of Defense Donald H. Rumsfeld, Andrews Air Force Base, Maryland, Friday, May 18, 2001
[106] Testimony Before the Senate Armed Services Committee: Defense Strategy Review, As Delivered by Secretary of Defense Donald H. Rumsfeld and Chairman of the Joint Chiefs of Staff General Hugh Shelt, Hart Senate Office Building, Washington, DC, Thursday, June 21, 2001
[107] Testimony Before the Senate Armed Services Committee: Defense Strategy Review, As Delivered by Secretary of Defense Donald H. Rumsfeld and Chairman of the Joint Chiefs of Staff General Hugh Shelt, Hart Senate Office Building, Washington, DC, Thursday, June 21, 2001
[108] National Press Club Newsmakers Luncheon, Remarks as Delivered by Secretary of Defense William S. Cohen, National Press Club, Washington, DC, Wednesday, January 10, 2001
[109] NATO Nuclear Planning Group (NPG), Statement as Prepared for Delivery by Secretary of Defense Donald H. Rumsfeld , Brussels, Belgium , Tuesday, December 18, 2001
[110] Presenter: Secretary of Defense Donald H. Rumsfeld. December 10, 2006, Town Hall Meeting with Secretary of Defense Donald Rumsfeld at Al Asad Air Base, Iraq

Robert M. Gates (discours étudiés: 2006-2011):

- Les cyberattaques évoquées sont de nature guerrière, militaire (Russie-Géorgie en 2008[111]). Il est question de la guerre, qui n'est plus homogène, simple à comprendre. Elle est désormais complexe, les belligérants peuvent utiliser des combinaisons multiples de méthodes, d'armes, de manières de combattre, et les enjeux peuvent même être divers.
- Apparaît la question du niveau de cyberattaque qui pourrait être qualifié d'acte de guerre. Cette notion "d'acte de guerre" n'était pas encore clairement apparue jusqu'alors[112].

Léon Panetta (discours étudiés: 2011-2013):

- A côté de dangers connus, traditionnels, comme le danger nucléaire, il faut se préparer à affronter de nouvelles menaces, comme celle des cyberattaques. L'Etat enregistre de nombreuses cyberattaques de la part d'acteurs étatiques et non-étatiques, et la perspective d'une attaque contre les infrastructures critiques paralysant tout le pays fait partie des possibilités[113]. Le monde dans lequel nous vivons est fait d'une multitude de dangers grandissant: violence extrémiste, prolifération nucléaire, puissances émergentes, cyberattaques[114]. Il faut donc se préparer à affronter ces menaces émergentes[115].

Nous retiendrons des discours de L. Panetta celui prononcé le 12 octobre 2012, essentiel pour la question du cyber, car lui étant entièrement dédié[116], intitulé "*Defending the Nation from Cyber Attack":*

- Il faut sécuriser le cyber domaine, le **cyberespace**, comme cela a été fait pour les autres domaines
- Le **cyberespace** est la nouvelle frontière, car il ouvre la voie à de nouvelles possibilités pour l'avenir, l'économie, le monde… La nouvelle frontière est celle des nouvelles possibilités, des nouveaux rêves pour la société moderne.
- Un espace, des possibilités, du positif ; mais en face des aspects négatifs, des **menaces**, et l'obligation de sécuriser. Internet est ouvert, il est aussi un nouveau terrain pour les **affrontements**
- La menace va au-delà de la simple criminalité, bien connue. Des **actes de terrorisme ou opérations étatiques** pourraient **paralyser la nation**. Un risque réel de cyber Pearl Harbor existe, défini comme une attaque qui provoquerait des dommages matériels importants et des pertes de vies humaines, de nature à paralyser le pays, choquer la nation et créer un sentiment profond de vulnérabilité.
- Il y a toujours plus inquiétant, alarmant, à l'exemple du ver Shamoon qui a détruit 30 000 ordinateurs. Ces attaques confirment et alimentent des **scénarios toujours plus pessimistes.** L'industrie est visée, dans son cœur, les agresseurs disposent de capacités qui leur donnent accès à des opérations destructrices. Des scénarios plus pessimistes envisagent des cyberattaques simultanées contre plusieurs systèmes critiques. **Pour faire face à ces menaces**, les agences de renseignement travaillent, le Département d'Etat agit pour créer un consensus international sur les rôles et responsabilités des nations dans la sécurisation du cyberespace, et le département de la défense a aussi son rôle à jouer. Le DoD a un rôle essentiel de soutien. Il ne s'agit pas pour lui de monitorer les ordinateurs des citoyens, mais d'assurer son rôle de défense de la nation comme il le

[111] National Defense University (Washington, D.C.), As Delivered by Secretary of Defense Robert M. Gates, Washington, D.C., Monday, September 29, 2008
[112] Carnegie Endowment for International Peace (Washington, D.C.), As Delivered by Secretary of Defense Robert M. Gates, Washington, D.C., Tuesday, October 28, 2008
[113] Lee H. Hamilton Lecture, As Delivered by Secretary of Defense Leon E. Panetta, Woodrow Wilson Center, Washington, DC, Tuesday, October 11, 2011
[114] Carnegie Europe (NATO), As Delivered by Secretary of Defense Leon E. Panetta, Brussels, Belgium, Wednesday, October 05, 2011
[115] DIA 50th Anniversary Gala, As Delivered by Secretary of Defense Leon E. Panetta, Washington, DC, Saturday, October 01, 2011
[116] Defending the Nation from Cyber Attack, (Business Executives for National Security), As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012

fait par ailleurs. Il développe pour cela de nouvelles capacités de cybersécurité, la part la plus importante de l'investissement se portant sur la formation et le recrutement de cyberguerriers. Le DoD s'est doté de capacités de cyberattaques permettant d'empêcher des cyberattaques ou d'y répondre. Sa **stratégie de dissuasion** consiste à faire savoir que les Etats-Unis sont disposés à répliquer, à se défendre, et renforcent leurs systèmes pour les rendre plus difficilement attaquables.
- Il est important de noter que ce discours sur la cyberdéfense ne fait pas une seule fois mention des notions partisanes (républicains/démocrates, libéraux/conservateurs). Il ne renvoie pas non plus à la notion de guerre froide.
- Le discours utilise un large spectre de notions liées au cyber : cyberattaque, cyber intrusion, cyber Pearl Harbor, cybersécurité, cybermenace, cybercapacité, cyber commandement, cyberforce, cyber opérations, cyberguerriers, cyberadversaires.

2.6. Cyberguerre

William James Perry (discours étudiés: 1995-1997):

- *Pas de référence*

William Sebastian Cohen (discours étudiés: 1997- 2001):

- La cyberguerre est l'une des caractéristiques du nouveau monde de menaces dans lequel nous vivons, menaces ayant pour seules limites la science et l'imagination des antagonistes 'armes chimiques, bactériologiques, informatiques...)[117]. La sécurité ne doit plus gérer des menaces conventionnelles, c'est-à-dire celles pour lesquelles elle était préparée, formée, conçue depuis des siècles: des agressions régionales, lutter contre des Etats voyous, etc.
- Des Etats mettent en place des cellules de professionnels dont la mission est de trouver les moyens d'interrompre les infrastructures américaines (transports, finances, production d'énergie...)[118]. Les Etats-Unis doivent se protéger contre ces possibilités. Des agences de sécurité dédiées (Joint Task Force for Civil Support; Defense Threat Reduction Agency...) travaillent à cette tâche de sécurisation. Les efforts portent sur la cyberguerre, avec une approche intégrée au sein du Space Command[119].

Donald Rumsfeld (discours étudiés: 2001-2006):

- La cyberguerre ouvre de nouvelles vulnérabilités. Les adversaires asymétriques peuvent exploiter les nouvelles possibilités (missiles, terrorisme, cyberguerre…) parce que les Etats-Unis et pays modernes sont davantage vulnérables sur ces domaines qu'ils ne le sont dans la guerre traditionnelle[120].
- Le gouvernement, la défense, investissent beaucoup d'argent « pour une chose appelée cyberguerre – guerre de l'information »[121]. Doit-on entendre dans cette formule que les deux concepts ne parviennent à se démarquer, qu'il s'agit de la même chose dans l'esprit de D. Rumsfeld?

[117] U.S. Leadership Vital to International Stability, Prepared remarks of Secretary of Defense William S. Cohen , University of Maine, Orono, Maine, Friday, March 20, 1998
[118] National Convention of the Veterans of Foreign Wars and The Ladies Auxiliary, Remarks as Delivered by Secretary of Defense William S. Cohen, Midwest Express Center, Milwaukee, Wisconsin, Monday, August 21, 2000
[119] Center for Strategic and International Studies, Remarks as Delivered by Secretary of Defense William S. Cohen, Washington, DC, Monday, October 02, 2000
[120] Testimony Before the Senate Armed Services Committee: Fiscal Year 2002 National Defense Authorization Budget Request, As Delivered by Secretary of Defense Donald H. Rumsfeld, Chairman of the Joint Chiefs of Staff General Hugh Shelton,, Dirksen Senate Office Building, Washington, DC, Thursday, June 28, 2001
[121] Testimony before the House Appropriations Committee: Fiscal Year 2002 Defense Budget Request, As Delivered by Secretary of Defense Donald H. Rumsfeld, Chairman of the Joint Chiefs of Staff General Hugh Shelton,, Rayburn House Office Building, Washington, DC, Monday, July 16, 2001

- Les CNO (Computer Network Operations) seraient conçues pour faire face à la cyberguerre[122].
- L'internet dont parle Rumsfeld[123], cet espace numérique, est tout autant exploité par l'armée américaine dans ses efforts d'informatisation, de maîtrise informationnelle, d'opérations d'informations, que par des adversaires qui savent recourir à toutes les possibilités nouvelles offertes, et qui plongent le conflit, l'affrontement, dans un environnement totalement imprégné de ces technologies et moyens nouveaux, au bénéfice des acteurs asymétriques. Le cyberespace et les cyber opérations dont parle Rumsfeld sont celles d'un chef de guerre, celles d'une armée en guerre et qui affronte un adversaire contre lequel elle n'était pas préparée véritablement à combattre.

