Quels outils et méthodes utilisés aux Etats-Unis et au Canada pour procéder à l'analyse stratégique du renseignement de sécurité intérieure ? Comparaison des agences de renseignement de ces deux pays (organisation, missions, moyens, efficience)

Guillaume DASQUIÉ – Directeur de recherche à l'IRIS

Étude réalisée pour le compte de la DAS au titre du marché public passé selon une procédure adaptée n°2004/106

Avertissement.

Cette étude s'appuie sur de nombreux documents produits par des agences fédérales des Etats-Unis. Nous avons choisi de montrer certains d'entre eux chaque fois que leur contenu semblait éloquent.

La plupart de ces documents nourrissant ainsi notre propos ont fait l'objet de procédures de déclassification, ou, lorsqu'ils n'étaient pas dûment classifiés, ont connu, sur l'instigation d'élus ou de responsables administratifs, une relative diffusion dans des cercles académiques nord-américains. En revanche, quelques pages évoquées ou présentées ci-après nous sont parvenues sans qu'aucune autorité américaine ou représentant de ce pays n'en soit informée ou n'y consente même tacitement. En conséquence, la lecture ou la diffusion de ce rapport sur le territoire des Etats-Unis pourrait exposer ses détenteurs à des actions en justice.

I – Le renseignement de sécurité intérieure remanié avant d'être repensé.

Dans les mois qui suivirent le 11 septembre 2001, parallèlement à la promotion d'une nouvelle politique de sécurité privilégiant désormais la protection du sanctuaire national, des critiques nourries ont mis en cause l'efficacité des services de renseignement dans la prévention des attaques terroristes. À mesure que les médias révélaient comment les auteurs de ces actes s'étaient préparés sur le sol des Etats-Unis, en particulier en prenant simplement des leçons dans des écoles de pilotages de Floride, le Congrès et la Maison Blanche dressèrent le même constat négatif quant aux capacités des institutions à produire un renseignement de sécurité intérieure fiable[1].

Les reproches culminèrent en décembre 2002 lors de la publication du rapport d'enquête parlementaire *Joint inquiry into intelligence community activities before and after the terrorist attacks of september 11, 2001* : en insistant sur les faiblesses du FBI (accusé de ne pas avoir pris en compte des notes rédigées par des fonctionnaires de terrain au sujet des cours de pilotage suivis par des militants islamistes), sur la culture de la CIA (accusée de ne pas avoir transmis des renseignements sur les entrées sur le territoire américain de futurs terroristes) et enfin sur le manque d'adaptabilité de la NSA (accusée d'avoir traduit et analysé le 12 septembre seulement une conversation téléphonique interceptée au Pakistan et portant sur la préparation des attentats). Ainsi, après le temps des récriminations, vint une période de propositions tous azimuts, de 18 mois environ. Dans un contexte alors confus, et tandis que les parlementaires réclamaient d'agréger la production et la diffusion du renseignement de nature contre-terroriste à l'intérieur d'un futur *Department of Homeland Security*, chaque service de renseignement, parfois au nom de sa propre survie, développa concurremment des dispositifs spécifiques.

[1] Nonobstant une sincérité discutable. Les débats provoqués par la divulgation du *briefing* présidentiel de la CIA d'août 2001 au sujet de la préparation d'attentats islamistes sur le sol américain ont surtout démontré que les services de renseignement n'avaient pas reçu du pouvoir exécutif l'ordre de travailler sur les phénomènes de cette nature.

C'est ainsi que le renseignement de sécurité amorça une autre mutation aux Etats-Unis : En devenant dans l'urgence un renseignement d'intérêt contre-terroriste et en se hissant au rang de préoccupation focale pour la plupart des institutions en charge du renseignement, dont les responsables comprirent qu'il s'agissait de premiers aménagements de circonstance précédant des réformes autrement ambitieuses. Pour ces raisons, dans une atmosphère parfois chaotique, le renseignement d'intérêt contre-terroriste prit la forme d'un champ d'expérimentation des nouvelles attributions et des nouveaux moyens que le pouvoir exécutif et parlementaire accorderaient aux services – au moins jusqu'au dernier trimestre 2004 – avant de s'affirmer comme la colonne vertébrale d'un renseignement de sécurité repensé, dans un cadre doctrinaire renouvelé.

1 - Les difficultés propres au renseignement de sécurité en matière de terrorisme. Valeur emblématique et enseignement technique du traitement de ce renseignement dans l'après 11 septembre.

a - La multiplication des centres de compétences en Amérique du Nord. Compétitivité bureaucratique, priorités politiques et contingences administratives.

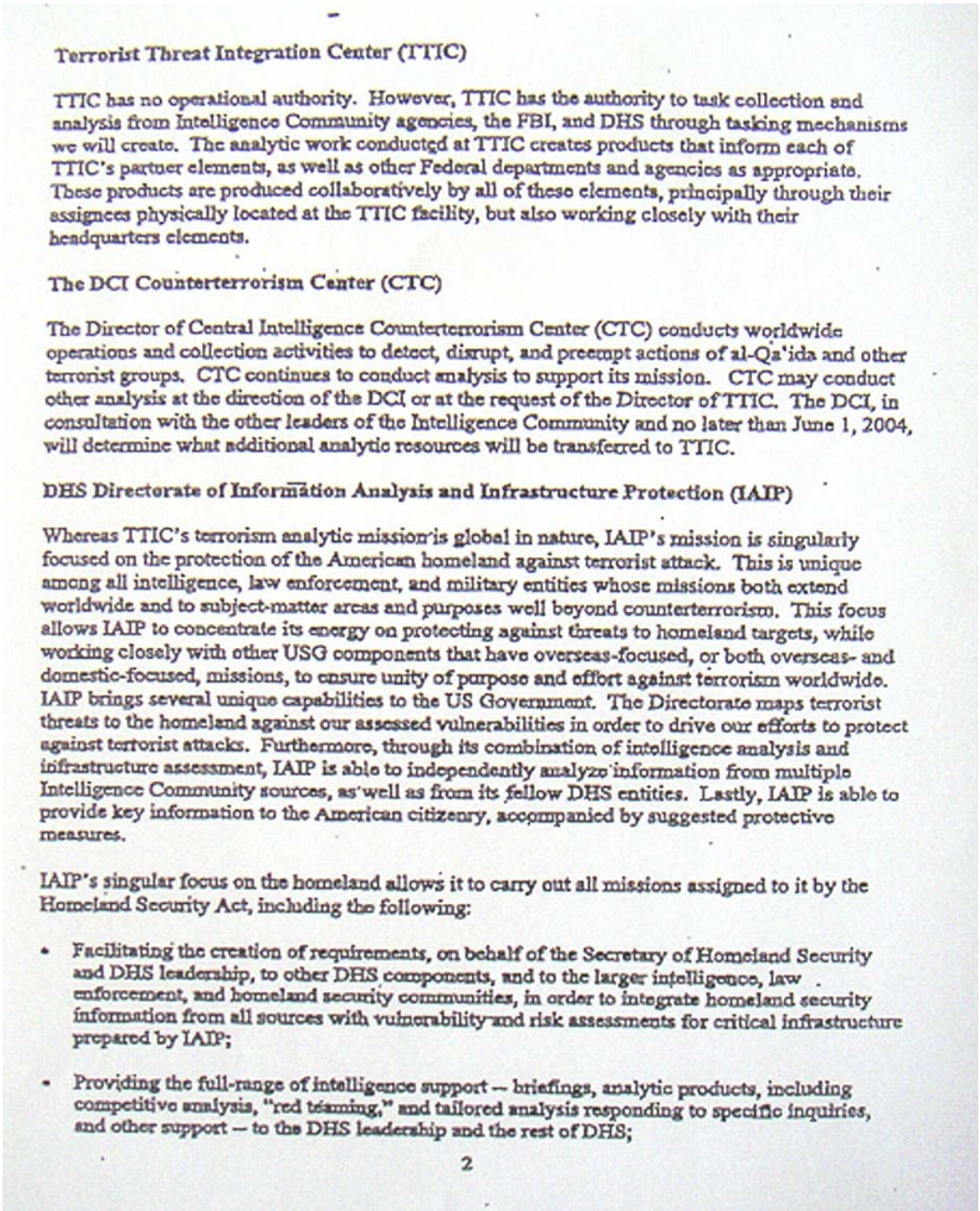
Près de deux ans après la publication par la Maison Blanche de sa *National Security Strategy*, à la fin de l'été 2004, nous comptions aux Etats-Unis plusieurs structures distinctes chargées d'atteindre les objectifs nationaux en matière de contre-terrorisme, tels qu'ils étaient assignés par ce document cadre – et le plus souvent dans une atmosphère de fortes rivalités. Ainsi, dans un premier temps, les nouvelles priorités étendirent largement les activités du renseignement de sécurité tout en les concentrant sur un sujet unique, le contre-terrorisme. Quatre entités se distinguaient principalement : La Division contre-terroriste du FBI (CTD) et ses diverses branches, le Centre de contre-terrorisme de la CIA (CTC), la Direction de l'analyse de l'information et de la protection des infrastructures (IAIP) du nouveau département de la Sécurité Intérieure, et enfin le Centre d'information sur les menaces terroristes (TTIC), une entité transversale théoriquement destinée à obliger les services de renseignement à coopérer au nom de la protection du sanctuaire national.

Ainsi, loin des premières déclarations officielles appelant à fédérer le renseignement de sécurité intérieure au sein du département du même nom, au contraire, les évènements nous portaient à observer que chaque administration du renseignement s'employait à agrandir son champ d'intervention en matière de contre-terrorisme, dans l'espoir de réduire celui du département de la Sécurité Intérieure en gestation. Devant le Congrès, les différents cadres du FBI affirmèrent de manière persistante qu'ils ne renonceraient pas à leurs pré-

rogatives en matière de renseignement. Parallèlement, le directeur de la CIA durant cette période, George Tenet, multiplia les interventions d'ordre politique afin que son service coordonne dans les faits le nouveau Centre d'information sur les menaces terroristes (TTIC, opérationnel depuis le 1er mai 2003), supposé irriguer l'ensemble des agences fédérales en charge de la sécurité intérieure ; d'abord en l'hébergeant dans un immeuble appartenant à la CIA, puis en le plaçant sous la direction de l'un de ses ex adjoints, John Brennan.

À partir de la fin 2003, les membres du Comité sur les affaires de renseignement du Sénat exprimèrent à plusieurs reprises leurs craintes que cette multiplicité d'intervenants nuise à la qualité de la production. Et c'est après des demandes répétées d'informations que les responsables tutélaires des quatre entités concernées adressèrent, en date du 13 avril 2004, une lettre à leurs interlocuteurs du Sénat (*voir page suivante*) tentant de les rassurer sur la complémentarité et l'efficacité de cet ensemble de dispositifs. À cette occasion, faisant taire pour un temps leur dissension, Tom Ridge (département de la Sécurité Intérieure), Robert Mueller (FBI), George intérieure.
et John Brennan consentirent à délimiter officiellement, vaille que vaille, leur territoire : Le TTIC fédère l'analyse du renseignement d'intérêt contre-terroriste et alerte les agences nationales, mais est dépourvu d'autorité opérationnelle ; le CTC de la CIA conduit des missions à travers le monde pour produire du renseignement sur les mouvements terroristes (sans s'interdire de poursuivre à l'intérieur du territoire des investigations débutées à l'étranger), le CTD du FBI conduit des missions sur le sol américain pour neutraliser dans un cadre judiciaire les mouvements terroristes qui y évoluent (sans s'interdire de poursuivre à l'extérieur des frontières des investigations débutées sur le sol national) ; l'IAIP enfin adresse des alertes aux responsables locaux et fédéraux pour mettre en place les mesures de police et de sécurité civile appropriées en cas d'alerte terroriste.

Lettre du 13 avril 2004 de MM. Ridge, Mueller et Brennan au Sénat (extraits)[2].



Terrorist Threat Integration Center (TTIC)

TTIC has no operational authority. However, TTIC has the authority to task collection and analysis from Intelligence Community agencies, the FBI, and DHS through tasking mechanisms we will create. The analytic work conducted at TTIC creates products that inform each of TTIC's partner elements, as well as other Federal departments and agencies as appropriate. These products are produced collaboratively by all of these elements, principally through their assignees physically located at the TTIC facility, but also working closely with their headquarters elements.

The DCI Counterterrorism Center (CTC)

The Director of Central Intelligence Counterterrorism Center (CTC) conducts worldwide operations and collection activities to detect, disrupt, and preempt actions of al-Qa'ida and other terrorist groups. CTC continues to conduct analysis to support its mission. CTC may conduct other analysis at the direction of the DCI or at the request of the Director of TTIC. The DCI, in consultation with the other leaders of the Intelligence Community and no later than June 1, 2004, will determine what additional analytic resources will be transferred to TTIC.

DHS Directorate of Information Analysis and Infrastructure Protection (IAIP)

Whereas TTIC's terrorism analytic mission is global in nature, IAIP's mission is singularly focused on the protection of the American homeland against terrorist attack. This is unique among all intelligence, law enforcement, and military entities whose missions both extend worldwide and to subject-matter areas and purposes well beyond counterterrorism. This focus allows IAIP to concentrate its energy on protecting against threats to homeland targets, while working closely with other USG components that have overseas-focused, or both overseas- and domestic-focused, missions, to ensure unity of purpose and effort against terrorism worldwide. IAIP brings several unique capabilities to the US Government. The Directorate maps terrorist threats to the homeland against our assessed vulnerabilities in order to drive our efforts to protect against terrorist attacks. Furthermore, through its combination of intelligence analysis and infrastructure assessment, IAIP is able to independently analyze information from multiple Intelligence Community sources, as well as from its fellow DHS entities. Lastly, IAIP is able to provide key information to the American citizenry, accompanied by suggested protective measures.

IAIP's singular focus on the homeland allows it to carry out all missions assigned to it by the Homeland Security Act, including the following:

- Facilitating the creation of requirements, on behalf of the Secretary of Homeland Security and DHS leadership, to other DHS components, and to the larger intelligence, law enforcement, and homeland security communities, in order to integrate homeland security information from all sources with vulnerability and risk assessments for critical infrastructure prepared by IAIP;
- Providing the full-range of intelligence support -- briefings, analytic products, including competitive analysis, "red teaming," and tailored analysis responding to specific inquiries, and other support -- to the DHS leadership and the rest of DHS;

2

[2] Ce courrier se trouve reproduit in extenso dans les annexes.

Lettre du 13 avril 2004 de MM. Ridge, Mueller et Brennan au Sénat (extraits).

information. Nothing in this explanatory letter is intended to modify the definitions or obligations of this MOU or other relevant directives or agreements.

The President and Congress have not directed, and, as a matter of effective government and common sense, should not direct, that all USG functions related to terrorism, including defense, intelligence, domestic law enforcement, diplomatic, economic, and a host of others be carried out by a single department or agency. In order both to ensure that no vital piece of intelligence is missed and to ensure that all departments and agencies, as well as our national leadership, receive the best possible analytic support, it is necessary to treat the analysis of terrorism-related information as a shared responsibility.

We look forward to continuing to work with your Committee as we strive to enhance our ability to protect our Nation from terrorists seeking to harm us. If you have any questions about this matter, then please have your staff contact Phil Lago with the Director of Central Intelligence at 703-482-6590, or Eleni Kalisch with the Director of the Federal Bureau of Investigation at 202-324-5051, or Ken Hill with the Secretary of Homeland Security at 202-282-8222, or Cynthia Bower with the Director of the Terrorist Threat Integration Center at 703-482-3354.

Sincerely,

Thomas J. Ridge
Secretary,
Department of Homeland Security

Robert S. Mueller III
Director,
Federal Bureau of Investigation

George J. Tenet
Director of Central Intelligence

John O. Brennan
Director,
Terrorist Threat Integration Center

4

Aux Etats-Unis, il fallut attendre le 12 décembre 2004 et la promulgation de la nouvelle législation sur la communauté du renseignement – *Intelligence Reform and Terrorism Prevention Act* – pour que cet échafaudage administratif parfois incertain trouva une base légale et fut soumis à un effort de rationalisation. Le texte détermina ainsi la création d'un très fédérateur *National Counterterrorism Center* (NCTC), auprès du non moins nouveau *Director of National Intelligence* (DNI) – chargé de coiffer l'ensemble de la communauté du renseignement. Placé à la fois sous la tutelle du DNI et du Président des Etats-Unis, le directeur du NCTC anime et coordonne l'ensemble des services pour le renseignement de nature contre-terroriste tout en intégrant les personnels et les missions du TTIC, mettant fin ainsi – espère-t-on – aux désaccords relatifs aux partages des compétences.

