UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LA SÉCURISATION DU CYBERTERRORISME AUX ÉTATS-UNIS

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN SCIENCE POLITIQUE

PAR

MATHIEU LABRIE

JANVIER 2011

TABLE DES MATIÈRES

RÉSUMÉ

Dans ce mémoire, nous avons entamé une réflexion exploratoire sur l'enjeu du cyberterrorisme aux États-Unis, car il y a peu d'étude sur le sujet et les quelques textes désiraient donner des conseils pratiques aux gouvernements. La seule exception est le texte de Myriam Cavelty (2007) qui s'intéressait à la sécurisation du cyberterrorisme par le gouvernement des États-Unis, mais ne traitait pas de la prépondérance des experts sur cette problématique. Croyant qu'ils ont eu une influence et qu'ils ont peut-être cherché à sécuriser cet enjeu, nous nous sommes posé la question suivante : Comment les experts de la sécurité tentent-ils de faire du cyberterrorisme un enjeu de sécurité aux États-Unis depuis la fin des années 1990 et quelles sont les variables qui influencent la réussite ou l'échec de ces tentatives?

Pour répondre à cette question, nous avons utilisé la même approche théorique que Cavelty, soit la théorie des cadres. Nous avons retenu trois cadres, le cadre diagnostique, pronostique et motivationnel, qui correspondent chacun à un chapitre de ce mémoire. Ensuite, en suivant une perspective temporelle, nous avons comparé chaque cadre des experts de la sécurité à celui du gouvernement afin de déterminer s'ils l'ont influencé. À l'aide de ces cadres, nous vérifierons notre hypothèse principale, qui est : « Les experts de la sécurité ont échoué dans leurs tentatives pour faire du cyberterrorisme un enjeu de sécurité aux États-Unis depuis la fin des années 1990 ».

Nos résultats sont que les experts de la sécurité n'ont pas réussi leur tentative de sécurisation. En fait, ils ne sont pas parvenus à imposer leur cadre diagnostique, car le gouvernement a ciblé les cybermenaces, et non le cyberterrorisme spécifiquement, comme l'ennemi. Aussi, le cadre pronostique et le cadre motivationnel des experts de la sécurité n'ont pas été bien établis parce qu'ils proposent les mêmes solutions que ceux du gouvernement. De plus, ce dernier avait déjà identifié cette menace et il avait entrepris des actions directes pour le contrer.

CYBERMENACES, CYBERTERRORISME, EXPERTS, INFRASTRUCTURES ESSENTIELLES, SÉCURISATION

INTRODUCTION

Les études sur le terrorisme englobent plusieurs sujets connexes. Ceux-ci comprennent notamment les gouvernements et leurs agences ou encore les groupes terroristes. D'un autre côté, les nouvelles technologies et leurs effets sont rarement analysés par les théories de la sécurisation[1]. Il ne faut pas s'étonner si le cyberterrorisme est peu étudié, car ce récent concept n'est guère connu en science politique. La majorité des écrits sur le sujet sont des conseils politiques. De plus, la totalité des textes s'intéresse essentiellement qu'aux gouvernements, et plus exactement à celui des États-Unis. Le rôle des experts de la sécurité sur ce sujet est inconnu.

Par ailleurs, le cyberterrorisme semble être devenu un enjeu prioritaire pour la sécurité nationale. Paradoxalement, nous n'avons qu'une vague idée du processus et des acteurs qui y ont contribué. Certains affirment que le 11 septembre 2001 est l'élément déclencheur de ce phénomène. Toutefois, certains documents s'intéressaient déjà à cette question avant cette date comme le National plan for information systems protection, version 1.0 : an invitation to a dialogue (États-Unis. White House, 2000).

Nous considérons qu'il est judicieux d'analyser l'impact des experts de la sécurité sur le processus de sécurisation de l'enjeu du cyberterrorisme, d'autant plus qu'il n'y a qu'une seule étude sur le sujet. Elle s'intéresse uniquement au gouvernement des États-Unis et elle néglige le rôle des experts de la sécurité non liés au gouvernement (Cavelty, 2007). Pour ces raisons, nous estimons que l'analyse du processus de sécurisation de l'enjeu du cyberterrorisme doit les intégrer. En effet, la théorie de la sécurisation, que nous expliciterons plus bas, stipule que les experts de la sécurité et la population peuvent, sous certaines conditions influencer les