Robert M. Gates (discours étudiés: 2006-2011):

- La montée en puissance des capacités de cyberguerre chinoises constitue une potentielle menace pour l'armée américaine[124]. La création du cyber commandement apparaît comme l'une des solutions à la nécessaire adaptation de l'armée à l'environnement du monde moderne, fait de nouvelles menaces, où il est indispensable, vital, d'assurer la défense, la sécurité du cyberespace sur lequel repose l'armée.[125]

Léon Panetta (discours étudiés: 2011-2013):

- Le soutien des services de renseignement est indispensable dans la cyberguerre[126].
- La cyberguerre fait partie des nouveaux challenges de la sécurité[127].
- le DoD investit dans des systèmes de drone et des moyens de cyberguerre, indispensables à la mission de la Langley Air Force Base[128].

2.7. Cyberterrorisme

William James Perry (discours étudiés: 1995-1997):

- *Pas de référence*

William Sebastian Cohen (discours étudiés: 1997- 2001):

- Les cyber terroristes frappent notre Talon d'Achille de leurs flèches empoisonnées[129].

[122] Testimony before the House Appropriations Committee: Fiscal Year 2002 Defense Budget Request, As Delivered by Secretary of Defense Donald H. Rumsfeld, Chairman of the Joint Chiefs of Staff General Hugh Shelton,, Rayburn House Office Building, Washington, DC, Monday, July 16, 2001
[123] Town Hall Meeting, As Delivered by Secretary of Defense Donald H. Rumsfeld, Al Asad Air Base, Iraq, Sunday, December 10, 2006
[124] National Defense University (Washington, D.C.), As Delivered by Secretary of Defense Robert M. Gates, Washington, D.C., Monday, September 29, 2008 ; Submitted Statement on DoD Challenges to the Senate Armed Services Committee, As Submitted by Secretary of Defense Robert M. Gates, Room SD-106, Dirksen Senate Office Building, Washington, D.C., Tuesday, January 27, 2009
[125] Submitted Statement Senate Armed Services Committee (Budget Request), As Submitted by Secretary of Defense Robert M. Gates, Room SD-G50, Dirksen Senate Office Building, Washington, D.C., Tuesday, February 02, 2010
[126] DIA Change of Director. As Delivered by Secretary of Defense Leon E. Panetta, Bolling AFB, Washington D.C., Tuesday, July 24, 2012
[127] Institute for Defense Studies and Analyses: "The U.S. and India: Partners in the 21st Century". As Delivered by Secretary of Defense Leon E. Panetta, New Delhi, India, Wednesday, June 06, 2012
[128] Hampton Roads Chamber of Commerce, As Delivered by Secretary of Defense Leon E. Panetta, Hampton Roads, VA , Friday, October 19, 2012
[129] Ohio Wesleyan University Grad, As Delivered by Secretary of Defense William S. Cohen, Ohio Wesleyan University, Ohio, Sunday, May 10, 1998

- Le plus grand défi de l'avenir ne réside pas tant dans le terrorisme traditionnel que dans ses nouvelles formes: cyber, biologique, chimique[130].
- Le cyberterrorisme est défini comme toutes cyberattaques menées contre les infrastructures critiques[131]: cyberattaques possibles contre le DoD, la NSA, le système de santé, les banques, les systèmes de contrôle aérien, etc.[132]
- Les cyberterroristes sont de jeunes gens, qui savent utiliser les ordinateurs et s'en servir pour attaquer les infrastructures sensibles, vitales[133].
- Le cyberterrorisme est une menace de nature totalement nouvelle[134]. Le monde fait face à de nouvelles menaces, une nouvelle anarchie ("*The Coming Anarchy*", pour reprendre le titre d'un ouvrage de Robert Kaplan) dont le terrorisme informatique est l'une des modalités[135].

Donald Rumsfeld (discours étudiés: 2001-2006):

- Les Etats-Unis sont qualifiés de cyber-nation. Cette nation sera de plus en plus soumise à des attaques cyberterroristes[136].
- Il y aura de plus en plus d'assauts de la part des cyberguerriers[137] (on ne comprend pas dans ce discours si les cyber-soldats dont il est question sont les acteurs du cyberterrorisme ou s'il s'agit de deux sources distinctes de la menace).
- Affirmation de l'existence de cellules, unités de cyber-soldats déployées dans plusieurs pays (mais aucun pays n'est mentionné dans le discours)[138].
- Les menaces actuelles peuvent être moins visibles que durant la guerre froide, mais elles ne sont pas moins létales ou catastrophiques, destructrices. Les menaces s'additionnent : conflits ethniques, nationalismes, crise économique, attaques cyberterroristes… [139] La dimension cyber apparaît toujours comme une couche supplémentaire dans l'ensemble des menaces qui se superposent. Image d'un monde chaotique, où le chaos et l'anarchie ne sont plus seulement le fait des Etats, mais d'acteurs plus diffus.
- Le monde post-guerre froide est plus intégré, les armes et technologies qui n'étaient accessibles qu'à un certain nombre prolifèrent et y accèdent Etats et entités non étatiques. Si le monde semble à l'abri d'une menace de guerre nucléaire massive, d'autres formes de menaces sont apparues, dont le cyberterrorisme[140].
- Le cyberterroriste est placé au même niveau de dangerosité que les marchands de plutonium et les dictateurs, dans un contexte de prolifération des armes de destruction massive.

---

[130] Ceremony Presenting Secretary William S. Cohen with the Nixon Center "Architect of the New Century" Award, Remarks As Delivered by Secretary of Defense William S. Cohen , The Mayflower Hotel Washington DC , Tuesday, December 08, 1998

[131] Change of Command Ceremony, Commander-in-Chief US Pacific Command, Remarks as Prepared for Delivery by Secretary of Defense William S. Cohen , Camp Smith, Hawaii, Saturday, February 20, 1999

[132] John Goodwin Tower Center for Political Studies, Southern Methodist University, Remarks as Delivered by Secretary of Defense William S. Cohen, Dallas, Texas, Wednesday, November 10, 1999

[133] John Goodwin Tower Center for Political Studies, Southern Methodist University, Remarks as Delivered by Secretary of Defense William S. Cohen, Dallas, Texas, Wednesday, November 10, 1999

[134] Remarks at the Alaska Salute to the Armed Forces, Remarks as Delivered by Secretary of Defense William S. Cohen , Anchorage, Alaska , Friday, February 19, 1999

[135] American Turkish Council, Remarks as Delivered by Secretary of Defense William S. Cohen, Grand Hyatt Hotel, Washington, DC, Friday, March 31, 2000

[136] National Press Club Newsmakers Luncheon, Remarks as Delivered by Secretary of Defense William S. Cohen, National Press Club, Washington, DC, Wednesday, January 10, 2001

[137] National Press Club Newsmakers Luncheon, Remarks as Delivered by Secretary of Defense William S. Cohen, National Press Club, Washington, DC, Wednesday, January 10, 2001

[138] National Press Club Newsmakers Luncheon, Remarks as Delivered by Secretary of Defense William S. Cohen, National Press Club, Washington, DC, Wednesday, January 10, 2001

[139] Preserving History's Greatest Alliance, By Secretary of Defense William S. Cohen, As Printed in The Washington Post, Monday, January 08, 2001

[140] Munich Conference on European Security Policy, Remarks as Delivered by Secretary of Defense Donald H. Rumsfeld, Munich, Germany, Saturday, February 03, 2001

- Face à toutes ces menaces la meilleure manière de préserver la paix est de redéfinir la guerre. Il faut construire le futur avec de nouveaux concepts, de nouvelles stratégies[141].

Robert M. Gates (discours étudiés: 2006-2011):

- Les terroristes pourraient utiliser les armes nouvelles. On note que progressivement dans le discours du DoD apparaissent tous les termes qui vont constituer le lexique de la cyberdéfense. Il est ici question des cyber-armes, terme qui n'était encore pas apparu dans les discours précédents[142].
- Constat de l'inadéquation des forces armées par rapport aux menaces du monde nouveau. R. Gates fait référence à un discours de G. Bush, alors sénateur, intitulé "*A period of Consequencies*" (prononcé le 23 septembre 1999)[143], dans lequel il formule ce constat et inscrit les cyberterroristes au même degré de dangerosité que les dictateurs[144]

Léon Panetta (discours étudiés: 2011-2013):

- Est cyberterroriste une attaque qui serait perpétrée par des Etats ou des groupes extrémistes violents, et dont les effets seraient destructeurs, paralyseraient la nation[145]. Cette menace va bien au-delà de la simple criminalité.

2.8. Cyberespace

William James Perry (discours étudiés: 1995-1997):
- *Pas de référence*

William Sebastian Cohen (discours étudiés: 1997- 2001):
- Une référence évoquant le cyberespace comme vecteur de communication utilisé pour diffuser son discours[146].