⇨ **Ces changements, loin de traduire l'existence d'un effort conceptuel qui aurait précédé les multiples aménagements rythmant depuis près de quatre ans la vie de la communauté américaine du renseignement, résultent principalement d'un seul phénomène corporatiste : chaque administration s'est efforcée de capter les missions d'intérêts prioritaires pour assurer sa pérennité dans la structure fédérale. Au-delà des discours officiels, nous constatons que les vastes réformes du renseignement adoptées récemment harmonisent leurs relations en entérinant les positions prises par les différents acteurs.**

Au Canada en revanche, un processus exactement inverse est observé. Les institutions en charge du renseignement, épargnées des remises en cause adressées à leurs homologues des Etats-Unis, n'ont pas connu une telle période d'amendements par soubresauts. Au contraire, leur fonctionnement se caractérise par une relative stabili-

té jusqu'à la promulgation du nouveau cadre juridique des activités de sécurité, le 27 avril 2004 – *Securing an open society : Canada's National Security Policy*. Entre 2001 et 2004, sur le plan de l'organisation des services, des modifications secondaires les touchèrent pour les activités de surveillance des frontières et des flux migratoires. Parallèlement, au terme des débats parlementaires engagés pour définir la nouvelle politique sécuritaire du pays, le Premier Ministre avalisa l'idée de fonder une structure sur le modèle du NCTC américain, en l'inscrivant dans le document d'avril 2004. C'est ainsi qu'en octobre 2004, dans un cadre juridique retouché, le *Canadian Security Intelligence Service* (CSIS) inaugura une structure dédiée à la fusion du renseignement de sécurité en matière de terrorisme, le *Integrated Threat Assessment Center* (ITAC). Parfaitement intégré au sein du service de renseignement canadien, il s'impose comme un interlocuteur unique maîtrisant l'ensemble de la chaîne des métiers du renseignement – collecte, analyse, production, fusion, dissémination. Les autres services de la communauté canadienne ont parfois, selon leur spécialité, installé des bureaux réservé aux échanges avec l'ITAC, à l'image du *Communications Security Etablishment* (CSE, chargés des interceptions) qui a créé un *Office of Counterterrorism.*

b – Les problèmes de concurrence inhérents à la communauté américaine du renseignement. Mise en place du *NIPF*.

Aux Etats-Unis, la superposition des missions des services – entre TTIC, CTC ou IATIC – postérieurement aux évènements du 11 septembre, a mis en exergue la contre productivité dans laquelle leurs querelles les confinaient, aux yeux d'une population de responsables politiques auparavant peu préoccupée par la bureaucratie du renseignement.

⇨ **Pendant plus de cinquante ans, le *National Security Council* se contenta de déterminer globalement les besoins en renseignement du pouvoir exécutif, en se félicitant parfois que les antagonismes internes à la communauté du renseignement soit le gage d'une obéissance renforcée et d'une production de qualité.**

C'était le temps où l'échelon politique se préoccupait dans le meilleur des cas de la rédaction annuelle du *National Foreign Intellligence Program*[3]. Sa gestion administrative et le soin au quotidien de ventiler les missions correspondantes entre les divers services incombaient ensuite à deux hommes : le secrétaire à la Défense et le directeur central du renseignement (*Director of Central Intelligence* – DCI). Or ce dernier cumulait ce titre avec celui de patron de la CIA[4], une superposition dont il ne tirait que rarement profit, cette confusion des fonctions entre figure de proue du renseignement et chef de la CIA n'ayant jamais été accompagnée par les extensions d'autorité correspondantes qui auraient pu régler les conflits de compétences avec les agences du département de la Défense, celles du département de la Justice, et du Trésor. Durant près de 50 ans, selon un dispositif bien connu dans de nombreux pays occidentaux, le pouvoir exécutif favorisait implicitement les jeux de concurrences (parfois dans le but de mener simultanément sur un même dossier des stratégies divergentes) et laissait divers organismes s'arrogeaient parallèlement les mêmes objectifs du *National Foreign Intelligence Program* – des comportements fratricides toujours confortés par les termes généralistes de cet ordre de mission.

[3] Document cadre annuel élaboré par les cadres du *National Security Council* et du *President Foreign Intelligence Advisory Board.* Depuis la loi de réforme du 12 décembre 2004, ce document cadre, comme nous le verrons plus loin, a vu son champ d'application considérablement élargi et a pris l'appellation de *National Intelligence Program.*

[4] Jusqu'à la récente réforme que nous détaillerons plus loin, le poste de *Director of Central Intelligence* et de *Director of the Central Intelligence Agency* revenait toujours au même homme. Or, le patron de la CIA, dans son rôle de coordinateur de la communauté du renseignement, a toujours été dépourvu de prérogatives contraignante (principalement d'un point de vue budgétaire) dans l'ancienne configuration.

Cependant, cette époque semble, pour partie, révolue. Dorénavant et pour la première fois depuis l'entrée en vigueur du *National Security Act* en 1947[5], un plan de renseignement établit précisément et formellement les priorités assignées aux différents services sur une base annuelle. Il s'agit du *National Intelligence Priorities Framework* (NIPF), régi par un décret présidentiel classifié[6], publié en mars 2003. Il se présente comme une charte d'accompagnement opérationnel au *National Intelligence Program* (NIP ; l'ex *National Foreign Intelligence Program).*

- ⇨ **Le NIP énumère et justifie les objectifs stratégiques.**
- ⇨ **Le NIPF désormais en traduit les priorités d'un point de vue tactique.**

Le NIPF s'impose donc comme un cadre concret, sorte de feuille de route pour les responsables de la coordination des services. Son instauration répond aux critiques des membres républicains des commissions spécialisées du Congrès, lesquels, depuis septembre 2001, reprochaient régulièrement aux agences de renseignement ce manque cruel de concertation dans les choix de leurs missions et une déperdition de leurs moyens. Selon les éléments évoqués par nos sources quant au contenu de ce décret présidentiel fondateur de mars 2003, le nouveau NIPF a ainsi pour vocation à transformer en objectifs détaillés – listant les cibles et les institutions chargées de les suivre – les diverses recommandations du *National Security Council* à la communauté du renseignement. En confiant l'accomplissement de cette tâche au nouveau *Director of National Intelligence*, auquel la Maison Blanche a cette fois conférer une véritable autorité, les structures de commandement du renseignement de sécurité possède un dispositif puissant, capable de répartir et d'imposer des missions de

[5] Cette loi réglemente la communauté du renseignement dans son ensemble. La plupart des réformes passées depuis le 11 septembre se présentent sous la forme d'amendements au *National Security Act*.
[6] *National Security Presidential Directive*, n° 26, mars 2003.

renseignement de sécurité entre le FBI, la CIA, le département de la Défense et le Trésor.

⇨ Les capacités des services de renseignement ne se dissolvent plus dans le fonctionnement de la puissance publique. À la faveur des redéfinitions opérées depuis le 11 septembre 2001, ils tendent à s'agréger aux plus hauts niveaux du pouvoir exécutif. Sur ce point, l'échelon administratif – toujours plus élevé – des dirigeants de la communauté du renseignement (l'actuel DNI a rang d'ambassadeur) traduit le pouvoir politique qu'ils conquièrent en ce moment.

2. La recherche d'une centralisation et d'une reconnaissance du renseignement de sécurité.

a - L'institutionnalisation d'un traitement transversal du renseignement de sécurité, au détriment d'une intégration verticale.

Au regard de notre problématique, l'instauration de ce poste de Directeur national du renseignement (ie. le responsable de toute la communauté du renseignement aux yeux des pouvoirs exécutif et parlementaire) nous intéresse prioritairement car elle crée un nouvel espace de coordination et d'homogénéisation du renseignement de sécurité intérieure.

Etabli par la loi de réforme de la communauté du renseignement précitée du 12 décembre 2004, ce poste met d'abord fin au projet de bâtir « *un MI5 à l'Américaine* ». Cette question-là, longuement débattue, ne fut réellement tranchée que lors de la rédaction finale, en février et mars 2005, du rapport parlementaire intitulé *Intelligence Capabilities of the U.S regarding Weapons of Mass Destruction*[7] ; conférant simultanément à ce futur Directeur national du renseignement une autorité indiscutée sur les questions intérieures. Bien que consacrée au renseignement en matière de prolifération des armes de destruction massives, cette enquête du Congrès s'appuyait en effet sur un audit quasi-exhaustif des moyens et des performances des services de renseignement. Et après plusieurs mois d'entretiens de leurs responsables et d'analyses des productions internes, il engageait vivement le pouvoir politique à renoncer à l'idée de singulariser le renseignement de sécurité intérieure sur le modèle britannique : « *We recom-*

[7] *Report of the WMD Commission*. 31 mars 2005. Ce rapport public est accessible via un site dédié, www.wmd.gov.

mended that the policymakers re-evaluate the wisdom of creating a separate agency – an equivalent to the British MI5… »[8]

La clarté de cette prise de position clôturait en réalité des débats lancés dès la mi-septembre 2001 à l'intérieur de ces mêmes enceintes du Capitole à l'instigation du futur conseiller pour les affaires de sécurité intérieure de la Maison Blanche, Tom Ridge. Celui-ci ne disposait alors que d'un bureau rattaché au *National Security Council*, mais l'histoire le désignait déjà comme le père fondateur du département de la Sécurité Intérieure[9]. Le sujet fut ainsi une première fois exploré par la Commission conjointe des affaires de renseignement de la Chambre des Représentants et du Sénat, qui tenta la première d'identifier les dysfonctionnements ayant facilité les attaques du 11 septembre[10]. Avant d'être définitivement tranché courant 2005. Les parlementaires opposés à ce projet de « MI5 à l'Américaine » et qui avaient enquêté sur la performance de la communauté du renseignement avançaient trois arguments :

- ⇨ **La communauté américaine du renseignement était une utopie. Il n'existait pas réellement avant 2001 de « communauté », et cette carence expliquait à elle seule bien des errements. Rajouter une énième structure ne résolvait rien.**

- ⇨ **La création théoriquement ex-nihilo d'une telle structure revenait dans la pratique soit à démanteler le FBI soit à simplement le requalifier. Or le problème ne portait pas, notamment, sur la légitimité du FBI, mais sur son mode de gestion opérationnel des données en matière de contre-terrorisme, et sur la fusion de ces données avec celles qui sont produites par d'autres services…**

[8] Ibid., p. 468.
[9] Dans le courant de l'année 2002, Tom Ridge multipliera les déplacements à Londres pour rencontrer les responsables du MI5 et des représentants du *Joint Intelligence Committee.*
[10] *Joint Inquiry Report*, 11 décembre 2002.

⇨ **Les défaillances observées semblaient provoquer par un manque cruel de coordination entre divers services de sécurité ayant chacune des missions non exhaustives, voire marginales, sur les questions intérieures (la CIA, le Trésor, les Douanes…). Une structure exclusive dédiée au renseignement de sécurité intérieure n'y changeait rien.**

En creux, les discussions sur l'adaptabilité du modèle du *MI5* aboutirent à conforter les partisans d'un plan de réforme concentré sur le renforcement de la coordination interservices, militant pour de légères innovations organiques qui contraindraient « *la communauté du renseignement à véritablement travailler en commun* » sur les questions sécuritaires. L'idée-force de ceux-là – telle qu'elle s'imposera dans la loi de réforme de décembre 2004 – était bien de stimuler une approche transversale des organisations. Ainsi s'imposa la proposition d'instituer un poste de Directeur national du renseignement, officiellement en charge de gérer l'ensemble de la communauté du renseignement.

Cependant, comme souvent dans l'administration fédérale, les prérogatives liées à cette nouvelle fonction dépendaient étroitement des capacités de son premier titulaire à manœuvrer au sein de la bureaucratie sécuritaire pour obtenir les décrets du président et les directives du NSC lui octroyant *effectivement* les prééminences adéquates sur les autres barons de cette communauté, comme le souhaitaient la plupart des parlementaires.

b - La victoire provisoire de John Negroponte contre l'appareil de renseignement du département de la Défense.

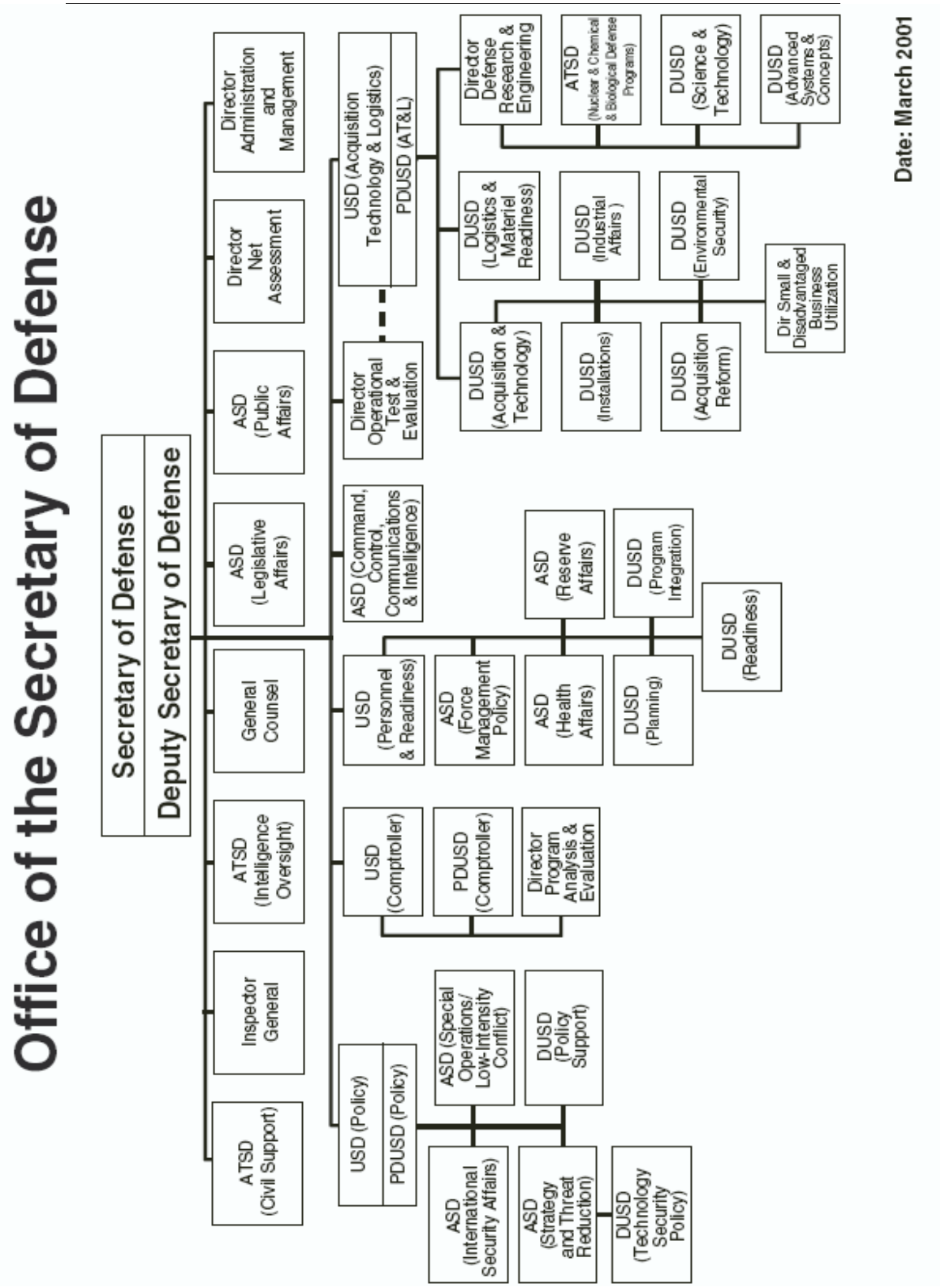
La décision des commissions du Sénat et de la Chambre des Représentants d'inscrire la création de ce poste dans la loi de réforme de décembre 2004 fut anticipée au Pentagone par un changement au sein du bureau de Donald Rumsfeld qui prit toutes les apparences d'un acte de guérilla bureaucratique : fin 2002, on instaura subitement un nouveau Sous-secrétaire à la Défense en charge du renseignement.

Confié le 7 mars 2003 à Stephen Cambone – l'un des théoriciens du bouclier antimissile[11] – ce nouveau Sous-secrétariat réservé aux affaires de renseignement se vit immédiatement assigné un rôle de coordinateur en direction des autres entités extérieures à l'administration de la défense. Donald Rumsfeld en personne, le 20 mai 2003, expliqua qu'il entendait ainsi « *améliorer les interactions* » entre les diverses activités de renseignement de ses services et les autres agences du gouvernement, en particulier la CIA[12]. Pour le sérail, ce voeu pieux caractérisait les démarches entreprises par la Défense pour neutraliser toute velléité de coordination du renseignement qui lui échapperait.

[11] Ancien directeur des politiques stratégiques au bureau du Secrétaire à la Défense, de 1990 à 1993. Ancien directeur de cabinet de la Commission parlementaire sur la gestion et l'organisation de la sécurité nationale dans le domaine spatial, de juillet 2000 à janvier 2001, dont le rapport final servit assez largement de plate-forme de programme durant les premiers mois d'exercice de Donald Rumsfeld au Pentagone.