[1] Nous utilisons la traduction de *Securitization* telle qu'employée par Jef Huysmans. 1998. « Dire et écrire la sécurité : le dilemme normatif des études de sécurité ». *Cultures & Conflits*, no 31-32, p. 177-202.

politiques gouvernementales. De plus, des indices nous laissent croire qu'il soit possible qu'ils aient tenté eux-mêmes un processus de sécurisation. Des experts, comme Winn Schwartau, nommé depuis plusieurs années consécutives comme une des personnalités les plus influentes en matière de sécurité, pourraient avoir eu une influence sur la rédaction de documents officiels sur le sujet (1994). Aussi, notre connaissance sur les variables qui influencent la réussite et l'échec dans une tentative de sécurisation est pauvre. Nous soutenons qu'il est capital d'appréhender comment et sous quelles conditions s'amorce un processus de sécurisation. En fait, les individus qui entament un processus de sécurisation sont appelés acteurs sécuritaires. Ils considèrent une situation spécifique comme une menace à leur existence. Alors, ils exigent que le gouvernement prenne des mesures qui passent outre les règles normalement établies. Il est alors intéressant de comprendre les raisons qui poussent ces individus à demander de telles mesures. Plus importants encore, comment réussissent-ils à convaincre les acteurs décisionnels ainsi que la population à accepter et légitimer ces mêmes actions. Dans cette optique, nous désirons découvrir les conditions qui facilitent ou diminuent les chances d'une sécurisation. Finalement, il est impossible pour un acteur sécuritaire de tout sécuriser, il doit faire un choix. Dans cette optique, la compréhension du processus de sécurisation nous permettra d'expliquer les raisons qui l'incitent à privilégier la sécurisation d'une situation par rapport à une autre. La connaissance des conditions d'émergence nous indiquera les circonstances plus susceptibles d'être sécurisées. En suivant cette logique, nous posons la question de recherche suivante :

Comment les experts de la sécurité tentent-ils de faire du cyberterrorisme un enjeu de sécurité aux États-Unis depuis la fin des années 1990 et quelles sont les variables qui influencent la réussite ou l'échec de ces tentatives?

Hypothèses

Notre hypothèse de recherche principale est la suivante : « Les experts de la sécurité ont échoué dans leurs tentatives pour faire du cyberterrorisme un enjeu de sécurité aux États-Unis depuis la fin des années 1990 ». Cette hypothèse est différente de celle de Cavelty dans la

mesure où elle s'intéresse aux tentatives de sécurisation de l'enjeu du cyberterrorisme par le gouvernement des États-Unis. Par conséquent, l'acteur étudié est différent.

Il est aussi important de préciser que notre espace géographique se limite aux États-Unis, parce que ce pays est le principal intéressé pour les questions de terrorisme et que la majeure partie des écrits provient d'auteurs états-uniens. Ces écrits sont du gouvernement des États-Unis et des experts de la sécurité. Pour cette raison, nous avons décidé d'étudier les experts de la sécurité des États-Unis. Nous nous concentrons sur la période de 1990 à aujourd'hui, car Internet apparaît et se propage durant cette période et nous ne pouvons pas parler de cyberterrorisme avant l'évènement d'Internet.

Cette hypothèse nous amène à formuler trois hypothèses secondaires. La première est la suivante : « Le cadre diagnostique a été bien établi par les experts de la sécurité, car ils ont réussi à cibler un ennemi, les cyberterroristes, et ce qu'ils menacent, les services essentiels des États-Unis ».

La seconde est la suivante : « Le cadre pronostique n'a pas été bien établi par les experts de la sécurité, car ils n'offrent pas de réelle solution contre la menace qu'ils ont désignée ».

La troisième est la suivante : « Le cadre motivationnel n'a pas été bien établi par les experts de la sécurité, car ils ne sont pas capables de rallier l'opinion publique contre la menace du cyberterrorisme, car celui-ci reste une menace théorique ».

Ces hypothèses secondaires sont pertinentes à notre étude, car elles permettront de confirmer ou d'infirmer notre hypothèse principale de recherche. Plus précisément, elles nous permettront d'évaluer chacun des trois éléments essentiels de la théorie du cadrage que nous utiliserons.