Donald Rumsfeld (discours étudiés: 2001-2006):

- Dans la guerre contre le terrorisme il n'y a pas de règles préétablies. Cette guerre introduira un nouveau vocabulaire. Lorsqu'il sera question d'envahir/occuper le territoire de l'ennemi, cela pourra signifier occuper son cyberespace. Le cyberespace est associé à la notion de territoire[147].
- Les règles de cette lutte contre le terrorisme ne sont pas préétablies, elles le seront au fur et à mesure, en fonction des objectifs, des enjeux, du contexte. Les règles du déploiement des troupes

[141] Testimony by Secretary of Defense Donald H. Rumsfeld on Crusader Artillery System before Senate Armed Services Committee (transcript), *As Delivered by Secretary of Defense Donald H. Rumsfeld, Dirksen Senate office building, Washington, D.C. , Thursday, May 16, 2002*

[142] Special Operations Forces International Conference (Tampa, FL), As Delivered by Secretary of Defense Robert M. Gates, Tampa, FL, Wednesday, May 21, 2008

[143] http://www3.citadel.edu/pao/addresses/pres_bush.html "*We see the contagious spread of missile technology and weapons of mass destruction. We know that this era of American preeminence is also an era of car bombers and plutonium merchants and cyber terrorists and drug cartels and unbalanced dictators – all the unconventional and invisible threats of new technologies and old hatreds. These challenges can be overcome, but they can not be ignored*."

[144] Armed Forces Farewell to the President of the United States (Arlington, VA), As Delivered by Secretary of Defense Robert M. Gates, Arlington, VA, Tuesday, January 06, 2009

[145] Defending the Nation from Cyber Attack" (Business Executives for National Security) As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012

[146] Acquisition and Logistics Reform Week Kick-Off, Remarks as Delivered by Secretary of Defense William S. Cohen, The Pentagon, Washington DC , Tuesday, June 08, 1999

[147] A New Kind Of War, as published in The New York Times Secretary of Defense Donald H. Rumsfeld, No location specified, Thursday, September 27, 2001

ne sont pas prédéfinies. Dans cette guerre, tous les espaces de lutte contre le terrorisme sont donc exploitables. Le cyberespace est de ceux-là.

- D. Rumsfeld utilise l'expression « leur cyberespace », ce qui sous-entend « notre » cyberespace, des espace de communication, d'échange, propres à chaque acteur, et qu'il faudra exploiter, attaquer, défendre, comme des cibles particulières, des territoires particuliers. Ici la notion de *global commons* s'estompe dans une telle perspective.

Robert M. Gates (discours étudiés: 2006-2011):

- L'U.S. Air Force doit maintenir sa domination dans les airs, l'espace et le cyberespace[148]. L'une de ses missions est la protection du cyberespace[149].
- Espace et cyberespace sont les *global commons* du 21° siècle[150]. En conséquence, la gestion du cyberespace doit passer par la coopération, l'adhésion à des règles et mécanismes qui permettent de maintenir la paix[151]. Le cyberespace doit rester ouvert car l'économie mondialisée, globalisée en dépend[152].
- Les *global commons*, dont le cyberespace fait partie, sont soumis à des menaces étatiques et non étatiques, nouvelles, différentes de celles auxquelles les forces américaines se préparaient au sortir de la guerre froide[153]. Le cyberespace est menacé[154].
- Un chapitre de discours[155] est dédié au cyberespace : « Defending space and cyberspace »: toute l'armée est dépendante du cyberespace ; le vaste cyber territoire que doit défendre l'armée est soumis à d'incessantes cyberattaques, contre lesquelles elle se défend, se protège ; l'attaque russe en Géorgie (2008) a été précédée de vastes opérations de cyberattaques ; le texte évoque également la question estonienne (2007) soulignant les possibilités dont disposent désormais les hackers pour s'en prendre à un Etat[156]. Ce chapitre emploie toute une gamme de termes, sans jamais les définir : *network defense, network attack, cyber attack, cyberspace, digital, cyber defense*
- Le cyberspace est également nommé cyber territoire[157].
- La politique américaine pour la protection du cyberespace s'appuie sur les relations internationales: privilégier la communication, les forums, les échanges, pour développer une compréhension partagée au sein de la communauté internationale, éviter les mauvaises interprétations qui

[148] POW/MIA Recognition Day (Pentagon Parade Field), Remarks as Delivered by Secretary of Defense Robert M. Gates, Pentagon Parade Field, Friday, September 21, 2007

[149] Welcoming Ceremony for Air Force Chief of Staff Norton Schwartz (Washington, D.C.), As Delivered by Secretary of Defense Robert M. Gates, Washington, D.C., Tuesday, August 12, 2008

[150] Remarks to Air War College (Montgomery, AL), As Delivered by Secretary of Defense Robert M. Gates, Maxwell-Gunter Air Force Base, Montgomery, AL, Monday, April 21, 2008

[151] International Institute for Strategic Studies, As Delivered by Secretary of Defense Robert M. Gates, Singapore, Saturday, May 30, 2009

[152] Our Military Kids (Washington, D.C.), As Prepared for Delivery by Secretary of Defense Robert M. Gates, Washington, D.C., Monday, April 07, 2008

[153] Opening Summary -- Senate Armed Services Committee (Budget Request), As Delivered by Secretary of Defense Robert M. Gates, Room SD-G50, Dirksen Senate Office Building, Washington, D.C., Tuesday, February 02, 2010

[154] Defense Budget/QDR Announcement, As Delivered by Secretary of Defense Robert M. Gates, Arlington, VA, Monday, February 01, 2010

[155] Submitted Statement on DoD Challenges to the Senate Armed Services Committee, As Submitted by Secretary of Defense Robert M. Gates, Room SD-106, Dirksen Senate Office Building, Washington, D.C., Tuesday, January 27, 2009

[156] Submitted Statement on DoD Challenges to the Senate Armed Services Committee, As Submitted by Secretary of Defense Robert M. Gates, Room SD-106, Dirksen Senate Office Building, Washington, D.C., Tuesday, January 27, 2009

[157] Promotion of General Keith Alexander/Activation of CYBERCOM, As Prepared for Delivery by Secretary of Defense Robert M. Gates, National Security Agency, Ft. Meade MD, Friday, May 21, 2010

pourraient déboucher sur des conflits. Cette stratégie s'applique aussi bien pour les questions relatives au cyberespace qu'à l'espace maritime, terrestre, aérien…[158]

Léon Panetta (discours étudiés: 2011-2013):

- Le cyberespace est placé sous surveillance. Il voit émerger de nouvelles menaces: "*la DIA est restée vigilante, ne quittant jamais des yeux les nouvelles menaces qui nous font face - surveillant les ambitions nucléaires de la Corée du Nord et de l'Iran, observant les capacités militaires étrangères dans l'espace et le cyberespace*"[159].
- La défense du cyberespace vise à défendre les intérêts partagés avec d'autres Etats: une capacité à commercer librement, définir des règles, assurer la liberté de mouvement dans l'ensemble des *global commons* (air, mer, espace, cyberespace). Ces intérêts sont aussi ceux des alliés des Etats-Unis[160].
- Le cyberespace a transformé fondamentalement l'économie globale[161]
- L. Panetta rappelle d'ailleurs que l'une des missions du Département d'Etat est de créer un consensus international sur la responsabilité qui incombe aux Etats de sécuriser le cyberespace[162].

2.9. Cybersécurité et cyberdéfense

William James Perry (discours étudiés: 1995-1997):
- *Pas de référence*

William Sebastian Cohen (discours étudiés: 1997- 2001):
- *Pas de référence*

Donald Rumsfeld (discours étudiés: 2001-2006):
- La cyberdéfense est l'un des éléments de la nouvelle défense américaine, aux côtés des capacités de défense balistique, missiles de croisière, défense spatiale, et venant compléter la force nucléaire et les capacités conventionnelles[163].

Robert M. Gates (discours étudiés: 2006-2011):
- Un chapitre du discours prononcé le 13 mai 2009[164] est dédié à la cybersécurité. Il y est question d'augmentation des budgets et de formation de cyber experts. Dans ce chapitre, le secrétaire utilise une large gamme de termes qui ne sont jamais définis pour autant : cyber espace, cyber expert, cyber infrastructure, cyber menaces…

[158] International Institute For Strategic Studies (Shangri-La--Asia Security), Remarks as Delivered by Secretary of Defense Robert M. Gates, Shangri-La Hotel, Singapore, Saturday, June 05, 2010
[159] DIA 50th Anniversary Ceremony, As Delivered by Secretary of Defense Leon E. Panetta, Bolling AFB, Washington, DC, Thursday, September 29, 2011
[160] Halifax International Security Forum, As Delivered by Secretary of Defense Leon E. Panetta, Halifax, Nova Scotia, Friday, November 18, 2011
[161] "Defending the Nation from Cyber Attack" (Business Executives for National Security) As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012
[162] "Defending the Nation from Cyber Attack" (Business Executives for National Security) As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012
[163] Prepared Testimony for the Senate Foreign Relations Committee regarding the Moscow Treaty, Prepared Testimony of Secretary of Defense Donald H. Rumsfeld, Dirksen Senate Office Building, Washington, D.C, Wednesday, July 17, 2002
[164] Submitted Statement on the FY 2010 Budget to the House Armed Services Committee, As Submitted by Secretary of Defense Robert M. Gates, Room 2118, Rayburn House Office Building, Washington, D.C., Wednesday, May 13, 2009

Léon Panetta (discours étudiés: 2011-2013):

- L'OTAN doit renforcer ses capacités de cyberdéfense[165].
- Une politique active de renforcement des capacités de cyberdéfense est menée par le gouvernement. L'expérience du DoD est également partagée avec le secteur privé pour la défense des infrastructures critiques[166].
- Lorsqu'on pense à la cybersécurité on pense généralement aux hackers, à la cybercriminalité. Mais il y a une menace bien plus forte, celle des attaques perpétrées par des Etats nations et des groupes terroristes[167].
- Le Département de la défense investit chaque année plus de 3 milliards de $[168].
- En matière de cybersécurité/cyberdéfense, les agences de l'Etat sont toutes investies: le DHS pour la sécurité intérieure, le FBI pour la prévention des attaques, les agences de renseignement, le Département d'Etat qui tente de forger un consensus international sur les rôles et responsabilités des nations dans la sécurisation du cyberespace, et le DoD qui a un rôle de soutien, essentiel[169].