[12] In. « *New office to help set DoD intelligence priorities* », American Forces Press Service, 20 mai 2003.

Fig.2： La place du renseignement dans la direction de l'administration de la Défense avant septembre 2001.



Dans la pratique, les conseillers de Rumsfeld l'avaient convaincu de placer le travail de toutes les agences de renseignement internes du Pentagone[13] sous la houlette d'un responsable unique, dont le nouveau niveau hiérarchique le placerait au moins dans une relation d'égal à égal avec le directeur de la CIA et, dans un futur proche, avec d'éventuels coordinateurs désignés par la Présidence. Sur la base d'une telle stratégie, et au regard des adaptations aux missions de *Homeland security* exigées par la Maison Blanche, la gestion des affaires de renseignement et de sécurité intérieure au Pentagone a connu d'importants remaniements ces trois dernières années :

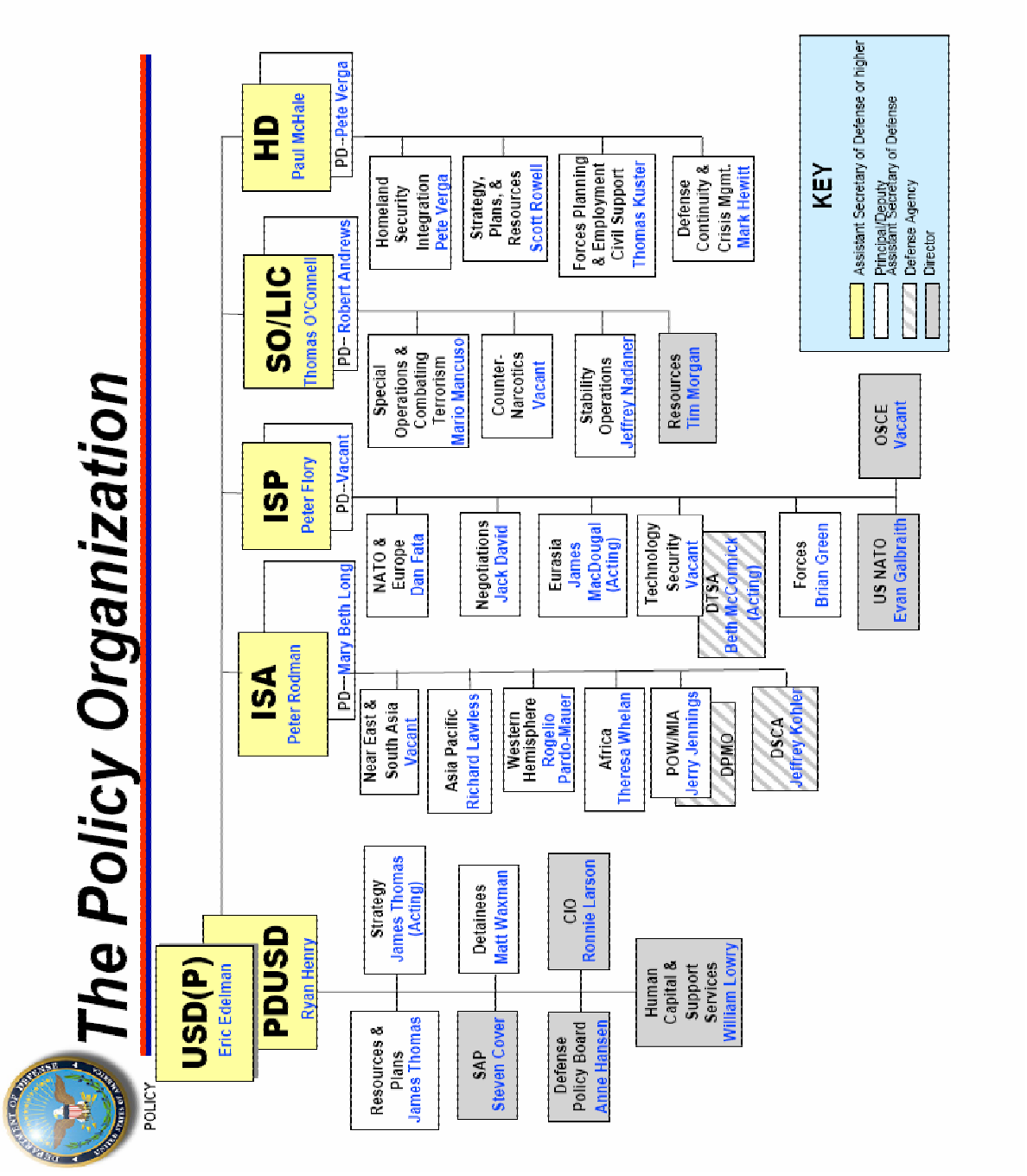
- ⇨ **Ce récent poste d'*Under-secretary of Defense for Intelligence* coordonne les deux grandes activités de renseignement du département : celles qui sont menées à des fins stratégiques ou tactiques par des agences militaires sous la tutelle exclusive du bureau du secrétaire à la Défense ; et celles qui sont menées à des fins tactiques seulement par des unités opérationnelles appartenant à la chaîne de commandement du *Joint Chiefs of Staff*.**
- ⇨ **Le poste d'*Under-secretary of Defense for Policy* (voir organigramme figure 3) occupe une place centrale pour notre problématique. Il concentre en effet la planification des *Special Operations Low Intensity Conflict* (SO/LIC, c'est-à-dire en particulier les opérations antiterroristes menées hors des théâtres de guerre – Afghanistan et Irak – à l'image de celles qui sont engagées depuis 2002 au Yémen, en Arabie Saoudite, en Somalie, au Kenya, en Mauritanie) et le suivi des politiques de *Homeland defense* (avec l'intégration des objectifs de *Homeland security* au travers les organes du département de la Défense).**

[13] C'est-à-dire les agences de renseignement relevant statutairement du bureau du Secrétaire de la Défense : la *National Security Agency*, de la *Defense Intelligence Agency*, de la *National Imagery and Mapping Agency,* du *National Reconnaissance Office*, du *Counterintelligence Field Activity Board* et du *Defense Security Service*. Nous n'évoquons pas ici les régiments et les bataillons chargés du renseignement tactique, dont la direction relève du *Joint Chief of Staff*.

- ⇨ Le poste d'*Assistant to the Secretary of Defense for Intelligence Oversight* (un poste créé en 1982 et extrait des services de l'Inspection générale du département) centralise – et protège – toutes les activités de contrôle des services de renseignement.
- ⇨ Le poste d'*Assistant to the Secretary of Defense for Networks and Information Integration* (qui remplace le poste *d'Assistant to the Secretary of Defense for Command Control Communication and Intelligence*) pilote les nouveaux programmes de *networks-centric warfare*. La directive précisant ses attributions a été signée au mois de mai 2005. Il influencera de manière incidente la production du renseignement tactique de par son rôle de coordination des réseaux d'informations.

Outre une volonté ancienne de maintenir son contrôle sur le renseignement produit pour le gouvernement, ces différentes démarches du Pentagone répondirent également au souci de la hiérarchie de la défense (civile et militaire) de ne pas être dépossédées au profit des bénéficiaires de la politique de *Homeland security*. A fortiori dans le domaine du renseignement ; dès lors que le pouvoir exécutif privilégiât une approche transversale du renseignement de sécurité intérieure, elle impliquait – peu ou proue – que les agences ad hoc de la Défense se mobilisent pour combattre le terrorisme aussi bien à l'intérieur qu'à l'extérieur du territoire.

Fig.3 : L'intégration de la gestion du contre-terrorisme et de la *Homeland security policy* au sein du Sous-secrétariat à la Défense pour les affaires politiques.



Témoin de ce phénomène : la croissance des missions de la NSA à l'intérieur du territoire consécutivement aux dispositions juridiques introduites par le *US Patriot Act*.

Ainsi, entre fin 2002 et fin 2004, la création d'un poste de *Director of National Intelligence* a bien été sapée par le bureau du secrétaire de la Défense, qui, sur les différents champs du renseignement, le percevait surtout comme une initiative visant à circonscrire son pouvoir aux opérations tactiques – au moment où la Maison Blanche sommait la hiérarchie du Pentagone d'atteindre plus rapidement des résultats tangibles en Irak et en Afghanistan (mise en place d'un processus démocratique avec élection au suffrage universel).

Dans un premier temps, et comme souvent dans la vie politique américaine, le pouvoir exécutif n'a pas vraiment déterminé dans les textes officiels la répartition détaillée des prérogatives entre l'ancienne institution et sa nouvelle rivale sur les questions de renseignement. Laissant aux femmes et aux hommes en charge de les diriger de se départager par eux-mêmes, quite à se combattre âprement. Le choix de George Bush et de Condoleeza Rice, le 17 mars 2005, de désigner une personnalité de la carrure de l'ambassadeur John Negroponte indiquait simplement leur intention qu'une administration nationale du renseignement s'affranchît réellement du Pentagone. Leur favori offrait plusieurs atouts. Profitant d'abord de l'indéniable avantage d'avoir assumé les fonctions d'ambassadeur des Etats-Unis auprès des Nations-Unies depuis 2001, et à ce titre d'avoir géré les conséquences diplomatiques des errements de la communauté du renseignement lors de la crise irakienne, puis d'ambassadeur à Bagdad[14], Negroponte, grâce à un parcours singulier, possédait à ce stade aux yeux de tous une autorité suffisante sur les questions de renseignement aux Etats-Unis.

[14] Jusqu'en mars 2005, où il rattrapa – vaille que vaille – les maladresses de l'administrateur Paul Bremer.

⇨ *John Dimitri Negroponte, né le 21 juillet 1939 à Londres. Fils d'un armateur grec. Diplômé de Yale en 1960 et fonctionnaire du département d'Etat de 1960 à 1997 (recouvrant probablement des responsabilités à la CIA de 1960 à 1975). Ambassadeur au Honduras de 1981 à 1985 (durant cette période, l'aide militaire américaine au Honduras passa de 4 millions $ par an à 77 millions $ aux fins de financer les sites paramilitaires des Contras – en particulier la base El Aguacate – chargés de déstabiliser le pouvoir sandiniste au Nicaragua voisin) ; dans ces fonctions, il fut accusé d'avoir couvert les opérations antipersonnelles d'un groupe coordonné par la CIA, le Battalion 3-16 , reconnu coupable d'avoir assassiné plusieurs personnalités sandinistes. Nos sources évoquent en outre plusieurs dossiers détaillant sa responsabilité dans l'affaire dite Iran-contras, des ventes d'armes clandestines à l'Iran via l'aide aux contras. Assistant du Secrétaire d'État pour les affaires océaniques, environnementales et scientifiques de 1985 à 1987. Membre du National Security Council de 1987 à 1989. Ambassadeur au Mexique de 1989 à 1993. Ambassadeur aux Philippines de 1993 à 1996. De 1997 à 2001 il travaille dans le secteur privé, comme conseiller de la direction du groupe McGrall Hill – un fleuron de l'industrie de l'information spécialisée, propriétaire du cabinet de notation Standard & Poor's et des groupes de presse Aviation Week (destinés aux professionnels de l'aérospatial), Platts (l'un des leaders sur le marché de l'information pétrolière) et Business Week. À la faveur de l'investiture de George W Bush en janvier 2001, il a repris des responsabilités au département d'Etat en étant choisi par la Maison Blanche pour prendre le poste d'ambassadeur aux Nations-Unies. Le 19 avril 2004, le président l'a nommé ambassadeur des Etats-Unis en Irak. John Negroponte est marié depuis décembre 1976 à Diana née Villiers, ressortissante britanni-*

que naturalisée en 1981, fille de Sir Charles Villiers, jadis président de l'un des plus grand groupe sidérurgique britannique, British Steel Corporation (ils se sont rencontrés en 1967 à Saïgon alors qu'elle rendait visite à son oncle, l'ambassadeur britannique auprès du Sud Vietnam, Peter Wilkinson). Le couple a cinq enfants, dont quatre adoptés au Honduras. John Negroponte parle français et grec. Son frère cadet, Nicholas Negroponte (né en 1943) réalise une brillante carrière dans l'industrie de l'information ; il est le fondateur du très influent magasine de la côte Ouest Wired, et surtout il préside aux destinées du Media Lab (l'un des pôles pour la recherche sur l'évolution des systèmes d'information) au sein du Massachusetts Institute of Technology (MIT).

Au terme de plusieurs escarmouches politiques, tenues au Congrès et à la Maison Blanche, John Negroponte a obtenu depuis mai 2005 que deux attributions majeures soient transférées sur son poste. Dorénavant :

- **Le *Director of National Intelligence* supervisera la ventilation des fonds secrets - actuellement évalués à 60 milliards $ - sur lesquels le Pentagone avait la haute main depuis 1947. En outre, c'est lui qui préparera les autorisations budgétaires pour l'ensemble de la communauté du renseignement, en concertation avec le département du Trésor et le directeur du bureau du Budget de la Maison Blanche.**

- **Le *Director of National Intelligence* déterminera les choix des futurs patrons des agences de renseignement – y compris celles qui sont dépendantes du Pentagone. Il transmettra au Congrès les propositions de nominations pour les postes suivants : directeur de la NSA, directeur du NRO, directeur de la NGIA, assistant du secrétaire d'Etat**

en charge du renseignement et de la recherche, directeur du bureau renseignement du département à l'Energie, directeur du bureau de contre-espionnage du département à l'Energie, assistant du secrétaire au Trésor en charge du renseignement, assistant exécutif du directeur du renseignement du FBI et assistant du secrétaire de la Sécurité Intérieure en charge de l'information et de l'analyse. En cas de désaccords avec le département de la Défense sur les personnalités à soumettre au vote de confirmation du Congrès pour ces postes, il reviendra au président de trancher personnellement.

Ces évolutions, réclamées et négociées depuis sa prise de fonction par Negroponte, en particulier celle – si sensible – portant sur le financement de la communauté du renseignement, n'ont pris une dimension officielle que depuis juin 2005, au moment où la Chambre des Représentants a dû se prononcer en faveur de la loi d'autorisation budgétaire pour les activités de renseignement[15] qui entérine cette captation d'autorité par le *Director of National Intelligence*, au détriment des hiérarques du Pentagone. Pour compensation, ils ont obtenu la nomination du général Michael Hayden – le patron de la NSA jusqu'en juin 2005 - au poste d'adjoint de Negroponte ; manière de s'assurer que le nerf du renseignement américain (ses dispositifs d'écoute) demeurera, notamment, entre les mains d'un responsable militaire.

[15] *Intelligence Authorization Act for FY 2006*. H.R 2475.

c – L'objectif de rationalisation du DNI pour les méthodes et les outils de renseignement mis en œuvre au profit de la sécurité intérieure.

Compte tenu de la jeunesse de ces transformations organiques, on ne constate pas, à proprement parler, l'apparition de méthodes et d'outils inédits pour le renseignement de sécurité intérieure qu'aurait promu le nouveau DNI.

En revanche, ses objectifs dans ce domaine traduisent une volonté de rupture manifeste. Ceux-ci s'articulent autour de la priorité de fusionner les productions des services en charge du renseignement administratif et des services en charge du renseignement judiciaire, non pas sur des bases théoriques mais au regard de finalités opérationnelles. Ainsi, à l'intérieur du nouveau DNI, puisque le *Patriot Act* abaissait les frontières entre le renseignement judiciaire et le renseignement administratif, plus rien ne commandait de maintenir une distinction entre renseignement de sécurité intérieure et renseignement extérieur.