Opérationnalisation

Pour vérifier ces hypothèses, nous utiliserons la théorie du cadrage[2] comme la Cavelty (2007). Pour opérationnaliser notre cadre théorique, nous procéderons comme suit. Chaque chapitre de notre mémoire sera consacré à un des trois cadres, soit le cadre diagnostique, le cadre pronostique et le cadre motivationnel. Pour chacune de ces parties, nous suivrons chronologiquement l'évolution de ce cadre. Pour ce faire, nous commencerons par analyser les textes officiels et ensuite, nous ferons le même exercice pour les textes des experts de la sécurité. Ainsi, il nous sera possible de tracer un cadre du cyberterrorisme pour le groupe que constitue le gouvernement ainsi qu'un pour les experts de la sécurité. Nous allons pouvoir comparer ces cadres afin d'apercevoir leur similitude et leur divergence. Par la suite, nous devrons déterminer si le cadre des experts de la sécurité a influencé celui du gouvernement et s'il y a eu sécurisation, étant donné qu'une fois qu'un cadre est approuvé par un auditoire, il influe sur l'action des acteurs et en définit le sens pour le reste de la population (Cavelty, 2007). Il y a une possibilité d'une sécurisation si un cadre est accepté. Cette distinction est importante parce que si les acteurs décisionnels sécurisaient un enjeu sans l'appui de la majorité de la population, celle-ci ne légitimerait pas les actions hors-normes. Alors, la menace ne sera pas sécurisée, car les acteurs décisionnels n'auront plus la légitimité sur les mesures qu'ils ont prises. L'acceptation du cadre par les acteurs décisionnels et le reste de la population est un critère qui guidera notre démarche.

Avant de passer au second critère, il est important de spécifier comment nous déterminons qu'un auditoire accepte, ou non, un cadre. Nous utiliserons des sondages états-uniens en lien avec le cyberterrterrorisme. Toutefois, nous reconnaissons une limite à notre recherche en cet aspect. Les sondages sur le cyberterrorisme sont très rares et nous n'avons pas beaucoup de données. Néanmoins, l'utilisation de sondages n'est pas toujours impérative. En effet, lorsque nous déterminons que les experts de la sécurité n'ont pas influencé le

[2] Nous tenons à faire remarquer au lecteur que la *Théorie du cadrage* a plusieurs synonymes. Plus exactement, nous pourrions le remplacer par le terme de *Théorie des perspectives*, par celui de *Théorie des cadres de l'expérience* ou par celui de *Théorie de l'encadrage*. Pour des fins de simplifications, nous avons décidé d'utiliser l'expression *Théorie du cadrage*.

gouvernement, il n'est pas nécessaire de connaître l'opinion du public états-unien, car ils auraient échoué dans leur tentative de sécurisation.

Le second critère est temporel et permet de déterminer si les experts de la sécurité ont influencé un des cadres. Nous considérons que le cadre présenté par les experts de la sécurité doit être créé avant celui des acteurs décisionnels. En fait, si le gouvernement a préalablement mis au point des cadres sur le sujet antérieurement des experts de la sécurité, il se trouve peut-être que ce sont ces derniers qui sont influencés. Dans ce cas, les experts de la sécurité ne pourraient tenter de sécurisation, car elle serait déjà amorcée par les acteurs décisionnels. Il apparait envisageable que les experts de la sécurité et les acteurs décisionnels aient développé des cadres dans le même espace de temps. Alors, il est possible que les experts de la sécurité influencent les résultats des cadres utilisés par les acteurs décisionnels. Dans cette situation, les experts de la sécurité pourraient tenter une sécurisation d'un enjeu. Il est primordial de suivre l'évolution de ces cadres afin de déterminer si les experts de la sécurité ont été en mesure d'influencer les cadres retenus par les acteurs décisionnels.

Finalement, le dernier critère est que le cadre élaboré par les experts de la sécurité soit identique ou très semblable à celui des acteurs décisionnels. Nous ne pourrons parler de sécurisation réussie des experts de la sécurité si leur cadre diffère de celui des acteurs décisionnels, car celui-ci ne serait pas parvenu à être accepté comme cadre principal.

Précision sur la méthodologie

En ce qui concerne la méthodologie, notre question de recherche est de type exploratoire en raison de sa nouveauté et du faible nombre d'études effectuées sur le cyberterrorisme. Nous utiliserons l'analyse documentaire comme stratégie de preuve parce qu'elle permet de mieux prendre en considération un phénomène qui se porte difficilement aux études statistiques comme la sécurisation (Roy, 2003).