2.10. Cyber Pearl Harbor

William James Perry (discours étudiés: 1995-1997):

- *Pas de référence*

William Sebastian Cohen (discours étudiés: 1997- 2001):

- *Pas de référence*

Donald Rumsfeld (discours étudiés: 2001-2006):

- *Pas de référence*

Robert M. Gates (discours étudiés: 2006-2011):

- *Pas de référence*

Léon Panetta (discours étudiés: 2011-2013):

- L. Panetta utilise l'expression "*Digital Pearl Harbor*", que nous n'avions pas relevée dans l'ensemble des discours depuis 1995[170]. Dans son propos il évoque notamment un passé où l'armée ne comptait qu'une dizaine d'ordinateurs et l'on ne craignait ni ne parlait de cyberattaques[171].
- Risque réel de cyber Pearl Harbor, qui serait le résultat d'une attaque provoquant des dégâts matériels et la perte de vies humaines. Cette attaque paralyserait et choquerait la nation, et créerait un nouveau et profond sentiment de vulnérabilité[172].

---

[165] King's College London, As Delivered by Secretary of Defense Leon E. Panetta, London, UK, Friday, January 18, 2013

[166] "Defending the Nation from Cyber Attack" (Business Executives for National Security) As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012

[167] "Defending the Nation from Cyber Attack" (Business Executives for National Security) As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012

[168] "Defending the Nation from Cyber Attack" (Business Executives for National Security) As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012

[169] "Defending the Nation from Cyber Attack" (Business Executives for National Security) As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012

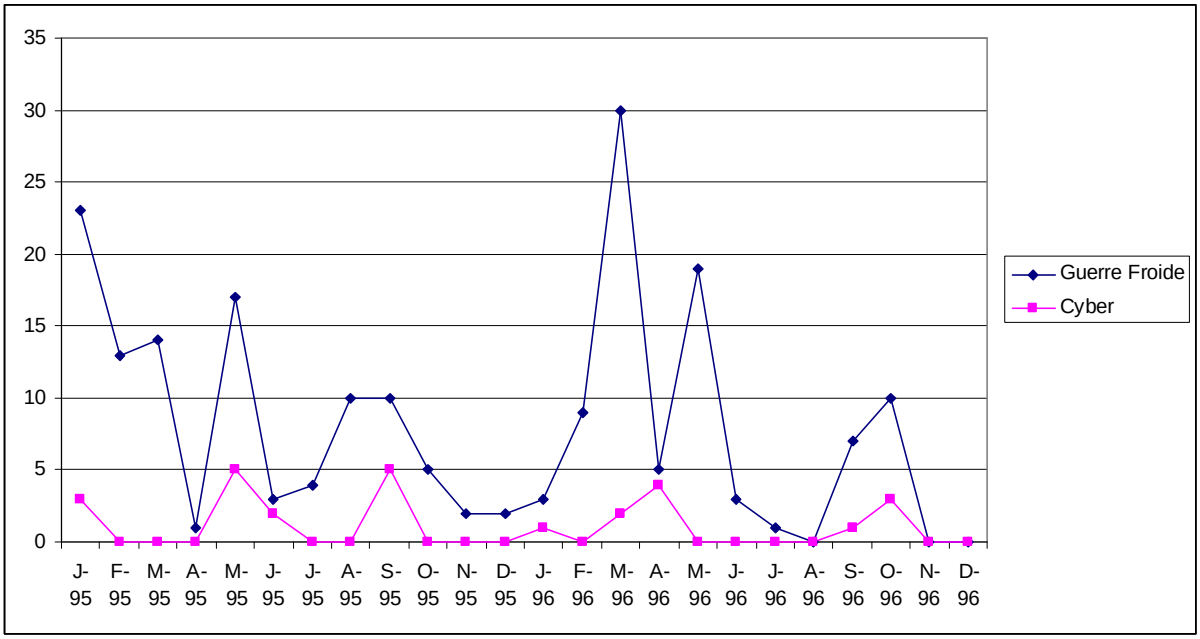
[170] Farewell Tribute to General Cartwright by Secretary Panetta, As Delivered by Secretary of Defense Leon E. Panetta, Marine Corps Barracks, Washington, DC, Wednesday, August 03, 2011

[171] Farewell Tribute to General Cartwright by Secretary Panetta, As Delivered by Secretary of Defense Leon E. Panetta, Marine Corps Barracks, Washington, DC, Wednesday, August 03, 2011

[172] "Defending the Nation from Cyber Attack" (Business Executives for National Security) As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012

2.10. Quelques statistiques

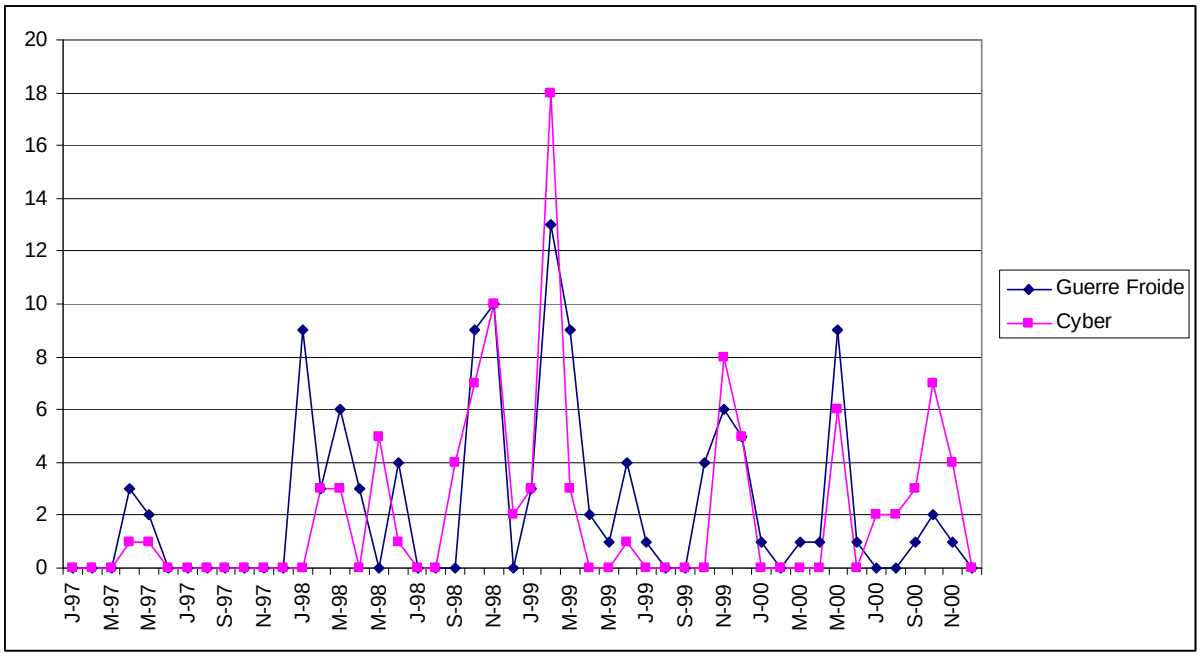
Nous comparons ci-dessous l'évolution des discours sur deux objets particuliers: le thème de la Guerre froide, dont le monde vient de sortir mais qui demeure l'un des sujets essentiels du discours (il contribue à construire l'identité américaine, sortie victorieuse de cette "guerre"); et l'objet "cyber", symbolique d'une nouvelle ère, qui succède à la Guerre Froide.



Discours de W.J. Perry (statistique: nombre de termes liés au sujet apparaissant dans chaque discours)

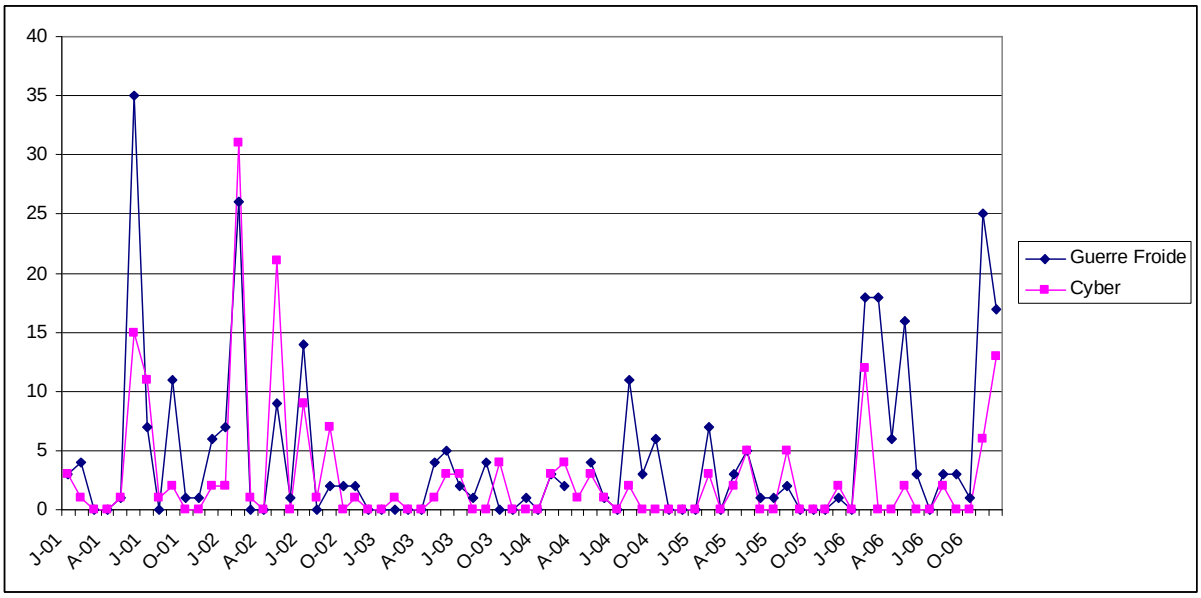
Dans le discours de W.J. Perry les éléments du "cyber" (ordinateurs, informatique...) sont encore marginaux, par rapport à d'autres thèmes, comme par exemple celui de la Guerre froide. Les notions de "cyberterrorisme" ou "cyberguerre" sont absentes.