> ⇨ **La lutte contre le terrorisme s'imposant comme la priorité ultime du pays, la seule typologie opérationnelle est celle distinguant le renseignement judiciaire et administratif de nature défensive, du renseignement opérationnel de nature offensive.**

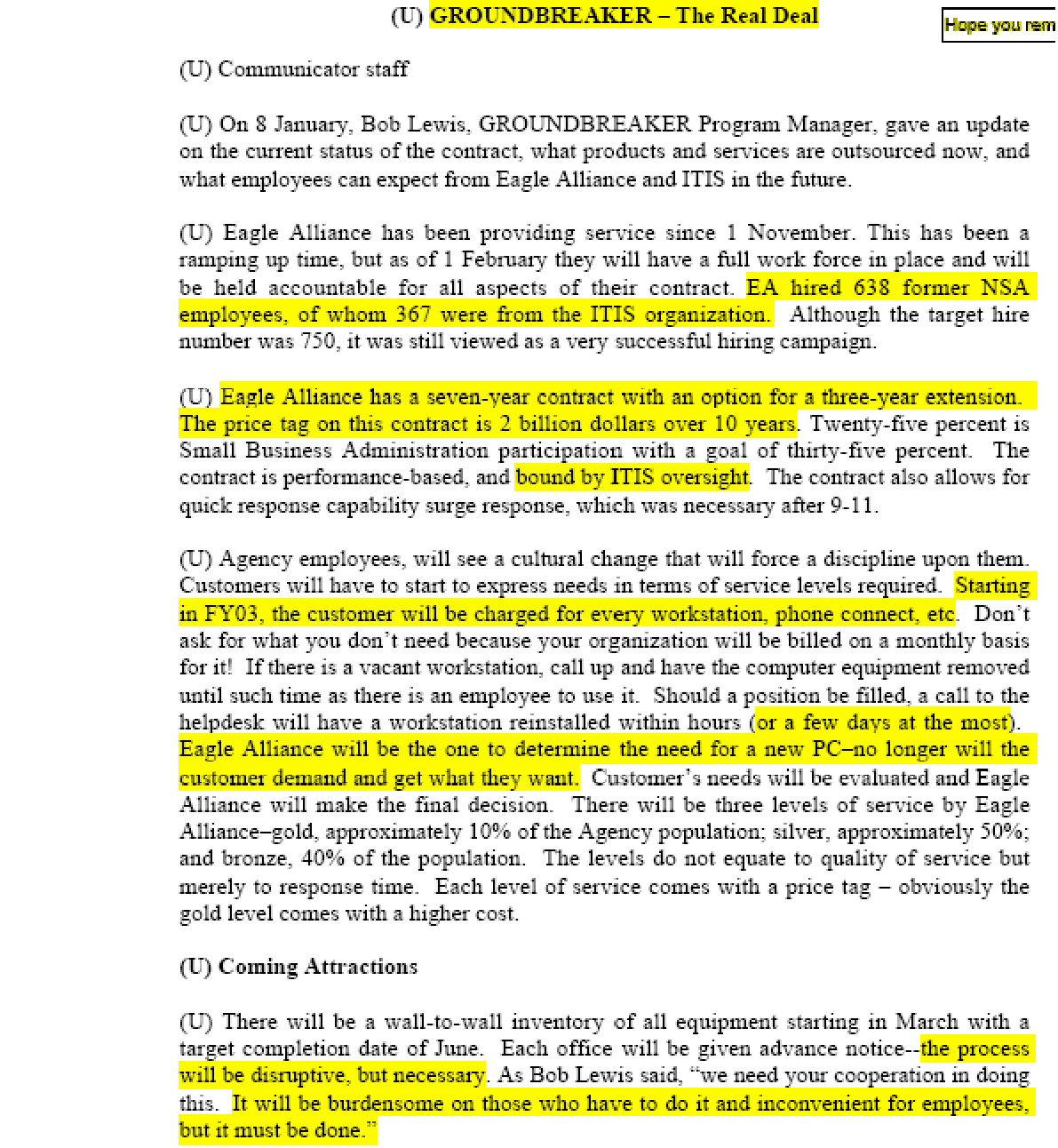
Cette préoccupation s'est notamment traduite par le rattachement auprès du DNI du nouveau *National Counterterrorism Center* (NCTC), qu'il anime en agrégeant les productions de la CIA, de la NSA, du FBI, du Trésor et du département de la Sécurité Intérieure, et qui est chargé d'informer directement le bureau ovale. Initialement prévu par un décret présidentiel du 27 août 2004[16], ce NCTC

[16] Executive Order 13354.

devait être rattaché au département de la Sécurité Intérieure ; traduisant alors la permanence d'une approche du renseignement privilégiant la distinction entre intérieur et extérieur au territoire. Cependant, après le vote de la réforme de la communauté du renseignement du 12 décembre 2004 instituant le DNI, une autre rationalité de la gestion du renseignement s'imposait. On ne distinguait plus dès lors de catégories du renseignement selon ses modes et ses lieux de production (intérieur, extérieur, administratif, judiciaire) mais bien selon ses finalités (prévention du terrorisme, de l'espionnage, des trafics de drogue, des trafics d'arme, du blanchiment et de la prolifération).

Progressivement, ces changements de fonds devraient se traduire par le développement d'outils adaptés. Mais dès à présent, sur la seule problématique touchant le renseignement en matière de contre-terrorisme, de nouvelles méthodes lourdes de conséquences prédominent. Il s'agit en particulier des diverses démarches pour fusionner des productions apparemment disparates, aboutissant à rapprocher le renseignement en matière de terrorisme avec le renseignement en matière de criminalité, de contrefaçon ou de trafic d'armes. Cette approche tient compte d'observations effectuées à l'échelon opérationnel, où il apparaissait par exemple évident que la compréhension de réseau de contrefaçon permet d'identifier la construction de structures de financement cherchant offrir une assistance clandestine à une future cellule de militants islamistes – de tels constats ayant laminé la pertinence des typologies, voire des cloisonnements, naguère à l'œuvre dans les services américains, et qui demeurent en Europe.

Fig. Le malaise des agences internes au Pentagone pour répondre à la croissance des requêtes. Note de travail interne à la NSA sur l'état d'avancement du programme *Groundbreaker* (sous-traitance des fonctions de maintenance pour libérer des personnels et ainsi mieux répondre aux demandes de missions de la communauté du renseignement).



(U) GROUNDBREAKER – The Real Deal

Hope you rem

(U) Communicator staff

(U) On 8 January, Bob Lewis, GROUNDBREAKER Program Manager, gave an update on the current status of the contract, what products and services are outsourced now, and what employees can expect from Eagle Alliance and ITIS in the future.

(U) Eagle Alliance has been providing service since 1 November. This has been a ramping up time, but as of 1 February they will have a full work force in place and will be held accountable for all aspects of their contract. EA hired 638 former NSA employees, of whom 367 were from the ITIS organization. Although the target hire number was 750, it was still viewed as a very successful hiring campaign.

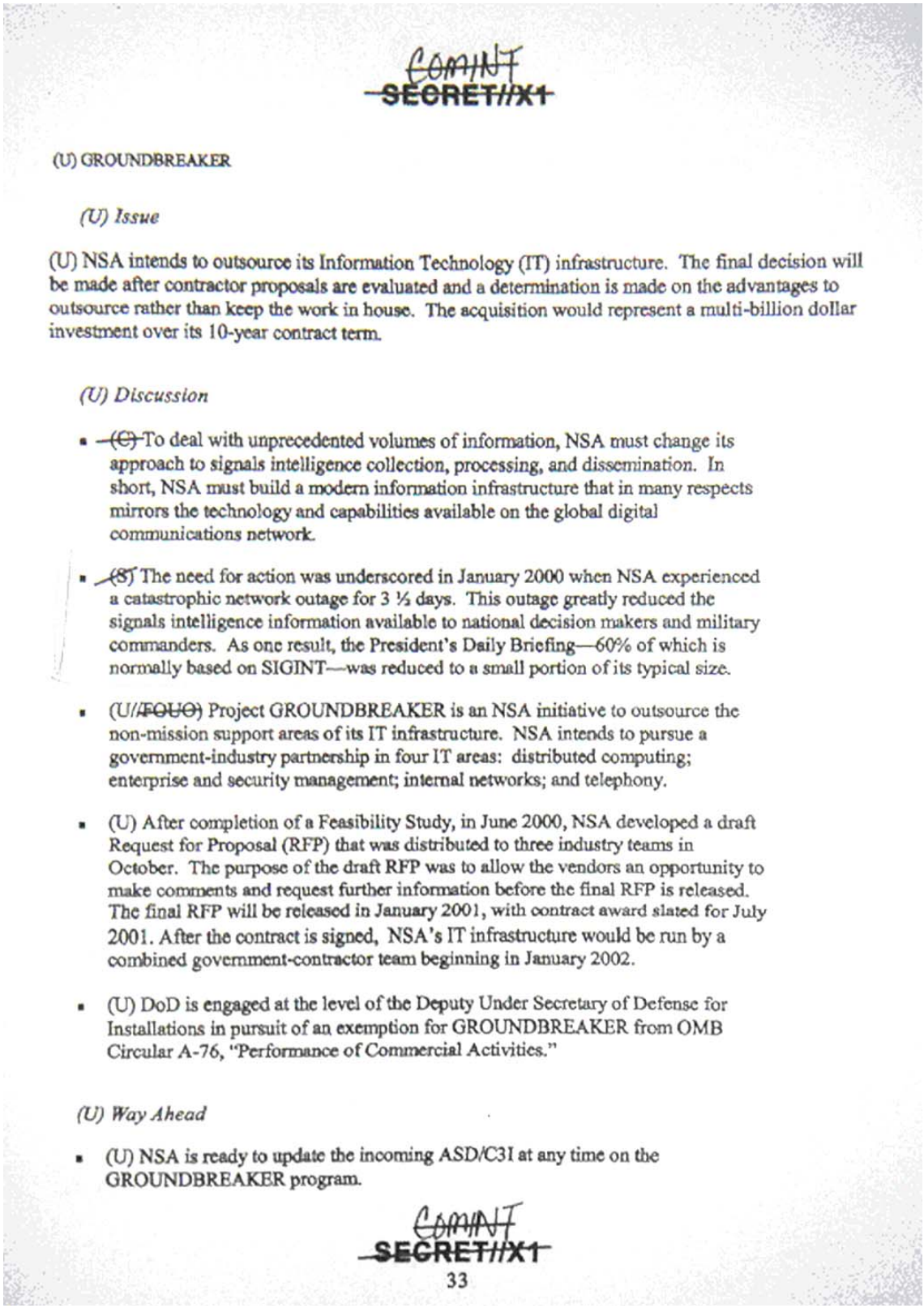
(U) Eagle Alliance has a seven-year contract with an option for a three-year extension. The price tag on this contract is 2 billion dollars over 10 years. Twenty-five percent is Small Business Administration participation with a goal of thirty-five percent. The contract is performance-based, and bound by ITIS oversight. The contract also allows for quick response capability surge response, which was necessary after 9-11.

(U) Agency employees, will see a cultural change that will force a discipline upon them. Customers will have to start to express needs in terms of service levels required. Starting in FY03, the customer will be charged for every workstation, phone connect, etc. Don't ask for what you don't need because your organization will be billed on a monthly basis for it! If there is a vacant workstation, call up and have the computer equipment removed until such time as there is an employee to use it. Should a position be filled, a call to the helpdesk will have a workstation reinstalled within hours (or a few days at the most). Eagle Alliance will be the one to determine the need for a new PC–no longer will the customer demand and get what they want. Customer's needs will be evaluated and Eagle Alliance will make the final decision. There will be three levels of service by Eagle Alliance–gold, approximately 10% of the Agency population; silver, approximately 50%; and bronze, 40% of the population. The levels do not equate to quality of service but merely to response time. Each level of service comes with a price tag – obviously the gold level comes with a higher cost.

(U) Coming Attractions

(U) There will be a wall-to-wall inventory of all equipment starting in March with a target completion date of June. Each office will be given advance notice--the process will be disruptive, but necessary. As Bob Lewis said, "we need your cooperation in doing this. It will be burdensome on those who have to do it and inconvenient for employees, but it must be done."

Fig. Document officiel de la NSA présentant le programme Groundbreaker.



~~COMINT~~
~~SECRET//X1~~

(U) GROUNDBREAKER

(U) Issue

(U) NSA intends to outsource its Information Technology (IT) infrastructure. The final decision will be made after contractor proposals are evaluated and a determination is made on the advantages to outsource rather than keep the work in house. The acquisition would represent a multi-billion dollar investment over its 10-year contract term.

(U) Discussion

- ~~(C)~~ To deal with unprecedented volumes of information, NSA must change its approach to signals intelligence collection, processing, and dissemination. In short, NSA must build a modern information infrastructure that in many respects mirrors the technology and capabilities available on the global digital communications network.
- ~~(S)~~ The need for action was underscored in January 2000 when NSA experienced a catastrophic network outage for 3 ½ days. This outage greatly reduced the signals intelligence information available to national decision makers and military commanders. As one result, the President's Daily Briefing—60% of which is normally based on SIGINT—was reduced to a small portion of its typical size.
- (U//~~FOUO~~) Project GROUNDBREAKER is an NSA initiative to outsource the non-mission support areas of its IT infrastructure. NSA intends to pursue a government-industry partnership in four IT areas: distributed computing; enterprise and security management; internal networks; and telephony.
- (U) After completion of a Feasibility Study, in June 2000, NSA developed a draft Request for Proposal (RFP) that was distributed to three industry teams in October. The purpose of the draft RFP was to allow the vendors an opportunity to make comments and request further information before the final RFP is released. The final RFP will be released in January 2001, with contract award slated for July 2001. After the contract is signed, NSA's IT infrastructure would be run by a combined government-contractor team beginning in January 2002.
- (U) DoD is engaged at the level of the Deputy Under Secretary of Defense for Installations in pursuit of an exemption for GROUNDBREAKER from OMB Circular A-76, "Performance of Commercial Activities."

(U) Way Ahead

- (U) NSA is ready to update the incoming ASD/C3I at any time on the GROUNDBREAKER program.

~~COMINT~~
~~SECRET//X1~~

33

3 - Le renouveau du FBI, fer de lance de la collecte du renseignement de sécurité intérieure.

Avant le 11 septembre 2001, la croissance du budget du département de la Justice se justifiait déjà par un programme de modernisation pluriannuel du FBI. C'est ainsi qu'entre la loi d'autorisation fiscale pour 2000 (préparée et votée au printemps 1999) et celle qui est pour 2005, la seule ligne de crédit du département réservée à l'agence d'investigation a connu une augmentation de 68%. Après le 11 septembre et jusqu'en mai 2005 (date des derniers aménagements organiques qui ont touché l'agence), les débats et les réformes engagés s'inscrivirent donc dans le sillage d'un constat critique déjà dressé quant à la nécessité d'adapter le FBI.

a – La décision de bâtir un *National Security Service* responsable de la production du renseignement de sécurité.

Comme nous l'avons précédemment observé, peu de temps après les attaques contre le *World Trade Center* et le Pentagone, plusieurs responsables politiques explorèrent l'idée de développer une nouvelle structure sur le modèle du *MI5* britannique. Dans cette perspective, les adjoints du ministre de la Justice John Aschcroft proposèrent d'utiliser l'organisation du FBI comme socle de ce projet. Aussi, durant cette période d'incertitude (de janvier 2002 à mars 2003), le directeur du FBI Robert Mueller prit plusieurs dispositions afin de démontrer les capacités de son agence de se muer en *MI5* ; lui permettant d'une part de couper court aux projets opportunistes du département de la Sécurité Intérieure en ce domaine, et d'autre part d'apporter des premières réponses aux critiques les plus féroces de la presse et des parlementaires contre l'agence.

⇨ **La *Terrorism Task Force* du FBI, basé à New York, enquêtait sur Oussama Bin Laden depuis 1995 et s'était avérée incapable de loger la cellule de Hambourg et de connaître**

ses intentions, notamment à cause de la propension des directeurs de l'agence à partager le moins possible l'information la plus stratégique en termes de sécurité.

Robert Mueller ordonna donc de développer progressivement une direction du Renseignement (*Directorate of Intelligence*), chargé d'animer un nouveau réseau de groupes de contacts (les *Field Intelligence Groups*), c'est-à-dire des petites unités d'agents (de trois à une douzaine selon les États) formés à l'analyse du renseignement et placées dans chacune des 56 succursales du FBI répartis sur le territoire. Selon les plans du directeur, cette entité devait soit servir de plate-forme à un futur *MI5* (option d'un traitement vertical du renseignement de sécurité), soit intégrer un futur système d'agrégation et de coordination (option – retenue in fine – du traitement horizontal du renseignement de sécurité, chapeauté par le *Director of National Intelligence*).

Parallèlement à ces aménagements, le pouvoir exécutif tirait peu à peu les enseignements des travaux des diverses commissions parlementaires. La Maison Blanche les synthétisa sous la forme d'un mémorandum[17], adressé le 23 novembre 2004 au département de la Justice et qui recommandait de centraliser au niveau du bureau du directeur de l'agence toutes les productions recouvrant des questions de sécurité nationale, et de les placer sous les tutelles conjointes du patron du FBI et du directeur national du renseignement (DNI).