Par rapport au thème de la Guerre Froide, omniprésent dans les discours, la place du cyber devient plus significative chez W. Cohen comme le montre le graphique ci-dessous:



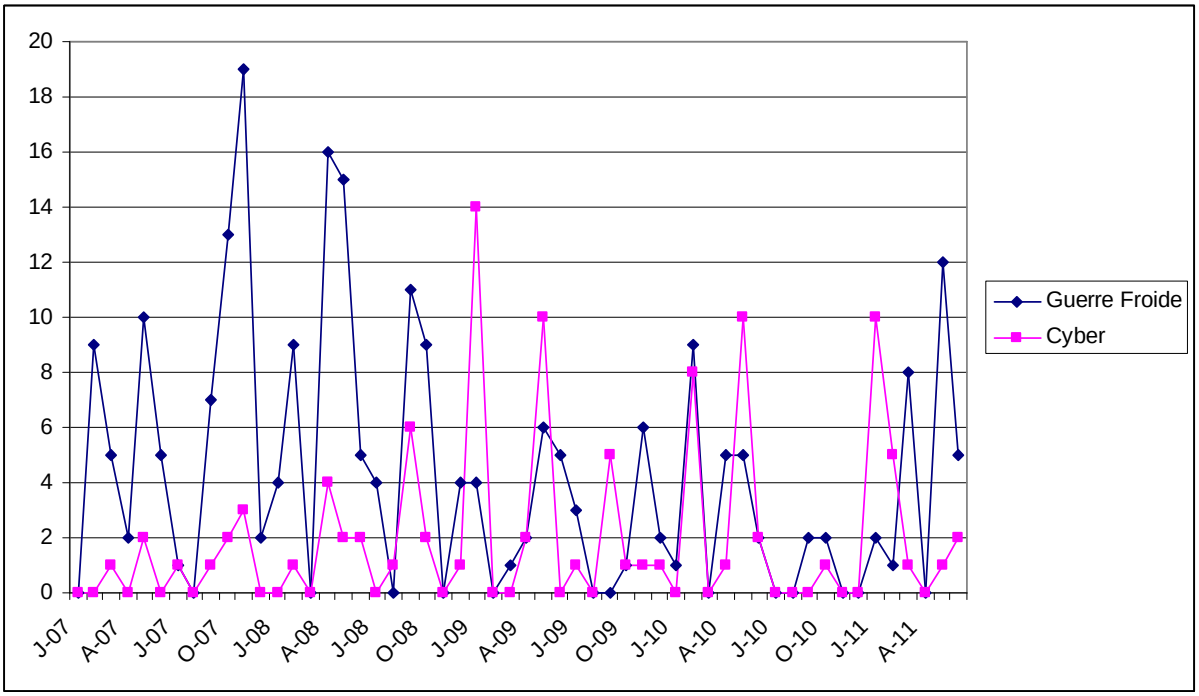
Discours de W. Cohen (statistique: nombre de termes liés au sujet apparaissant dans chaque discours)

Dans le discours de D. Rumsfeld, le thème de la guerre froide est toujours omniprésent, et celui du "cyber" ne s'impose pas.



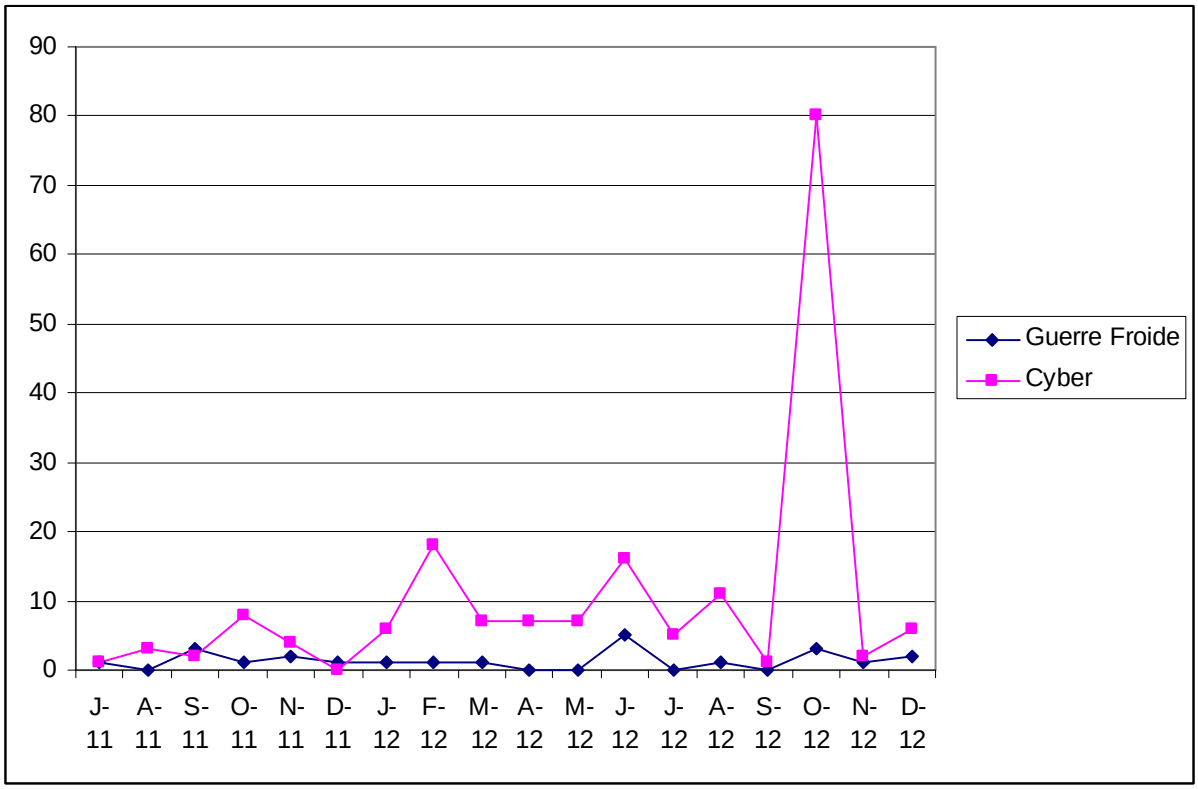
Discours de D. Rumsfeld (statistique: nombre de termes liés au sujet apparaissant dans chaque discours)

L'approche de R. Gates conserve au thème de la guerre froide une place importante mais l'objet "cyber" tend à s'affirme davantage dans le discours, et ce de manière évidente dans la première moitié de son exercice.



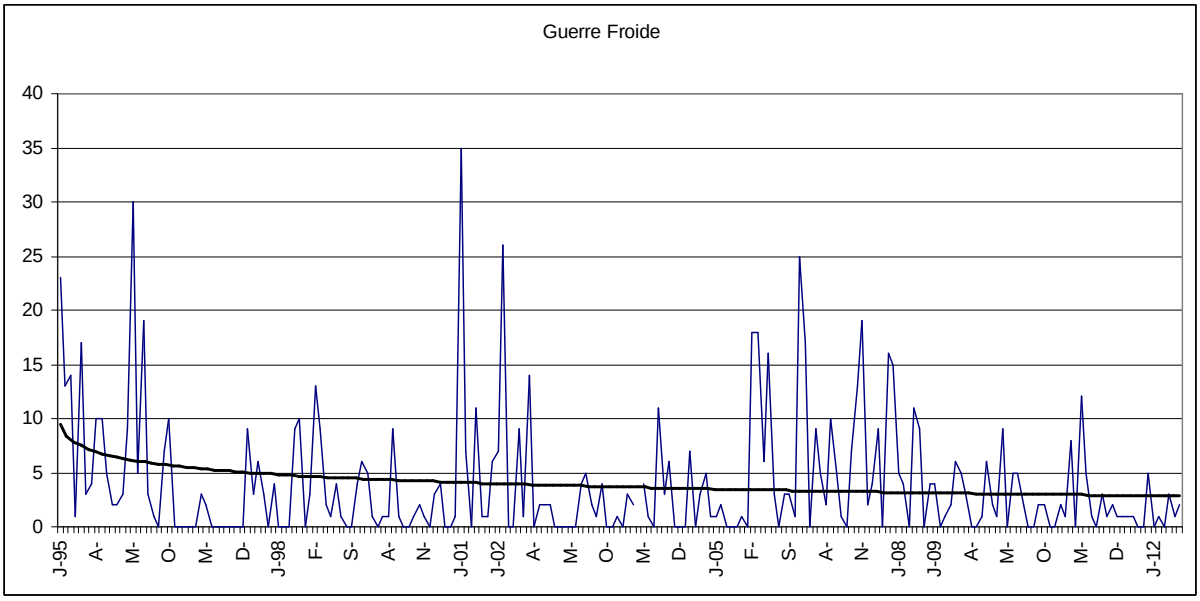
Discours de R. Gates (statistique: nombre de termes liés au sujet apparaissant dans chaque discours)