Après de longs échanges administratifs entre le bureau ovale et le département de la Justice, ponctués notamment par l'envoi d'un rapport classifié daté du 16 février 2005 où tous les responsables du FBI en charge d'activités de renseignement tentaient de dresser l'inventaire de leurs capacités, le président George Bush décida de

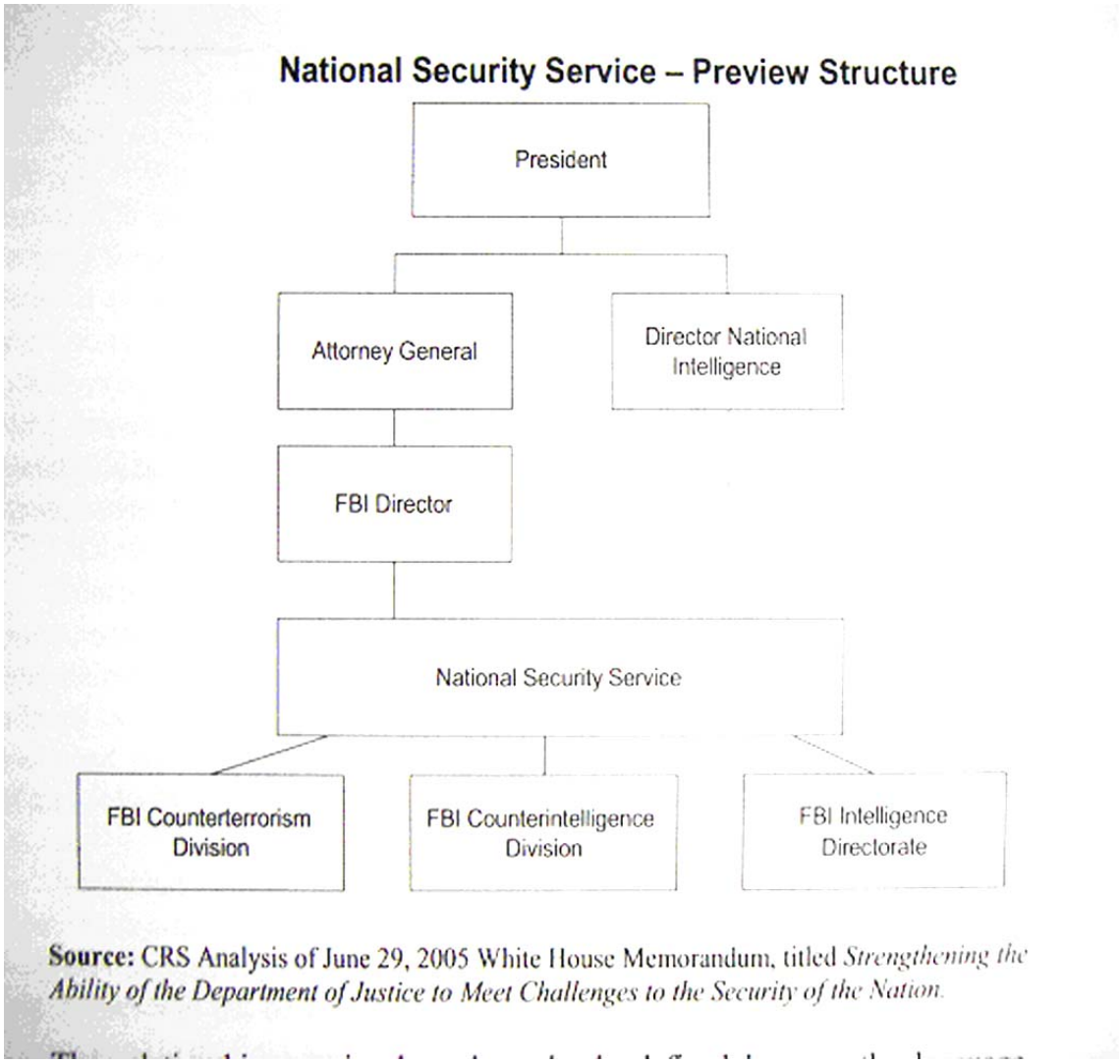
[17] "*Further strengthening Federal Bureau of Investigation Capabilities*", Memorandum for the Attorney General, Nov. 23, 2004.

coiffer d'une structure ad hoc les activités du FBI touchant les questions de sécurité nationale – le *National Security Service* (NSS).

> ⇨ **Principale innovation : le *National Security Service* répond à la fois au directeur du FBI et au directeur national du renseignement (DNI). Celui-ci a pour principale charge d'agréger le renseignement de sécurité intéressant la nation et produit par la *FBI Counterterrorism Division*, la *FBI Counterintelligence Division* et la *FBI Intelligence Directorate*.**

Via ce *National Security Service* rattaché au *Director of National Intelligence*, la Maison Blanche semble avoir atteint son objectif ultime pour la communauté du renseignement, consistant à amener toutes les structures à travailler sous une approche commune, et surtout à convaincre le FBI de renoncer à son exclusivité en termes de renseignement intérieur, et de partager sa production avec celle des autres agences sous l'égide du DNI, au nom d'une approche privilégiant un découpage entre renseignement défensif et offensif, et non plus entre renseignement intérieur et extérieur.

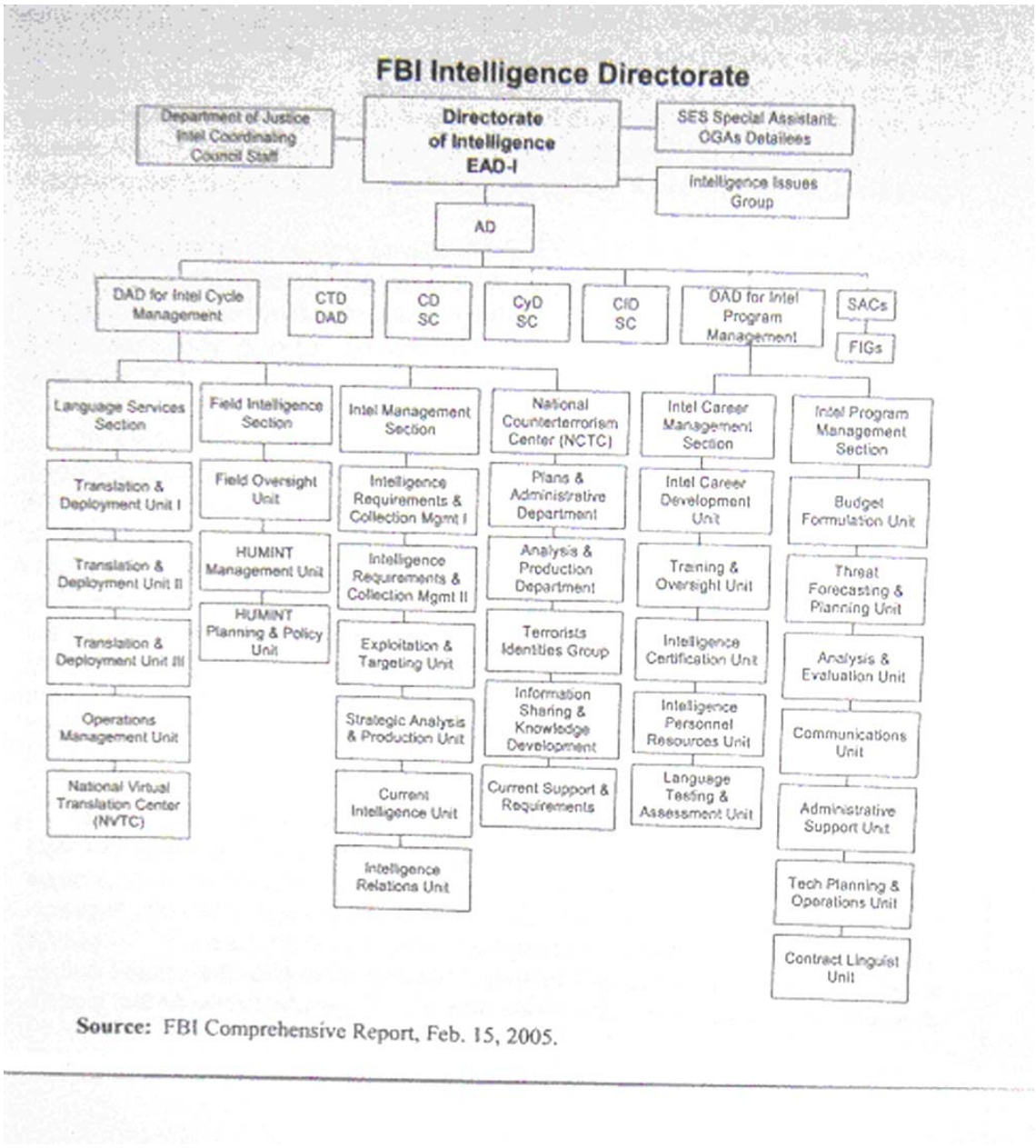
Fig. 4 : Le nouveau *National Security Service* dans l'administration du renseignement, tel qu'établie par la Maison Blanche du 29 juin 2005.



Source: CRS Analysis of June 29, 2005 White House Memorandum, titled *Strengthening the Ability of the Department of Justice to Meet Challenges to the Security of the Nation.*

Pilier de cette révolution culturelle, la *Directorate of Intelligence* (DI) du FBI a le mérite de reconnaître et de mieux tirer profit des compétences territoriales de l'agence, tout en plaçant l'exploitation de leur travail dans un cadre géographique décloisonné (avec les tutelles en cascade du *NSS* et du *DNI*). Sa situation dans l'organisation du renseignement à l'échelle fédérale permet d'optimiser la collecte de terrain, en formalisant les échanges auxquels ses fonctionnaires sont tenus. Officiellement, cette DI remplace l'*Office of Intelligence* (structure plus modeste autrefois placée auprès du directeur et chargée de coordonner la gestion du renseignement), en offrant des moyens étoffé. En réalité, elle représente une évolution majeure puisqu'elle puise sa raison d'être dans le travail de ses correspondants répartis dans l'ensemble des États, à travers les *Fiel Intelligence Groups*, lesquels ont été créés et placés en réseau en octobre 2003 seulement (autrefois, la circulation du renseignement de la base vers le sommet de l'agence n'obéissait à aucun formalisme). En termes de ressources humaines, sur le terrain, dans chacun des 56 bureaux hébergeant ces groupements, les analystes accèdent désormais au même statut et aux mêmes prérogatives que les « agents spéciaux » (responsables des investigations), garantissant théoriquement que leurs conclusions reçoivent la même attention.

Fig. 5 : L'organigramme de la *Directorate of Intelligence*, tel qu'établi par le bureau du directeur de l'agence, après qu'il ait évoqué pour la première fois en public l'existence de cette direction, le 3 juin 2004 au Congrès.



Source: FBI Comprehensive Report, Feb. 15, 2005.

b – La transformation du FBI et la fin d'un renseignement intérieur traité par des institutions spécifiques. L'organisation du « décloisonnement ».

« *C'est peut-être un analyste du FBI rattaché au bureau de San Francisco qui connaîtra le mieux le fonctionnement d'une cellule de militants islamistes d'origine jordanienne travaillant dans des restaurants de la côte Ouest. Mais c'est peut-être un agent de la CIA autrefois affecté à la division Moyen-Orient qui pourra immédiatement donner un sens à leurs contacts réguliers avec un imam du Caire auquel ils paraissent obéir. Et c'est peut-être le travail simultané de la NSA sur les communications de cet imam avec des correspondants au Pakistan, identifiés par la DIA, qui permettront d'anticiper la dangerosité de la cellule suivie par San Francisco* ». Ce scénario confié par l'assistant exécutif d'un sénateur habilité à suivre les débats à huis clos de la Commission des affaires de renseignement[18], illustre l'impératif de coopération de la communauté du renseignement que les responsables politiques ont tenté de codifier depuis la réforme du 12 décembre 2004. En termes de sécurité intérieure, elle supposait d'abaisser toutes les frontières administratives naguère dressées autour des finalités géographiques du renseignement (intérieur, extérieur).

Pour ce défi aussi, on observa le même phénomène que pour le traitement du terrorisme immédiatement après le 11 septembre. D'abord : des compromis administratifs se décident au nom de la survie des services de renseignement, puis des débats engageant le Congrès, les administrations concernés et la Maison Blanche préparent les évolutions conceptuelles et législatives, qui, le plus souvent, entérinent les premiers accommodements dictés par les nécessités d'aboutir à des résultats tangibles. Des processus éloquents quant aux forces de résistance des services de renseignement à toute politi-

[18] Rencontre avec l'auteur, août 2005.

que de changement en dehors des périodes de crise (et qui s'expriment également en Europe). C'est ainsi qu'au terme d'un accord longtemps demeuré secret, signé le 4 mars 2003, les services du département de la Justice, les agences de renseignement représentées par le DCI (c'est-à-dire le *Director of Central Intelligence*, cumulant cette fonction avec celle de patron de la CIA – avant la réforme de décembre 2004) et le nouveau *Department of Homeland Security* énonçaient les conditions d'une coopération totale, inédite dans l'histoire du renseignement américain.

⇨ **Intitulé "*Memorandum of Understanding between the intelligence community, federal law enforcement agencies and the department of homeland security concerning information sharing*"[19], c'est un document de 20 pages qui détermine juridiquement et organise matériellement le partage du renseignement. Pour plusieurs personnalités de la communauté du renseignement rencontrées à Washington, peut-être ce mémorandum est-il finalement l'acte fondateur « *d'une véritable communauté du renseignement* ».**

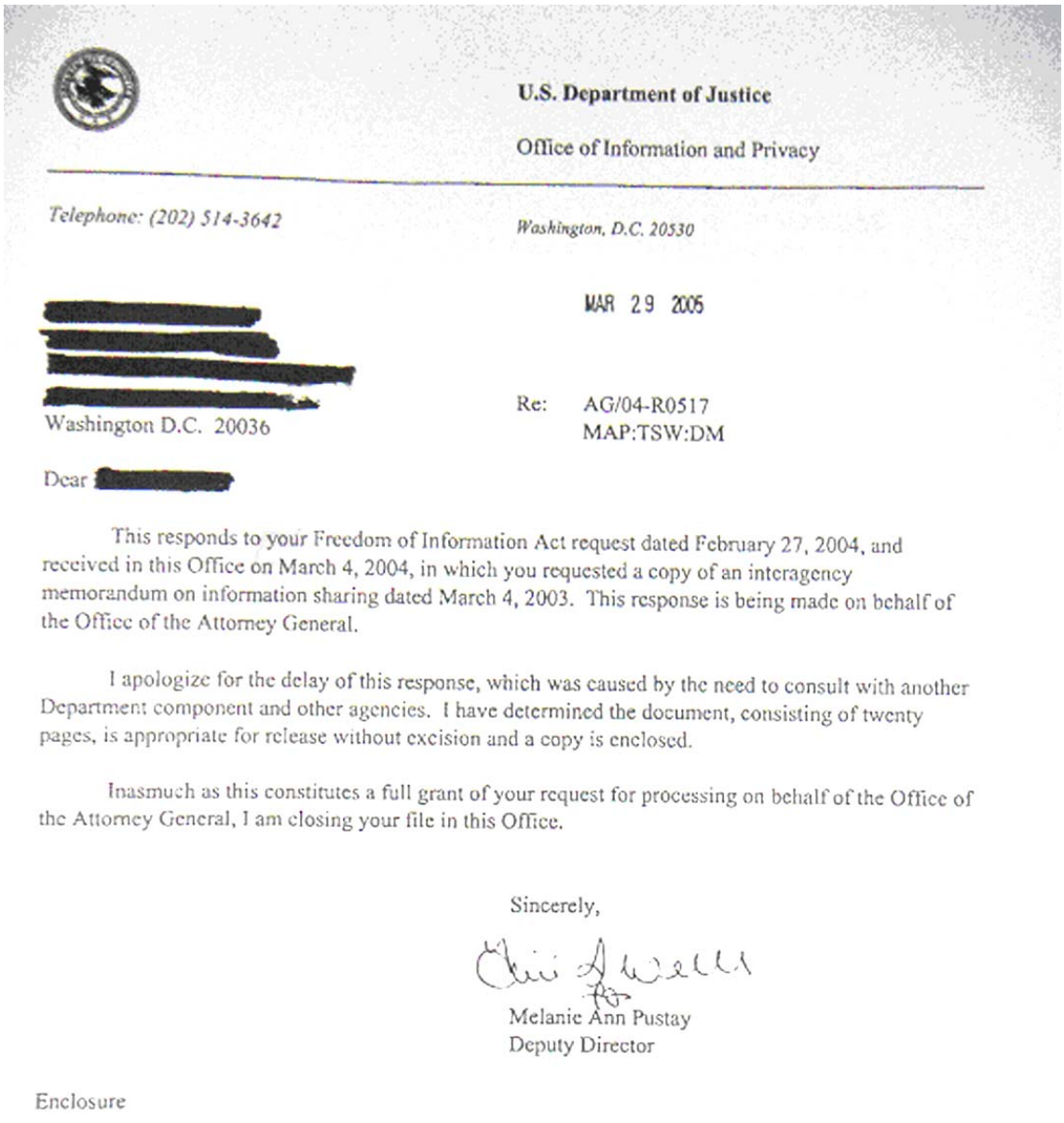
Naturellement, une telle concorde n'aurait pas été possible sans les transformations législatives fondamentales apportées par le *US Patriot Act*, voté par le Congrès au lendemain des attentats, le 26 octobre 2001. Au nom de la lutte antiterroriste, le texte autorise en effet pour la première fois les transmissions d'informations entre services de police judiciaire et services de renseignement. Fort de ces possibilités, le mémorandum de mars 2003 pose le principe que tous les renseignements portant sur des visées terroristes contre les Etats-Unis (quel que soit le service producteur) entre dans le cadre de l'obligation de partage affirmé par cet accord.

[19] Au terme d'une procédure au titre du *Freedom of Information Act* ouverte par un chercheur américain, le bureau de l'Information et des affaires privées du département de la Justice a reconnu l'existence de ce mémorandum, dans un courrier adressé à ce chercheur en date du 29 mars 2005. Vous trouverez, reproduit en annexe, une copie intégrale de ce document.