Le glissement est évident au cours de l'exercice de L. Panetta. Les références à la Guerre froide se font plus rares et s'affirme le thème du "cyber":



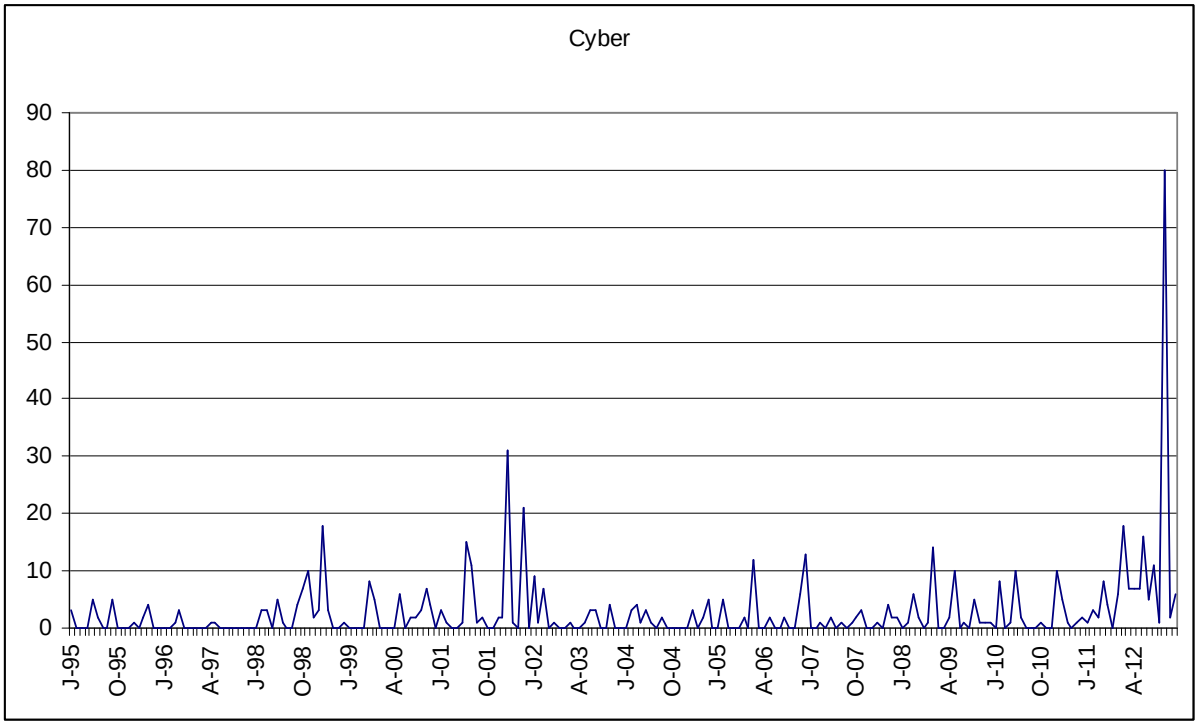
Discours de L. Panetta (statistique: nombre de termes liés au sujet apparaissant dans chaque discours)

La place du thème de la Guerre froide a certes régressé dans le discours, mais demeure.



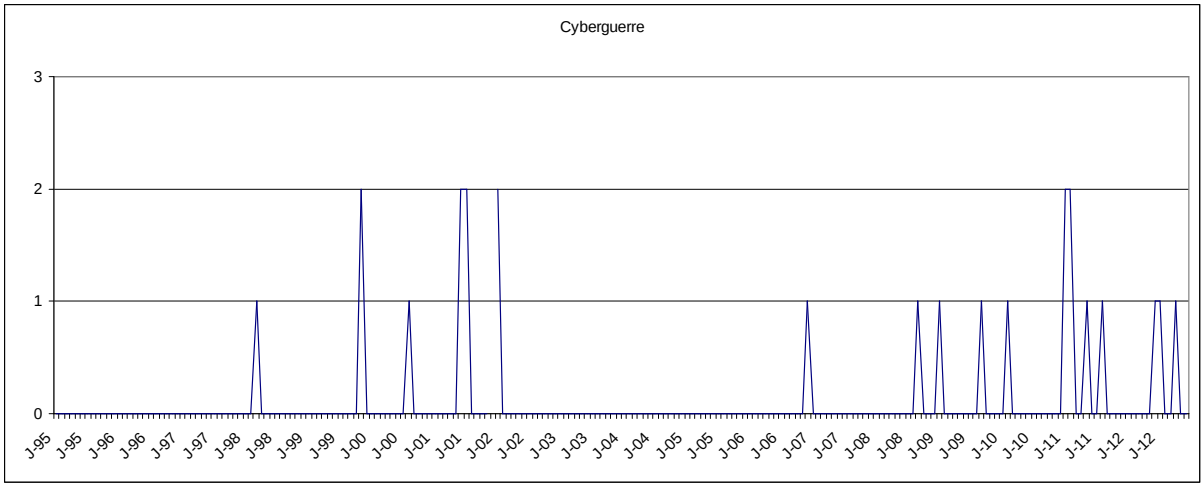
Evolution du thème "Guerre froide" dans les discours. Période 1°janvier 1995- 31 décembre 2012. En gras: courbe de tendance.

Quant à la thématique "cyber" (figure ci-dessous) elle s'insère relativement lentement dans le discours, connaissant deux phases plus intenses, la première centrée sur février 2002 (secrétaire Républicain, en début de mandat de G.W. Bush), la seconde sur octobre 2012 (secrétaire Démocrate, en fin de mandat de B. Obama). L'entrée en fonction de B. Obama, moment de transition politique (de Républicain à Démocrate) ne s'est pas traduite par une transition brutale dans la prise en compte du cyber dans les discours de la Défense, du moins ceux que nous avons analysés ici. D'autre part nous constatons que les attentats du 11 septembre 2001 n'ont pas provoqué de modification radicale de la place du "cyber dans le discours; d'autre part que ni les cyberattaques contre l'Estonie, ni le conflit russo-géorgien, ne font office de moteur à une réelle impulsion de la place du cyber dans le discours.



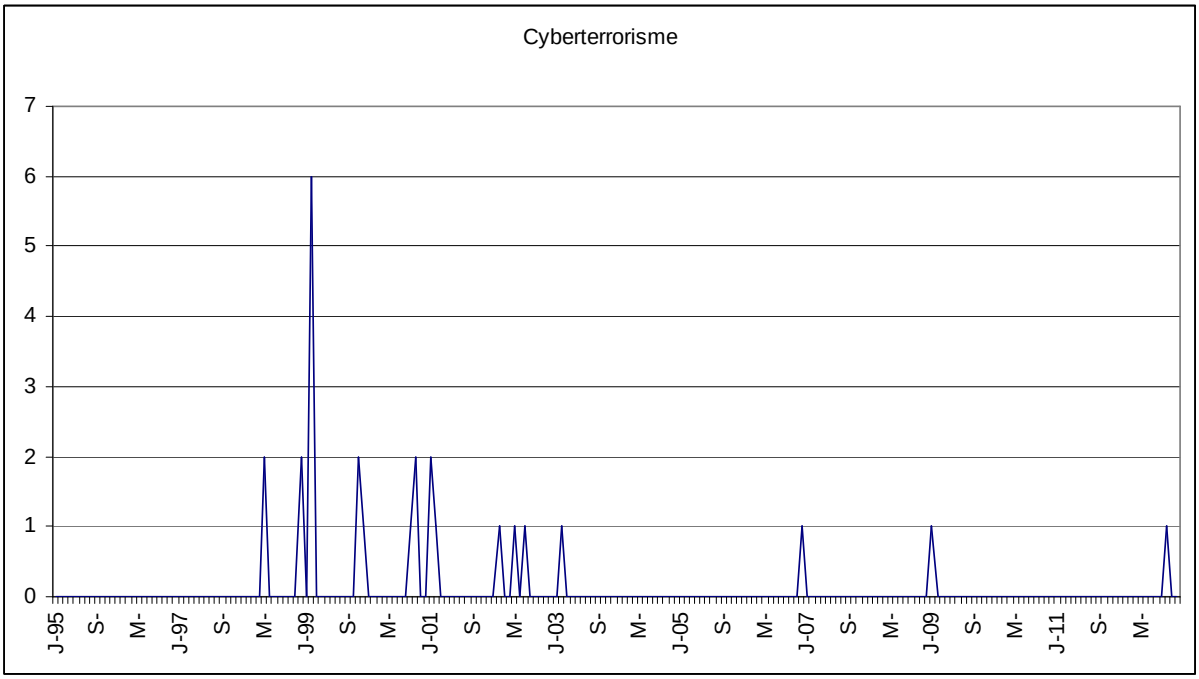
Evolution de l'objet "cyber" dans les discours. Période 1°janvier 1995- 31 décembre 2012

Il est peu question de "cyberguerre" dans les propos des secrétaires à la Défense. La fréquence des termes n'est pas véritablement significative pour en tirer de conclusions définitives, mais on constate que l'objet "cyberguerre" est utilisé dans des périodes de présidence démocrate (B. Clinton jusqu'en 2001; B. Obama, à compter de 2009), mais avec un secrétaire Républicain pour la première partie (1997-2001), puis n Républicain (2009-2011) et enfin un démocrate (2011-2012). La seule constante serait inscrite dans la période 2002-2009, Républicaine, où l'on enregistre l'absence d'utilisation du concept.



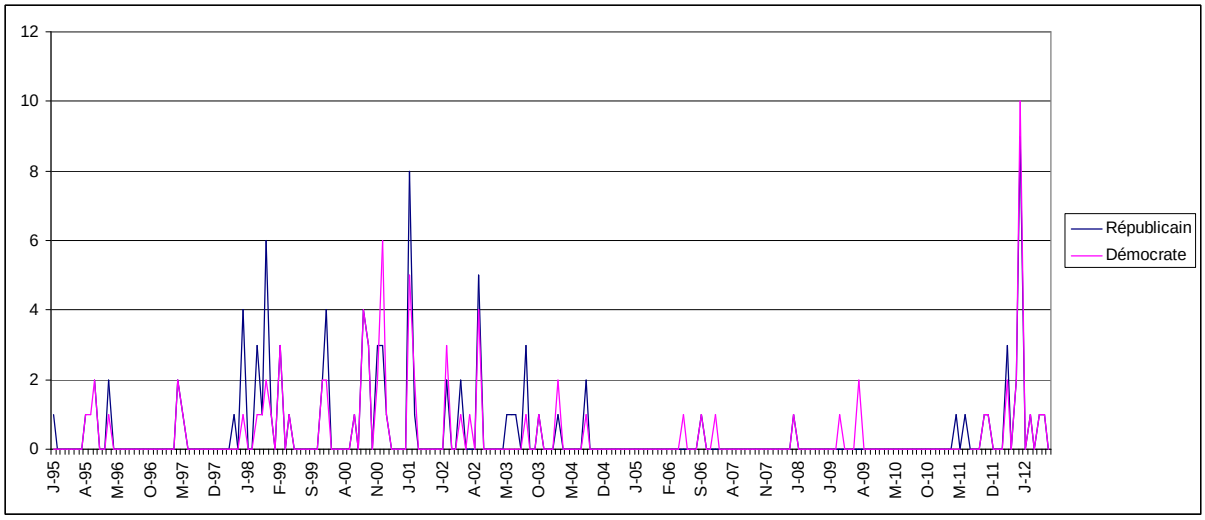
Evolution du thème "cyber guerre" dans les discours. Période 1°janvier 1995- 31 décembre 2012.

Quant à la notion de "cyberterrorisme", elle s'inscrit essentiellement dans la période démocrate de B. Clinton et le discours du secrétaire Républicain W.S. Cohen.



Evolution du thème "cyber terrorisme" dans les discours. Période 1°janvier 1995- 31 décembre 2012.

Quant aux références aux partis politiques, elles se manifestent approximativement sur une période 1998-2003 (secrétaires républicains), et à partir de 2011 (secrétaire et président démocrates mais Congrès à majorité républicaine). Les deux phases 1998-2001, 2011-2012, sont placées sous présidence démocrate avec un Congrès républicain.



III - Conclusion

Dans le tableau ci-dessous nous faisons la synthèse des principales caractéristiques qui ressortent de cette lecture.

	W.J. Perry (D) 1994-1997	**W. Cohen (R) 1997-2001**	**D. Rumsfeld (R) 2001-2006**	**R. Gates (R) 2006-2011**	**L. Panetta (D) 2011-2013**
Démocrates/Républicains	- convergences Républicains/Démocrates sur questions de relations internationales par exemple - divergence sur les moyens financiers à allouer au DoD	- il ne doit pas y avoir d'approche partisane dès lors qu'il est question de sécurité nationale, d'enjeux engageant la sécurité de la nation - Cohen est un républicain au sein d'un gouvernement démocrate, preuve du nécessaire abandon des considérations partisanes dans les affaires de sécurité.	- les sujets de sécurité sont plus importants que les considérations partisanes. - la défense appelle un consensus politique	- il est des questions, par exemple des sujets de relations internationales, qui font consensus, s'imposent aux dirigeants, quelle que soit leur couleur politique.	- la distinction Démocrates/Républicains s'efface devant les enjeux de sécurité nationale - Républicains et Démocrates assument la co-responsabilité de la baisse des budgets de la Défense dont les effets peuvent être désastreux.
Rôle de la technologie	- avantage stratégique conféré par la technologie; - rôle majeur de la technologie dans la supériorité militaire; succès, victoire et technologie sont étroitement liés - l'industrie tient une place centrale - Mise à niveau technologique permanente nécessaire - adapter les règles d'acquisition - adapter les budgets de la défense	- il faut développer, acquérir des moyens - il faut des règles et procédures d'acquisition plus souples, dynamiques - il faut maintenir les budgets d'acquisition - l'armée utilisera et dépendra de plus en plus d'Internet - les technologies qui font la force de l'armée et du pays peuvent se retourner contre nous	- il faut assurer la domination dans le cyberespace, dans l'espace informationnel - les ordinateurs ont permis la résurgence de la suprématie économique américaine - mais la dépendance des Etats aux réseaux les rend vulnérables - l'environnement sécuritaire moderne est extrêmement complexe, et les nouvelles	Tout le spectre des capacités militaires sur terre, air, mer dépend des communications numériques et des réseaux de données	- Il faut renforcer le développement des capacités cyber - les capacités cyber permettront d'affronter les adversaires sur tous les terrains

			technologies TIC y contribuent.		
Cyberattaques	-	- le monde a changé. le quotidien est désormais fait de cyberattaques émanant d'acteurs étatiques et non étatiques.	- La période actuelle est période de transition: d'un monde où l'on comprenait les menaces à un monde où les menaces sont de nature nouvelle et ne sont pas encore comprises - les cyberattaques contre les systèmes critiques peuvent avoir des effets comparables à ceux d'un conflit armé - les cyberattaques sont la plus grande menace	- les cyberattaques sont des opérations de guerre - pose la question: quel niveau de cyberattaque pourrait constituer un acte de guerre?	- les cyberattaques font parti des nouvelles menaces - scénarios de cyberattaques toujours plus pessimistes, et réalité toujours plus inquiétante - les capacités terroristes augmentent, l'Etat doit accroître les siennes - risque réel de Cyber Pearl Harbor
Cybersécurité / cyberdéfense	-	-	La cyberdéfense complète la gamme des outils de la défense américaine	Il faut accroître les budgets, recruter et former des cyber experts	Budgets importants accordés à la cyberdéfense; Le rôle du DoD n'est qu'un maillon de la politique de cybersécurité américaine Il y a des menaces plus grandes encore que la cybercriminalité: les

					actions menées par les Etats et les groupes terroristes
Cyberguerre	-	- la cyberguerre est l'une des caractéristiques du nouvel environnement mondial de la menace - des Etats développent des capacités de cyberguerre	- la cyberguerre ouvre de nouvelles vulnérabilités et perspectives pour les acteurs asymétriques - l'armée américaine ne serait pas véritablement préparée à affronter les acteurs asymétriques tirant notamment avantage du cyberespace	- les capacités de cyberguerre chinoises constituent une menace pour l'armée américaine	- la cyberguerre fait partie des nouveaux challenges de la sécurité
Guerre de l'information / opérations d'information	-	- la guerre de l'information, comme le terrorisme, est un moyen de lutte asymétrique utilisé par les acteurs des nouvelles menaces dans le monde - la guerre de l'information fait partie des diverses formes nouvelles de menace	- la guerre de l'information est une menace au même titre que la menace bactériologique, nucléaire, chimique, etc. - il est impératif d'assurer la sécurité des réseaux de la défense	- la place des opérations d'information s'est inversée. Désormais il s'agit de mener des campagnes stratégiques de communication accompagnées d'opérations militaires	-
Cyber Pearl Harbor / Digital Pearl Harbor	-	-	-	-	Un risque présent, réel. Attaque provoquant des dégâts matériels et la perte de vies humaines. Cette attaque paralyserait

					et chiquerait la nation, et créerait un nouveau et profond sentiment de vulnérabilité
Cyberespace	-	Outil de communication	- le cyberespace est un territoire - le cyberespace est l'un des espaces de lutte contre le terrorisme - chaque acteur dispose, crée son cyberespace: il y a celui des terroristes, il y a le nôtre, etc.	- l'US Air Force doit défendre le cyberespace - le cyberespace est un Global Commons, et un territoire - de nombreuses menaces, nouvelles, pèsent sur ces *global commons* - cybersécurité et cyberdéfense sont des enjeux qui doivent impliquer les acteurs de la scène internationale (il y a donc dans la politique de cybersécurité toute un nécessaire volet relations internationales, diplomatie, dépendant du Département d'Etat).	- Le cyberespace est placé sous surveillance - nécessité pour les Etats d'assurer leur responsabilité dans la sécurisation du cyberespace - la défense du cyberespace est une mission qui implique tous les acteurs de l'Etat, pas seulement le DoD - la défense du cyberespace est un objet des relations internationales: consensus international, responsabilités - le cyberespace est la nouvelle frontière (raison pour laquelle il faut impérativement le défendre) - le cyberespace est un domaine
Cyberterrorisme	-	- le cyberterrorisme frappe les points faibles - le cyberterrorisme: cyberattaques contre les infrastructures critiques - menace totalement nouvelle, manifestation de la nouvelle anarchie qui caractérise la scène internationale	- Les Etats seront soumis à des attaques cyberterroristes, menées par des cyber-soldats, agissant dans le cade d'opérations étatiques ou non-étatiques	- les terroristes pourront utiliser les armes nouvelles - les forces armées ne sont as préparées à faire face aux menaces d'un monde nouveau.	- attaque cyberterroriste est attaque perpétrée par des Etats ou des groupes terroristes, pouvant paralyser un pays.