⇨ **La principale condition des échanges concerne le contenu du renseignement, et non pas l'état d'avancement de la production de ce renseignement. Pour l'essentiel, l'accord décrit ensuite les processus techniques d'échange des informations les plus sensibles, en prévoyant la protection des sources de chaque service.**

La volonté des principales personnalités du renseignement de souscrire à cet accord s'explique également par les problèmes de communication interservices soulevés par la simple émergence du *Department of Homeland Security.* En même temps que le mémorandum désigne les flux de renseignement susceptibles de nourrir les activités de cette nouvelle administration, subséquemment, elle en délimite également les compétences (alors que le législateur ne tranchera officiellement ces questions qu'un an plus tard). Ainsi, ces services de la sécurité intérieure sont désignés comme les receveurs des informations d'alertes ; manière de les cantonner à un rôle de gestionnaires des crises et des procédures de prévention antiterroriste (et non de recherche et de production). Ce confinement expliquera pour partie la disgrâce qui frappera le département pour son incurie à répondre aux dégâts provoqués par l'ouragan Katrina.

Fig. 6 : Extrait du *Memorandum of Understanding between the intelligence community, federal law enforcement agencies and the department of homeland security concerning information sharing*.



U.S. Department of Justice

Office of Information and Privacy

Telephone: (202) 514-3642

Washington, D.C. 20530

MAR 29 2005

[redacted]
Washington D.C. 20036

Re: AG/04-R0517
MAP:TSW:DM

Dear [redacted]

This responds to your Freedom of Information Act request dated February 27, 2004, and received in this Office on March 4, 2004, in which you requested a copy of an interagency memorandum on information sharing dated March 4, 2003. This response is being made on behalf of the Office of the Attorney General.

I apologize for the delay of this response, which was caused by the need to consult with another Department component and other agencies. I have determined the document, consisting of twenty pages, is appropriate for release without excision and a copy is enclosed.

Inasmuch as this constitutes a full grant of your request for processing on behalf of the Office of the Attorney General, I am closing your file in this Office.

Sincerely,

Melanie Ann Pustay
Deputy Director

Enclosure

Fig.6 suite…

information relating to groups or individuals reasonably believed to be assisting or associated with them.

(s) "Vulnerabilities information" means all information relating to the susceptibility -- actual, perceived, or conceptual -- of the United States, including any portion, sector, population, geographic area, or industry, to terrorist attack.

(t) "Weapons of Mass Destruction information" or "WMD information" means terrorism information or vulnerabilities information relating to conventional explosive weapons and non-conventional weapons capable of causing mass casualties and damage, including chemical or biological agents, radioactive or nuclear materials, and the means to deliver them.

3. Policies and Procedures for Information Sharing, Handling and Use. Consistent with the DHS Legislation, and except as otherwise specifically provided in this Agreement, the following agreed-upon policies and procedures shall apply to the provision of covered information by any covered entity to any other covered entity, to the interpretation of all provisions of this Agreement, and to the resolution of all issues related to information sharing, handling and use, and the coordination and deconfliction of operations and analytic conclusions:

(a) *Priority on Preemption, Prevention, and Disruption.* All procedures, guidelines, and mechanisms under this Agreement shall be designed and implemented, and all determinations with regard to sharing information covered by this Agreement shall be made, with the understood, overriding priority of preventing, preempting, and disrupting terrorist threats to our homeland. The parties recognize and agree that, in some cases, this priority shall dictate information sharing even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. Nonetheless, the covered entities shall act under this Agreement in a manner to protect, to the greatest extent possible, these other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information.

(b) *Reciprocity and Transparency.* All information collected by any covered entity relevant to the missions and responsibilities of any other covered entities should be shared, to the greatest extent possible, between and among all covered entities. Likewise, the parties agree that, to the greatest extent possible, there should be transparency between and among the covered entities with regard to their activities to preempt, prevent, and disrupt terrorist attacks against U.S. persons and interests. Except as otherwise specified in this Agreement, or mandated by relevant Federal statutes or Presidential Directives, procedures and mechanisms for information sharing, use, and handling shall be interpreted and implemented consistently and reciprocally regardless of the role a particular covered entity plays as a provider or recipient of covered information. In other words, for example, international terrorism information collected by the Border Patrol should be shared by DHS with the IC to the same extent foreign intelligence information on terrorism is shared by the IC with DHS.

4

Fig.6 suite…

(c) *Scope of "Covered Information."* Consistent with the priority established in Section 3(a), information relating to terrorism, Weapons of Mass Destruction, vulnerabilities, or other functions of the Department of Homeland Security shall be presumed to be "covered information" under this Agreement. If, after applying this presumption, disagreement remains between covered entities about whether particular information is "covered information," such disagreement shall be resolved pursuant to Section 4(d).

(d) *Effective date of information sharing obligations.* Notwithstanding provisions of this Agreement mandating further agreement on mechanisms, procedures, or other issues, the parties recognize that the obligation to promptly begin the full range of information sharing mandated by the DHS Legislation came into force on January 24, 2003, and that obligations under this Agreement will be in force upon the signature of all parties.

(e) *Sharing Requirements Based on Substance Only.* Consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, the parties agree that this Agreement requires that covered information, including, but not limited to, terrorism information, WMD information, infrastructure, and vulnerabilities information, be provided by any covered entity that collects or analyzes that information to any other covered entity that has a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity, regardless of:

(i) The type of communication in which the information is incorporated. Covered information must be provided as required in this Agreement regardless of the type of communication in which it is originally reported by the providing agency. The fact that particular covered information may be contained originally in a particular type of communication shall not, under any circumstances, be grounds either to withhold or delay the sharing of any covered information. As illustrative examples only, covered information must be provided by CIA, within the time frames agreed to, whether such information is contained originally in communications referred to as "TDs," "intel cables," "ops cables," or any other type of communication. Likewise, covered information must be provided by the FBI, within the time frames agreed to, whether such information is contained originally in communications referred to as "302s," "ECs," "LHMs," or any other type of communication;

(ii) The manner in which the information is or may be conveyed to the intended agency or individual recipients. Covered entities shall continually endeavor to improve technological means of access to afford maximum flexibility, speed, and volume of information shared, consistent with the strictly necessary protection of intelligence or sensitive law enforcement sources and methods, and with section 3(a) and other relevant provisions of this Agreement.

5

4 - Les déboires du Department of Homeland Security *et son cantonnement à des missions de diffusion.*

Officiellement fondé le 1er mars 2002, le *Department of Homeland Security* incarnait la réponse administrative la plus démonstrative aux attaques du 11 septembre. Avec pour principal objet de fédérer pas moins de 22 agences fédérales et locales en charge de la sécurité du territoire, son institution a représenté le plus grand remaniement dans l'administration fédérale des Etats-Unis des cinquante dernières années.

Ses pères fondateurs voulurent lui assigner un rôle dans la communauté du renseignement à la mesure de cette révolution bureaucratique. Et les dizaines de firmes de sécurité et de renseignement privé qui dès les premiers mois se sont imposés comme les conseillers des maîtres d'œuvre de cette transformation encouragèrent largement cette tendance. L'ancien gouverneur de Pennsylvanie Tom Ridge, premier technocrate chargé de concevoir le ministère à partir de l'ex bureau pour la *Homeland Security* de la Maison Blanche, fit assaut de diplomatie auprès de la CIA et du Pentagone pour que ses services soient adoubés par la communauté du renseignement. Quant à son successeur, Michael Chertoff, ancien procureur détaché auprès de la division des Affaires Criminelles du département de la Justice, il décida de doter le département d'un dispositif de renseignement propre, qui ne se contenterait plus de fusionner et d'analyser le renseignement d'alerte transmis par d'autres agences. C'est dans cette perspective que le 13 juillet 2005 il annonça la création d'un *Office of Intelligence & Analysis*, placé sous la tutelle d'un *Chief Intelligence Officer,* qui prendrait directement ses ordres auprès du secrétaire pour la Sécurité Intérieure (voir Fig.7 organigramme du DHS proposé par Chertoff en juillet 2005).

Toutefois, le scandale consécutif aux diverses incapacités du *Department of Homeland Security* à répondre de manière appropriée au désastre provoqué par l'ouragan Katrina – en particulier par l'entremise de sa structure chargée de la gestion des catastrophes naturelles, la *Federal Emergency Management Agency* (FEMA) – semble, à cette date, avoir définitivement sapé tout projet de développement de cette administration. Depuis l'aménagement de ses fonctionnaires dans des bureaux en Virginie et jusqu'au passage de Katrina, plusieurs prérogatives spécifiques lui ont été confiées ; mais elles portent davantage sur des missions d'alerte et de sécurité. Si bien que pour l'heure, et dans l'attente de connaître les conclusions des commissions parlementaires sur l'étendue des responsabilités dans la faillite des services d'urgence en Louisiane, il nous paraît assuré que le département ne se verra pas confié les nouvelles responsabilités que son ministre entendait recevoir en matière de renseignement en juillet dernier. Parmi les pouvoirs dont ils disposent à la suite d'intégrations de structures anciennes, on relève 5 entités ayant une implication en termes de sécurité du territoire :

- ⇨ **Le *National Infrastructure Protection Center* (NIPC), naguère conçu par le FBI et dévolu à la cyber-sécurité du territoire.**
- ⇨ **Le *Secret Service*, autrefois agence indépendante chargée de la sécurité de la Maison Blanche, du président et de diverses missions de polices judiciaires (contrefaçons…).**
- ⇨ **Le *US Coast Guard* chargé de la sécurité des eaux territoriales américaines et de la surveillance des frets maritimes.**
- ⇨ **La *Transportation Security Administration* chargée de la police aux frontières (contrôle des visas…).**
- ⇨ **Le *Customs and Border Protection Service*, responsable de toutes les activités de douane.**

Sur la problématique de la gestion des menaces terroristes, considérée comme centrale lors de la création du département, cette administration réussit là à centraliser la plupart des fonctions d'alertes à destination des populations et des administrations civiles (que la CIA et le FBI lui ont volontiers cédé), même si ces missions ne présentent pas de caractère stratégique dans les activités de contre-terrorisme et d'antiterrorisme. Dans ce registre, le département participe aux opérations de 4 structures de coordination : la *FBI Joint Terrorism Task Force* ; le *Terrorist Threat Integration Center* (TTIC) où les différents services partagent leurs conclusions quant à l'évolution des menaces ; le *Terrorist Screening Center* (TSC), servant à tenir à jour les listes de personnes à risques, notamment utilisés par les fonctionnaires chargés de la sécurité aux frontières) ; et le *National Targeting Center* (NTC), chargés de vérifier les listes de passagers et de marchandises en instance d'arrivée sur le sol américain. Les activités de la *FBI Joint Terrorism Task Force* s'avèrent les plus en prise avec des préoccupations opérationnelles ; auprès d'elle, le *Homeland Security Operations Center* remplit des fonctions de dissémination vers les divers échelons administratifs. La lecture des bulletins[20] qu'il produit confirment cette vocation du département à demeurer un vecteur de communication.

[20] Documents *for official use only*. Voir annexes.

Fig. 8 – L'organigramme du *Department of Homeland Security* encore en vigueur en juin 2005, et celui proposé par Michael Chertoff en juillet 2005 (page suivante).

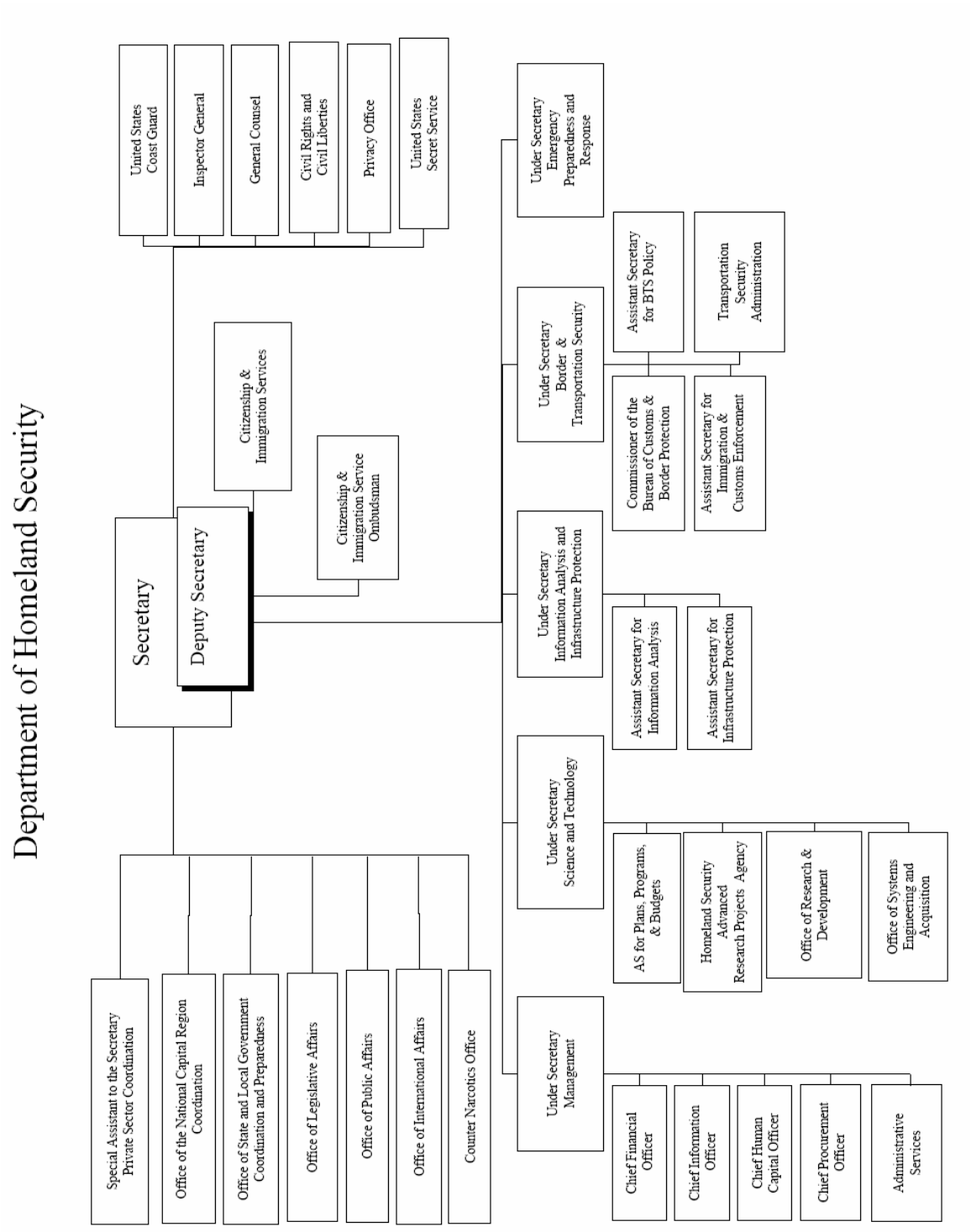
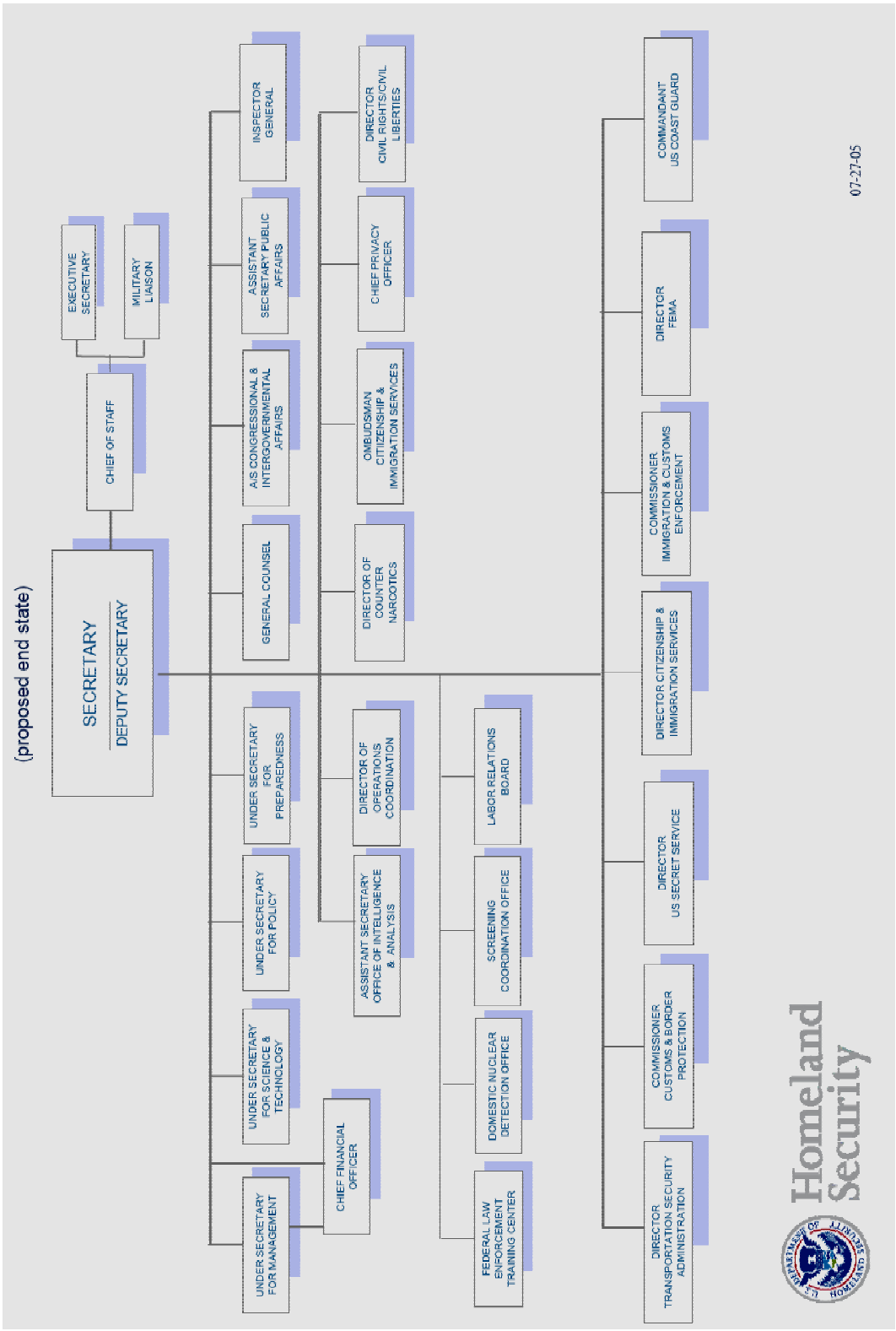


Fig. 8 Suite...


(proposed end state)
SECRETARY
DEPUTY SECRETARY
CHIEF OF STAFF
EXECUTIVE SECRETARY
MILITARY LIAISON
INSPECTOR GENERAL
ASSISTANT SECRETARY PUBLIC AFFAIRS
A/S CONGRESSIONAL & INTERGOVERNMENTAL AFFAIRS
GENERAL COUNSEL
DIRECTOR CIVIL RIGHTS/CIVIL LIBERTIES
CHIEF PRIVACY OFFICER
OMBUDSMAN CITIZENSHIP & IMMIGRATION SERVICES
DIRECTOR OF COUNTER NARCOTICS
UNDER SECRETARY FOR PREPAREDNESS
UNDER SECRETARY FOR POLICY
UNDER SECRETARY FOR SCIENCE & TECHNOLOGY
UNDER SECRETARY FOR MANAGEMENT
DIRECTOR OF OPERATIONS COORDINATION
ASSISTANT SECRETARY OFFICE OF INTELLIGENCE & ANALYSIS
CHIEF FINANCIAL OFFICER
LABOR RELATIONS BOARD
SCREENING COORDINATION OFFICE
DOMESTIC NUCLEAR DETECTION OFFICE
FEDERAL LAW ENFORCEMENT TRAINING CENTER
COMMANDANT US COAST GUARD
DIRECTOR FEMA
COMMISSIONER IMMIGRATION & CUSTOMS ENFORCEMENT
DIRECTOR CITIZENSHIP & IMMIGRATION SERVICES
DIRECTOR US SECRET SERVICE
COMMISSIONER CUSTOMS & BORDER PROTECTION
DIRECTOR TRANSPORTATION SECURITY ADMINISTRATION
07-27-05
Homeland Security

Après le désaveu politique essuyé par le département consécutif à la catastrophe de la Nouvelle-Orléans, il reste à identifier les ressources qu'il a captées ou qu'il a su développer et susceptibles d'intéresser le renseignement de sécurité. En ce domaine, il nous apparaît que le principal intérêt réside dans sa structure de recherche et développement, la *Homeland Security Advanced Research Project Agency* (HASPA), au travers des programmes scientifiques qu'elle finance et encadre. Parmi ceux-là, deux retiennent notre attention.

- ⇨ **Le projet *Enterprise Portal Program*. Il s'agit de concevoir un métasystème de gestion des connaissances. Avec un système informatique accessible à 1 million d'utilisateurs potentiels, qui centraliserait toutes les informations utiles au dépistage des terroristes et à la prévention de leurs actes. Un système autrement plus ambitieux que le bien connu *DHS Information Network.***
- ⇨ **Le projet *America Shield Initiative*. C'est un système d'intégration des différents moyens de surveillance déployés sur les frontières. Il vise à créer une plate-forme où convergent en temps réel les observations faites par satellites, drones, ou moyens infrarouges. Son développement associe le NORTHCOMMAND du Pentagone et matérialisera à terme les objectifs du département de la Défense en matière de *Homeland security policy.***

Fig. Exemples des productions du *Homeland Security Operations Center* réalisées en partenariat avec le FBI, et en direction de l'administration fédérale et des agences locales.

Information Bulletin
Title: Compressed Gas Cylinders as Components of IEDs
Date: September 10, 2004

Warning: This document is FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

This is a joint DHS and FBI Bulletin. Reference FBI Intelligence Bulletin No. 147.

Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS national threat level is YELLOW-ELEVATED. The current threat level for the financial services sectors in New York City, Northern New Jersey and Washington, DC is ORANGE-HIGH.

DHS and FBI encourage recipients of this Bulletin to report information concerning suspicious or criminal activity potentially related to terrorism to the local FBI Joint Terrorism Task Force (JTTF) – the FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm – and the Homeland Security Operations Center (HSOC). The HSOC can be reached via telephone at 202-282-8101 or by email at HSCenter@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the HSOC. The NICC can be reached via telephone at 202-282-9201 or via email at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact (POC).

ATTENTION: Federal Departments and Agencies, Homeland Security Advisors, State Emergency Managers, First Responders, Security Managers, and Information Sharing and Analysis Centers (ISACs).

(All agencies are authorized to pass this information to those who need it in the course of their official duties.)

OVERVIEW

Recent intelligence reporting indicates terrorists may be interested in devices using compressed, flammable gas cylinders to destroy buildings. However, these devices will not produce pressure waves equivalent to those from an explosive device. Instead, they tend to create large fireballs where most of the damage is a result of thermal (heat) effects. Damage and casualties resulting from such an event would not be as destructive

Information Bulletin
Title: Potential Threat to Homeland Using Heavy Transport Vehicles
Date: July 30, 2004

This is a joint DHS and FBI Information Bulletin.

DHS and FBI intend to update this Information Bulletin should they receive additional relevant information, including information provided to them by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is YELLOW-ELEVATED.

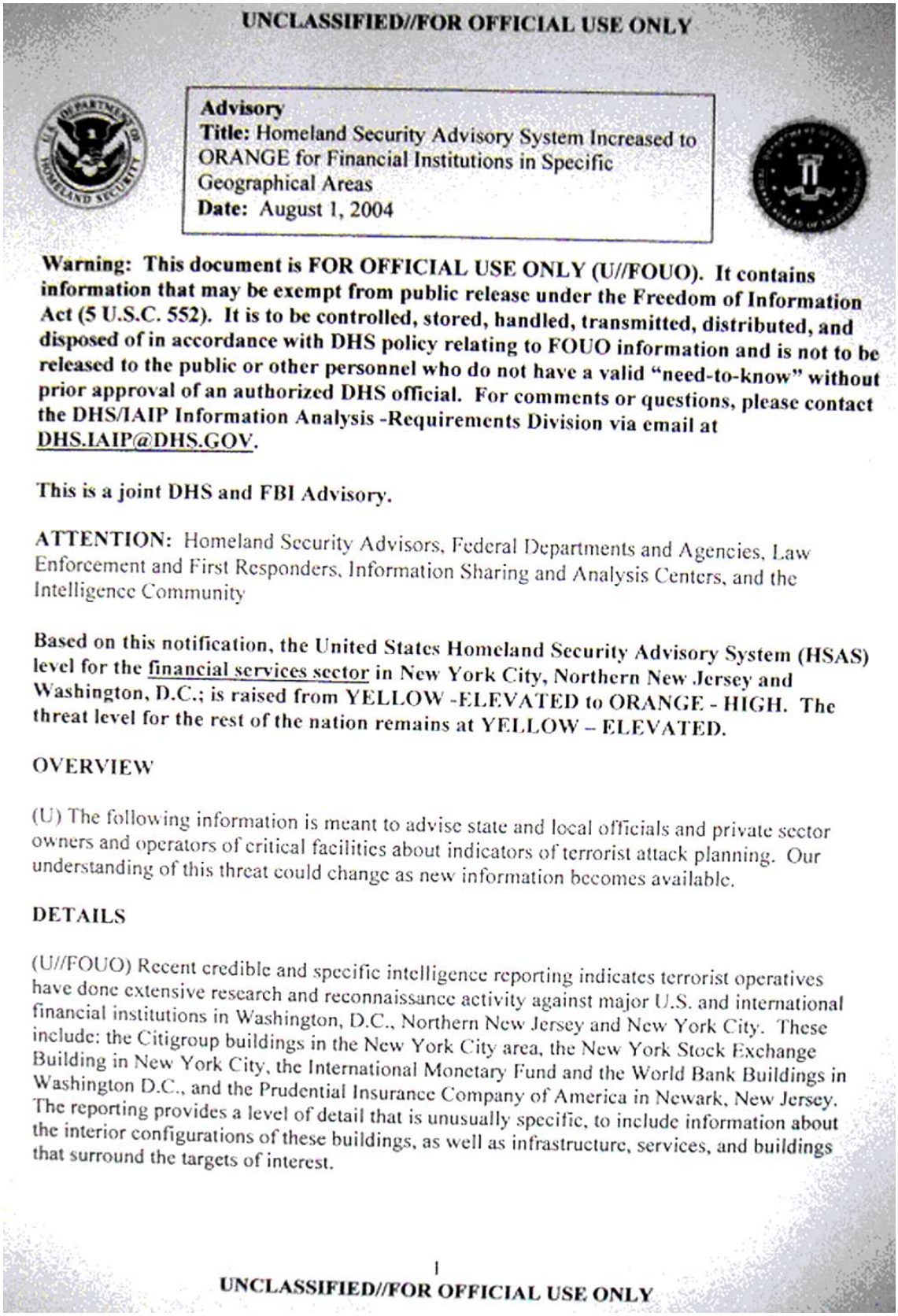
ATTENTION: State Homeland Security Advisors and Staff, Government Agencies, Information Sharing and Analysis Centers (ISACs), State Emergency Managers, Security Managers, and First Responders

OVERVIEW

This information bulletin is provided to sensitize state and local authorities and the private sector responsible for security of critical infrastructure and key resources to the potential for terrorists to use heavy transport vehicles as vehicle-borne improvised explosive devices (VBIEDs) against a range of attractive targets in the United States.

- Terrorists have repeatedly used heavy vehicles to conduct VBIED attacks in other countries as well as the United States.
- Some terrorist planners consider trucks to be one of the best tools to breach security measures and carry explosives since the U.S. airline industry significantly increased security procedures.
- Terrorist planners have considered how heavy vehicle drivers acquire training and Commercial Driver's Licenses (CDLs) with hazardous materials (HAZMAT) endorsement.
- Terrorists have shown an interest in planning attacks that employ quantities of HAZMAT that could be used as Weapons of Mass Effect (WME).
- There have been multiple suspicious incidents over the last six months that heighten concern over the potential terrorist acquisition of large trucks and commercial buses.
- VBIEDs can be used against symbolic icons and monuments or economic and infrastructure targets.

Page 1 of 7



UNCLASSIFIED//FOR OFFICIAL USE ONLY

Advisory
Title: Homeland Security Advisory System Increased to ORANGE for Financial Institutions in Specific Geographical Areas
Date: August 1, 2004

Warning: This document is FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. For comments or questions, please contact the DHS/IAIP Information Analysis -Requirements Division via email at DHS.IAIP@DHS.GOV.

This is a joint DHS and FBI Advisory.

ATTENTION: Homeland Security Advisors, Federal Departments and Agencies, Law Enforcement and First Responders, Information Sharing and Analysis Centers, and the Intelligence Community

Based on this notification, the United States Homeland Security Advisory System (HSAS) level for the financial services sector in New York City, Northern New Jersey and Washington, D.C.; is raised from YELLOW -ELEVATED to ORANGE - HIGH. The threat level for the rest of the nation remains at YELLOW – ELEVATED.

OVERVIEW

(U) The following information is meant to advise state and local officials and private sector owners and operators of critical facilities about indicators of terrorist attack planning. Our understanding of this threat could change as new information becomes available.

DETAILS

(U//FOUO) Recent credible and specific intelligence reporting indicates terrorist operatives have done extensive research and reconnaissance activity against major U.S. and international financial institutions in Washington, D.C., Northern New Jersey and New York City. These include: the Citigroup buildings in the New York City area, the New York Stock Exchange Building in New York City, the International Monetary Fund and the World Bank Buildings in Washington D.C., and the Prudential Insurance Company of America in Newark, New Jersey. The reporting provides a level of detail that is unusually specific, to include information about the interior configurations of these buildings, as well as infrastructure, services, and buildings that surround the targets of interest.

1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

II – Les évolutions conceptuelles qui sous-tendent les futures transformations des méthodes et des outils du renseignement de sécurité.

1- La fin des oppositions entre « sécurité extérieure » et « sécurité intérieure ».

a – Les bouleversements théoriques induits par le 11 septembre et leur prolongement pour les administrations en charge de la sécurité.

Le 11 septembre 2001 a redéfini la perception géographique des risques. Des chercheurs en ont rapidement pris conscience, comme Richard Kugler, professeur à l'Université nationale de Défense, à Washington, et conseiller de nombreux responsables de la sécurité et des forces armées. Selon lui : « *À l'origine, la mondialisation était considérée comme uniformément positive parce qu'elle offrait des possibilités de croissance économique et de démocratisation à toutes les régions du globe. Mais elle est vite apparue comme une hydre car elle met à rude épreuve des régions qui ne sont pas prêtes à entrer dans l'âge de l'information, de la modernisation et d'une forte concurrence sur les marchés mondiaux. La mondialisation produit un monde bipolaire* ». Et des frictions bipolaires d'un genre nouveau chambardaient la géopolitique du siècle débutant.

Avec la disparition des tensions entre l'Est et l'Ouest, ajoutée au mouvement de mondialisation des échanges et de dérégulation des marchés, la souveraineté des États s'est retrouvée véritablement amoindrie. Moins légitime, recourant plus rarement à la coercition, la puissance publique a partiellement abandonné à d'autres la faculté d'exercer le recours à la violence politique. Puisque les solidarités infranationales ne jouent plus (supplantées par des solidarités transna-

tionales), puisque les États perdent une partie de leurs prérogatives, alors des groupes sociaux peuvent s'agréger pour proposer ou imposer des modèles alternatifs, plus proches de leurs croyances et, surtout, plus appropriés aux instruments de captation de pouvoir qu'ils maîtrisent (cf. le recours au terrorisme pour les mouvements islamistes formés à l'action de guérilla en Afghanistan). En fin de compte, ils se comportent comme des entités politiques, recherchant des soutiens pour acquérir une autorité légitime, et n'hésitant pas à employer la force pour défendre le pouvoir de la communauté qu'ils incarnent. Les changements affectant les pratiques du terrorisme entre 1991 et 2001 en fournissent une traduction éloquente.

En l'espace de dix ans, le visage du terrorisme s'en est trouvé métamorphosé. Autrefois, il se pratiquait dans la plupart des cas avec le discret soutien d'un État, confiant ainsi à un autre acteur le soin de réaliser discrètement un acte de violence politique ; désormais, il dépend souvent de groupes non gouvernementaux, nullement associés à des États nations, mais davantage à des structures religieuses et financières transnationales, comme le montre l'organisation d'Al-Qaida (dont les commanditaires résident autant en Arabie Saoudite qu'au Qatar, au Koweït, à Sarjah, au Soudan et au Pakistan).

Ainsi, ce que les terroristes ont pulvérisé le 11 septembre 2001, au-delà des tours jumelles, c'est le bien-fondé de la stratégie de Washington fondée sur une grille de lecture commerciale de la géographie, participant aux affaires du monde au gré de ses intérêts de puissance économique – la doctrine *shaping the world* (façonner le monde, notamment sur un plan juridique et financier), énoncée sous la présidence Clinton dès 1997 – en la présentant comme la suite évidente de la doctrine de l'endiguement chère aux stratèges de l'après-guerre. En cela, la politique de l'équipe de George W. Bush est parfois moins en rupture avec celle de son prédécesseur que d'aucuns le croient. *Shaping the world*, c'était d'abord, à l'intérieur d'une planète globalement sûre, l'indispensable expansion américaine assurée

par la gouvernance d'un monde sans cesse rétréci grâce à l'ouverture des marchés, à moins de réglementations et grâce à de puissants réseaux de communication. Le 11 septembre, une frange radicale de la communauté musulmane exprime un refus contre cette construction du monde par les Etats-Unis et part en guerre contre la plus puissante nation pour imposer son propre dessein. Les pays industrialisés prennent acte qu'un fossé s'est creusé entre des communautés mondialement agrégées autour des valeurs les mieux véhiculées par la globalisation, et celles qui sont reléguées au rang de réseaux secondaires, dépendant pour l'essentiel de pouvoirs autoritaires (telles les communautés musulmanes traditionnelles du monde arabe).