			- la menace cyber n'est qu'une menace de plus dans l'environnement mondial de la menace - au regard de ce nouvel environnement il faut redéfinir la guerre pour mieux préserver la paix		

3.1. Convergences, consensus

A propos des considérations politiques :

- Les Secrétaires revendiquent tous, en matière de politique de défense nationale, une approche libérée de toute considération partisane et appellent les membres du Congrès, quelles que soient leurs convictions politiques, leur appartenance politique, à adopter une approche bipartisane constructive. Un consensus doit se faire lorsqu'il est question de défense nationale, il ne peut exister qu'un seul objectif.

A propos du "Cyber":

- Le discours sur la cybersécurité construit l'image d'un cyberespace devenu nouvelle source de vulnérabilité, de menace, lieu où prolifèrent des acteurs menaçants[173].
- La question "cyber" est exprimée en termes guerriers: cyberattaques et cybersécurité/cyberdéfense, mais surtout cyberguerre, guerre de l'information, et cyberterrorisme (ce qui permet d'établir un lien entre la menace émergeante qui se formalise par des cyberattaques, et le contexte de guerre contre le terrorisme des années 2000, dans lequel se développe l'objet cyberdéfense).
- Le langage guerrier suppose la mobilisation de ressources pour affronter des ennemis, il évoque un danger majeur pour la nation, voire la civilisation, la mise en péril de l'intégrité d'un groupe (nation), d'une identité.
- Deux formes de discours construisent, tant chez les secrétaires républicains que démocrates, les contours des politiques de cybersécurité/cyberdéfense :
    - un discours moderniste : le cyber est présenté comme un facteur central de la supériorité technologique qui garantit la victoire militaire et la supériorité militaire américaine sur tous les champs d'affrontement ; la défense nationale et le maintien de l'hégémonie militaire américaine imposent un développement capacitaire ne pouvant souffrir d'aucun ralentissement ; ce rythme impose la garantie de budgets suffisants, importants, maintenus, voire en augmentation) ;
    - un discours alarmiste (la menace est là !), voire catastrophiste : le cyberespace est porteur de nouvelles menaces, les cyberattaques viennent ajouter à la complexité de l'environnement international, constitué d'une multitude de menaces susceptibles de porter un choc violent à la civilisation (armes nucléaires, chimiques, bactériologiques…). Sans nécessairement recourir à l'expression « Cyber Pearl Harbor » l'ensemble des discours construit l'image d'un environnement chaotique, apocalyptique, dans lequel seule la puissance militaire américaine peut encore garantir les conditions de la sécurité et de la paix. La notion de cyberterrorisme concentre l'essentiel de ces menaces cybernétiques, asymétriques. En privilégiant une association à la notion de terrorisme, plutôt qu'à celle de guerre froide, la cyberdéfense s'inscrit dans un enjeu contemporain, mobilisateur, prenant caractère d'urgence. Elle devient objet consensuel.
- On peut également souligner que les discours ne recourent pas à certaines notions telles que le cyber espionnage, cyber guerre froide, cyber criminalité ; celle de Cyber Pearl Harbor est elle-même marginalisée. Le discours sur la cyberdéfense est ainsi élaboré à l'aide d'un nombre relativement réduit de concepts « cyber ». Les discours tendent à bien distinguer ce qui relèverait de la lutte contre la cybercriminalité, de la cybersécurité, des missions de la Défense, à savoir les affaires militaires, la cyberdéfense. Pour cela ils se concentrent sur quelques notions qui déplacent la menace cybernétique et les solutions de sécurisation vers le champ

[173] David Barnard-Wills, *Securing Virtual Space: cyber war, cyber terror, and risk*, Space and Culture, 15 mai 2012, pp.110-123

des affaires militaires : lutte contre le cyberterrorisme, cyberguerre, guerre de l'information, opérations d'information, contribution à la protection des infrastructures critiques.

- Convergence ou consensus dans la pratique: ne pas en faire de la cybersécurité/cyberdéfense un véritable sujet de débat de campagne électorale.

3.2. Divergences

A propos des considérations politiques:

- Les différences apparaissent entre Républicains et Démocrates sur des points particuliers tels que:
    - les questions budgétaires : les Républicains en appellent à l'augmentation des budgets de la Défense, quand les Démocrates sembleraient partisans de plus de modération. Or la cybersécurité/cyberdéfense fait exception à ce phénomène. Le gouvernement Démocrate de B. Obama n'a cessé d'accroître les budgets de la cyberdéfense (ce domaine connaissant une situation particulière, les budgets de la Défense connaissant souffrant généralement de restrictions).
    - les républicains sont hostiles à plus de régulation, réglementation.

A propos du "Cyber":

- Les anciennes générations, les responsables d'entreprises, et sans doute du gouvernement ne comprennent pas parfaitement, ne maîtrisent pas les possibilités et les enjeux des nouvelles technologies. Les jeunes générations, si[174]. Le "cyber" est donc peut-être une question politique, mais elle est aussi question de générations, de culture.
- Le parti Républicain afficherait une politique de cyberdéfense plus ouvertement offensive, critiquant le focus défensif de l'approche des Démocrates au pouvoir (mais les faits contredisent partiellement cette critique de faiblesse, de passivité).
- Le parti républicain, au travers de sa critique de la politique Obama, se montre soucieux du signal envoyé par les Etats-Unis sur la scène internationale. La posture en matière de cyberdéfense contribue à la puissance militaire, à la puissance de la nation sur la scène internationale, et à la sécurité nationale, à la seule condition qu'un signal fort soit envoyé au monde.
- Divergence sur les modalités de la coopération public-privé, qui en elle-même semble faire consensus: les Républicains veulent une coopération fondée sur le volontariat, les Démocrates voudraient encadrer, réguler.
- Les Républicains seraient moins soucieux de la défense des droits à la vie privée des citoyens.

3.3. Perspectives

Cette étude pourrait être prolongée et complétée par une analyse des débats menés au sein du Congrès américain: la cyberdéfense est-elle un nouvel objet d'opposition entre les partis? Sous quelle forme l'opposition se manifeste-elle? Pourquoi? Quand? Les convergences et divergences se manifestent-elles entre Républicains et Démocrates? Ou bien entre Sénateurs et membres de la Chambre des Représentants? L'objectif serait, dans la continuité de cette première étude, la recherche des facteurs déterminant les orientations des politiques de cyberdéfense.

[174] Ohio Wesleyan University Grad, As Delivered by Secretary of Defense William S. Cohen, Ohio Wesleyan University, Ohio, Sunday, May 10, 1998

Annexe 1: Les secrétaires à la Défense

Nom du secrétaire à la défense	Date de naissance	Parti politique	Dates en fonction	Président
William James Perry	11/10/1927	D	3 février 1994 – 24 janvier 1997	Bill Clinton (Démocrate) (janvier 1993-décembre 1996)
William Sebastian Cohen	28/08/1940	R	24 janvier 1997 – 20 janvier 2001	Bill Clinton (Démocrate) (janvier 1997 – décembre 2000)
Donald Rumsfeld	08/07/1932	R	20 janvier 2001 – 18 décembre 2006	G. W. Bush (Républicain) (janvier 2001 – décembre 2004 ; janvier 2005-décembre 2008)
Robert M. Gates	25/09/1943	R	18 décembre 2006 – 1 juillet 2011	G. W. Bush (Républicain) (→ décembre 2008)); B. Obama (janvier 2009 – décembre 2012. Démocrate)
Leon Panetta	28/06/1938	D	1 Juillet 2011 – 27 février 2013	B. Obama (Janvier 2013 – décembre 2016. Démocrate)
Chuck Hagel	1946	R	27 février 2013 - …	B. Obama

Congrès[175]	Période	Sénat	Chambre des représentants	Président des Etats-Unis	Parti du Président	Secretary of State	Secretary of DHS
103ème	1993-1995	D	D	B. Clinton	D	D[176]	
104ème	1995-1997	R	R	B. Clinton	D	D[177]	
105ème	1997-1999	R	R	B. Clinton	D	D[178]	
106ème	1999-2001	R	R	B. Clinton	D	D[179]	
107ème	2001-2003	=	R	G.W. Bush	R	R[180]	
108ème	2003-2005	R	R	G.W. Bush	R	R[181]	R[182]
109ème	2005-2007	R	R	G.W. Bush	R	R[183]	R[184]
110ème	2007-2009	=	D	G.W. Bush	R	R[185]	R[186]
111ème	2009-2011	D	D	B. Obama	D	D[187]	D[188]
112ème	2011-2013	D	R	B. Obama	D	D[189]	D[190]
113ème	2013-2015	D	R	B. Obama	D	D[191]	D[192]

Majorité : démocrate (D), républicaine (R), à égalité (=)

[175] Chiffres du Congrès extraits de http://www.infoplease.com/ipa/A0774721.html
[176] W. Christopher
[177] W. Christopher
[178] M. Albright
[179] M. Albright
[180] C. Powell
[181] C. Powell
[182] T. Ridge
[183] C. Rice
[184] M. Chertoff
[185] C. Rice
[186] M. Chertoff
[187] H. Clinton
[188] J. Napolitano
[189] H. Clinton
[190] J. Napolitano
[191] J. Kerry
[192] J. Napolitano

Sommaire du rapport