Outre les opérations consécutives en Afghanistan, cette réintroduction de la violence politique dans la vie de l'État américain le conduit, progressivement, à abandonner la démarche consistant à façonner le monde par l'incitation, pour le faire par la force, au nom de sa propre sécurité intérieure puisque la globalisation l'a déjà placé au centre du monde entier.

La nouvelle *US National Security* de la Maison Blanche, publiée en septembre 2002, en prend acte. Depuis, sans remettre en cause la dérégulation économique, les Etats-Unis réintroduisent la violence politique, non plus comme *ultima ratio* de la politique étrangère, mais bien à titre préventif, pour entretenir un cordon sanitaire entre eux et les zones du monde refusant la mondialisation au profit de règles sociétales différentes. Dans le monde industrialisé, la Maison Blanche souhaite davantage dominer un enchaînement de leaders régionaux, c'est-à-dire d'États nations emboîtés, exerçant une influence prépondérante dans diverses zones du monde - d'où la vision d'un monde en poupées russes.

⇨ **Théoriquement : à l'extérieur du monde industrialisé, l'administration américaine applique le principe de la « souveraineté défaillante », et laisse intervenir le Pentagone en lieu et place de ses**

diplomates sitôt un danger identifié, avec les limites que l'on perçoit. L'intervention militaire en Irak se justifiait au nom de ce principe, porteur d'une révolution géostratégique, dont la finalité est de constituer de futures régions accueillantes qui intègreront la partie globalisée de la planète.

b - La théorie des *pre-emptions acts* implique d'accorder une place centrale au renseignement de sécurité dans le dispositif de défense.

Désormais, la stratégie de l'appareil militaire américain privilégie des attaques préventives pour neutraliser l'objet même des menaces. John Chipman, le directeur de l'Institut international d'études stratégiques de Londres, a analysé le premier l'impact de ces transformations, dans l'édition 2002-2003 de son annuaire de défense. Pour cet expert, les choix de l'administration Bush bouleversent avant tout la vocation même des armées. La mise en œuvre de la nouvelle stratégie commande d'abandonner l'architecture classique des forces entre des armées de terre, de l'air et de mer. Historiquement, cette typologie entre terre, mer et air obéissait à un impératif ; la défense du territoire national, assurée autour de la préservation de ses trois dimensions géographiques. Cette vision a vécu. Les priorités ont changé. La nouvelle organisation s'articule autour d'armées offensives et d'armées défensives[21], réalisant un découpage qui gomme cette absolue nécessité de sanctuariser l'espace national — touché au cœur le 11 septembre. Il assigne aux militaires deux fonctions : tout d'abord mener des opérations transnationales contre des organisations ou des dirigeants menaçants (les modalités de définition de la menace demeurant assez floues, comme le montre l'affaire irakienne) ; ensuite se prémunir contre toutes les formes d'attaque visant les intérêts américains (qui ne se déroulent pas obligatoirement sur le territoire national, à l'image des attaques informatiques).

[21] Le développement d'une *Homeland Defense Policy* traduit cette évolution.

2- L'appareil de renseignement du Pentagone et de la communauté du renseignement appelés à accroître leur pouvoir.

a – Les perspectives offertes par le prochain *QDR*..

Le 10 janvier 2005, le cabinet du secrétaire à la Défense diffusait auprès des états-majors un document de 40 pages classifiées « secret » et intitulé « *QDR terms of reference* », précisant les axes stratégiques du prochain plan quadriennal du Pentagone (*QDR*, pour *Quadriennal Defense Review*, dont la vocation est de cadrer les budgets du département au regard des nouvelles doctrine). Invitant les différents responsables à transmettre leurs projets et leurs besoins, il présentait le prochain plan quadriennal comme celui qui marquera véritablement l'entrée du Pentagone dans l'ère des guerres non conventionnelles. Les auteurs insistaient sur la nécessité d'imaginer un nouvel appareil de défense, dotés de systèmes d'armes plus souples et plus ouverts, intégrant les nécessaires coopérations avec des agences gouvernementales n'appartenant pas au département de la Défense. Sur ce point, ils citaient la CIA et l'US AID (!) comme des interlocuteurs incontournables pour remporter les conflits futurs. Aussi, les rédacteurs de ce « *QDR terms of reference* », demandaient-ils de développer des programmes qui répondent à quatre critères, renvoyant aux quatre nouvelles priorités stratégiques du secrétaire à la Défense :

- ⇨ **La neutralisation des réseaux terroristes.**
- ⇨ **La gestion des états-voyous détenteurs de l'arme nucléaire.**
- ⇨ **L'intégration des missions de homeland security.**
- ⇨ **La prévention des risques de guerre conventionnelle d'une puissante émergeante.**

Initialement prévu pour juillet 2005, le QDR devrait s'appliquer aux débats budgétaires de 2006 à 2011 et il concernera donc les exercices

2007 à 2012. Le secrétaire à la Défense Donald Rumsfeld a rencontré au cours des derniers mois les principaux chefs d'états-majors et commandant en chef pour entériner l'axe central du futur plan, le présentant à loisir comme le plus audacieux et le plus global jamais transmis au Congrès.

Matériellement, il fait la part belle à tous les systèmes d'armes dédiés aux guerres non conventionnelles, en particulier des dispositifs de capteurs à l'attention des unités de renseignement tactique, provoquant par ricochet des demandes de restrictions budgétaires sur plusieurs programmes aéronautiques conventionnels (en particulier le F/A-22 et le F-35). Tout en respectant les 4 priorités stratégiques énoncées plus haut, au fil des réunions, les cadres du ministère ont précisé leur vision. Dans l'espace géographique que nous connaissons, marqué par une atténuation des frontières et où la doctrine *shaping the world* n'est plus adpatée, les responsable de la Défense du pays doivent être en mesure de produire du renseignement sur des menaces par nature « irrégulière, catastrophique et perturbante », selon la future terminologie officielle.

⇨ **Dans des textes d'accès restreints, ces trois qualificatifs sont ainsi définis : « *Irregular threats are those designed to erode US power in unconventional ways. Catastrophic threats are attacks aimed at paralyzing the United States with surprise hits on symbolic and high-value targets. Disruptive threats could include highly advanced sensors, information technology, bio-technology, miniaturization on the molecular level and cyber operations* » .**

Conséquence de ces évolutions : à la Maison Blanche, au sein du Conseil national de sécurité, plusieurs cadres ont plaidé en faveur d'un inédit *Quadriennal Strategic Review* (QSR), tant les débats organisés par le Pentagone visent à intégrer de nombreuses administrations civiles aux activités de défense.

b – Le renseignement de sécurité en tant que mission de gestion des flux d'information.

Parallèlement à l'augmentation significative de son budget pour financer ses opérations extérieures, le Pentagone a parachevé au cours de l'automne 2002 la mise en application du concept de « domination par l'information » (traduit de la formule *Information Dominance*, qu'utilisent les responsables de la doctrine du département de la défense pour désigner ces programmes). La phase ultime a ainsi été atteinte lorsqu'au mois d'octobre de cette année, le Commandement spatial (US Space Command) a intégré le Commandement des forces stratégiques (US Strategic Command). Vu de l'extérieur, c'était un simple changement dans l'organigramme du Pentagone. Il représente en réalité l'acte ultime d'une transformation majeure, plaçant l'information au cœur du Commandement stratégique, au même titre que l'arsenal nucléaire durant les années 70 et 80.

⇨ **Depuis la fin des années 90, progressivement, le Commandement spatial a pris la direction de toutes les activités entrant dans le cadre de l'objectif de domination par l'information. Maintenant, il se présente comme la structure ayant intégré les activités de défense qui se déroulent dans les champs extra tellurique (cyberespace, espace atmosphérique et extra atmosphérique…).**

Sa mutation avait débuté par un premier regroupement inattendu au mois d'octobre 1999, lorsque le nouveau service responsable de la guerre numérique, le Groupe de travail sur les réseaux informatiques de défense, créé six mois plus tôt, avait intégré le Commandement spatial. A priori, deux mondes allaient se télescoper. En réalité : rien de tel. En fait, l'application de la doctrine de la domination par

l'information requiert en réalité des structures hiérarchiques bâties selon les modalités de collecte et de maîtrise de l'information. Or, l'espace extra atmosphérique, tout comme le cyberespace, sont dépourvus de biens matériels représentant un quelconque intérêt militaire. Il s'agit de deux espaces dont la gestion repose pour l'essentiel sur des valeurs numériques.

C'est donc dans le courant du mois d'octobre 2002, que l'état-major du Commandement spatial, dirigé par le général Ralph Eberhart, a pris très officiellement ses quartiers dans les bureaux du Commandement stratégique. Depuis 1998, l'application de la doctrine de « domination par l'information » a conduit les militaires à privilégier les investissements dans le domaine spatial et dans les réseaux informatiques. Les apports de la constellation GPS (géré par l'armée de l'air américaine en liaison avec le Commandement spatial, le GPS accorde des moyens de positionnement par liaisons satellite qui servent toutes les branches de l'armée), les nouvelles possibilités de communication et de renseignement par satellite, ont rapidement conféré au Commandement spatial le rôle de héraut de cette marche pour la conquête de l'information.
Avec le temps, puisque les planificateurs du Pentagone plaçaient la guerre de l'information au centre de leur stratégie, il semblait inévitable que cette organisation prenne le pas sur celles, conventionnelles des commandements de l'armée de l'air, de la marine et de l'armée de terre. L'avènement du Commandement spatial au cœur du Commandement stratégique. Fer de lance des forces nucléaires stratégiques (sous-marines, balistiques aériennes et intercontinentales terrestres), entre 1990 et 2001, à l'heure des conflits régionaux, le Commandement stratégique se contentait ces dernières années de gérer des stocks et de suivre la politique de désarmement. Le 11 septembre lui a assigné d'autres priorités, auxquelles ne pouvaient répondre des batteries de missiles nucléaires intercontinentaux, concentrées lorsque l'ennemi avait encore la forme d'un bloc d'Etats aisément identifiables.

La poursuite de ces transformations, postérieurement au 11 septembre nous enseigne peut-être que pour les systèmes de défense évoluant dans une société de l'information, la suprématie totale dans les moyens de renseignement s'avère finalement aussi essentielle que la maîtrise de l'atome dans une société bipolaire marquée par une opposition radicale.

Conclusion

Lors des échanges et des réflexions qui engagèrent cette étude, dans le courant du mois de juillet 2004, aux Etats-Unis, la nouvelle administration du Département de la sécurité intérieure paraissait à plusieurs égards développer des stratégies innovantes visant à mieux gérer le renseignement de sécurité intérieure. Mais *a posteriori*, et après une période de dix-huit mois ponctuée par une campagne présidentielle où de constants effets d'annonce sur les thématiques sécuritaires polluèrent souvent les observations que les acteurs européens menaient sur le concept d'*Homeland Security*, celui-ci se révèle d'une portée bien plus limité que celle déclamée. Dorénavant, nul ne songe à le définir autrement que comme un instrument politique visant à satisfaire les besoins de réformes exprimés par l'opinion publique après le 11 septembre, et dont *in fine* la principale créature administrative (*Department of Homeland Security*) se caractérise principalement par des activités de sécurité civile à l'échelle du territoire américain, pour lesquelles en outre elle a très cruellement apporté la preuve de son manque de capacité (cf. la tragédie de la Nouvelle Orléans lors du passage de l'ouragan Katrina).

Cependant, s'il nous appartient de ne pas être dupe de ces jeux politiques dévaluant la portée des réformes engagées, au-delà des problématiques de *Homeland Security*, les divers débats et réaménagements intervenus en filigrane dans l'organisation du renseignement aux Etats-Unis portent en eux plusieurs enseignements. Le premier d'entre tous concernent l'impérieuse nécessité de stimuler de véritables communautés du renseignement, capable coûte que coûte de travailler transversalement et de se montrer innovantes dans la fusion et la réalisation de leurs produits – une urgence due autant aux contingences de l'époque qu'au contexte sécuritaire lié aux activités terroristes. A ce titre, au regard de l'ensemble des services de renseignement

français, l'exemple nord-américain nous invite d'abord à privilégier le développement d'autorité de coordination tactique (au sein d'une même administration et au-dessus de plusieurs administration) ; c'est-à-dire à favoriser les démarches qui permettraient à une structure nouvelle ou réaménagée de contraindre les services par exemple en charge du suivi des phénomènes terroristes à coopérer malgré eux. Car les Etats-Unis de manière éloquente avant le 11 septembre, et les pays d'Europe de manière plus discrète jusqu'à présent, ont amplement démontré que la coopération des services de renseignement – fut-ce au nom du contreterrorisme – s'apparente à des stratégies d'influence, dans lesquelles les diverses administrations se contente d'entretenir pour les responsables politiques des croyances quant à leur fonctionnement coopératif, dans le seul but de proposer un écho fidèle à leurs discours publics. En France, dans le seul domaine de la lutte contre le terrorisme, le fonctionnement quotidien de l'UCLAT ainsi que les épisodes fratricides réguliers entre la SAT, la DST et la DGSE, démontrent – de manière hélas si magistrale – l'étendue de la nonchalance intellectuelle et morale qui peut seule conditionner les discours glorifiant une prétendue coopération entre des équipes se livrant depuis leur création respective à des oppositions de type politique afin de préserver leur pré carré auprès des décideurs ministériels. Lesquels, par ailleurs, faut-il le rappeler, ne semblent pas s'émouvoir que leurs concitoyens ne débattent des services de sécurité et de renseignement dont ils ont la charge que dans le cadre de problématiques fantasmatiques – de *Big Brother* à *James Bond*.

Dès à présent, grâce aux chantiers engagés par plusieurs commissions parlementaires et services de sécurité aux Etats-Unis, sur la seule problématique touchant le renseignement en matière de contreterrorisme, de nouvelles méthodes lourdes de conséquences prédominent. Il s'agit en particulier des diverses démarches pour fusionner des productions apparemment disparates, aboutissant à rapprocher le renseignement en matière de terrorisme avec le renseignement en matière de criminalité, de contrefaçon ou de trafic

d'armes. Cette approche tient compte d'observations effectuées à l'échelon opérationnel, où il apparaissait par exemple évident que la compréhension de réseau de contrefaçon permet d'identifier la construction de structures de financement cherchant offrir une assistance clandestine à une future cellule de militants islamistes, et bénéficiant éventuellement de l'assistance de sociétés fiduciaires implantées dans des paradis *offshore* – de tels constats ayant laminé la pertinence des typologies, voire des cloisonnements, naguère à l'œuvre dans les services américains, et qui demeurent en Europe.

Ces diverses remarques nous conduisent à formuler les propositions suivantes pour la Gendarmerie Nationale avec pour dessein la mise en place à moyen terme d'un Centre de production du renseignement de sécurité intérieure ; qui tirerait les conséquences de ces évolutions, au niveau de la Gendarmerie Nationale. Son développement pourrait être utilement précédé par la :

1. Création d'une Mission de simulation d'une exploitation du renseignement sur un mode coopératif au profit de la prévention du terrorisme et des activités criminelles. Sur des périodes passées, antérieures d'au moins deux ans et n'excédant pas six mois (par exemple janvier à mai 2003), cette mission est chargée de dresser l'inventaire des données opérationnelles produites par l'ensemble des services de la Gendarmerie Nationale sur la période concernée et dans les domaines suivants : contrefaçon, vols et trafics de véhicules, stupéfiants, fraudes aux moyens de paiement, vols. Les éléments sont agrégés et croisés dans une même base de données avec pour objectif la recherche systématique d'occurrences entre les données opérationnelles (patronymes, plaques numérologiques, cartes SIM…), et l'interprétation des dites occurrences. Grâce à la distance temporelle retenue, cette mission détermine si un tel travail ap-

porte une valeur ajoutée réelle dans la prévention d'activités menées par des organisations criminelles ou des organisations terroristes.

2. Création d'une Mission de consultation interne en direction des brigades de la Gendarmerie Nationale établie sur l'ensemble du territoire afin de déterminer dans quelles conditions, au sein de chaque brigade, pourrait être promu un Délégué à la coordination du renseignement. Il s'agirait là d'évaluer les exigences permettant de disposer dans chaque brigade d'un interlocuteur dédié, garantissant la valeur et la nomenclature des données destinées à être agrégées au niveau national.

3. Création d'une Mission de soutien sur les sources ouvertes chargée de proposer des solutions d'analyse systématique des bases de données privées internationales (juridiques, financières, légales…). Il s'agit de rechercher dans des références liées à l'étranger des occurrences éclairant celles relevées sur le territoire dans une démarche prospective.