Afin d'obtenir une description en profondeur de notre corpus documentaire, nous emploierons l'analyse de discours. Nous allons interpréter les documents sélectionnés en tentant de faire ressortir la position ainsi que la vision de l'auteur par rapport à la problématique au moment de son l'écriture. Pour y arriver, nous allons analyser les idées principales et la signification des métaphores et du vocabulaire. Nous définissons le concept de métaphore par un : « Procédé de langage qui consiste à employer un terme concret dans un contexte abstrait par substitution analogique, sans qu'il ait d'élément introduisant formellement une comparaison. » (Société Dictionnaire le Robert, 2009, p.1584). Spécifiquement, nous nous intéresserons aux métaphores du « corps ». Aussi, nous analyserons le vocabulaire se référant à l'incertitude de la situation ou de la menace dont les États-Unis sont confrontés. Finalement, nous nous pencherons sur le vocabulaire qui renvoie à l'idée que les États-Unis sont entrés dans une nouvelle période. Nous expliquerons ce choix à la section 1.1.

Ensuite, la théorie du cadrage permet, à l'aide des cadres, de classifier les positions et les perceptions des auteurs par rapport à divers aspects de la problématique. Dans ces conditions, nous pouvons déterminer l'évolution des positions des auteurs dans le temps, en examinant les cadres et en notant les points de convergences et de divergences. Pour nous aider dans cette tâche, nous avons soumis notre corpus documentaire à une même liste de questions analytique. Voici cette liste :

- Quel est le but ou l'objectif du texte?
- À qui s'adresse-t-il?
- Quelle est la problématique? Quelle est sa cause?
- Quelles sont la ou les solutions envisagées?
- Demande-t-on la participation du public pour enrayer la problématique? Si oui, que propose-t-on?
- L'auteur utilise-t-il des métaphores ou des images pour illustrer certains propos en lien avec les trois questions précédentes? Si c'est le cas, quelles sont-elles?

- Mentionne-t-on d'autres auteurs ou textes qui auraient influencé l'écriture du document analysé?
- En général, comment le texte considère-t-il le cyberterrorisme? Tente-t-on de faire du cyberterrorisme un enjeu de sécurité?

Cette stratégie nous permettra d'étudier les divers cadres élaborés par les experts de la sécurité. Nous avons sélectionné des textes d'experts de la sécurité différents pour pouvoir déterminer si leurs cadres sont semblables. La période qui nous intéresse est celle du début des années 1990 à aujourd'hui, car Internet et le concept de cyberterrorisme font leurs apparitions à cette époque. Il est à noter que nous analyserons des textes écrits à différents moments de la période étudiés, car la séparation de la période étudiée en plusieurs segments permet d'observer l'évolution du cyberterrorisme et de sa sécurisation. De plus, cette triangulation des données nous permet de combler les lacunes ou les biais de nos sources d'informations (Ibid.).

Afin de déterminer si les experts de la sécurité ont réussi dans leurs tentatives de faire du cyberterrorisme un enjeu de sécurité, nous tenterons de vérifier s'ils ont influencé la rédaction de déclarations officielles des États-Unis. Nous utiliserons cette procédure de validation de notre démonstration pour plusieurs raisons.

En effet, nous analyserons les textes des experts de la sécurité dans une perspective historique afin de nous assurer qu'ils ont eu une influence sur les décisions en matière de cyberterrorisme. Plus précisément, nous allons étudier ces textes dans un point de vue temporel aux déclarations officielles du gouvernement des États-Unis. Cette étape permet de s'assurer que c'est bien les experts de la sécurité qui influencent les choix du gouvernement états-unien en matière de cyberterrorisme. Par conséquent, si nous retrouvons les cadres des experts de la sécurité dans les documents officiels du gouvernement états-unien à priori des textes des experts de la sécurité, il nous sera difficile d'établir leur influence sur les politiques touchant le cyberterrorisme. Finalement, nous procéderons cadre par cadre afin de déterminer l'efficacité de chacun.

Les textes gouvernementaux principaux que nous étudierons proviendront du *Department of Homeland Security*, du *Government Accounting Office* et les *Executive Orders* du Président des États-Unis. Aussi, nous analyserons le *President's Commission on Critical Infrastructures Protection* (PCCIP), car elle est la première étude du gouvernement des États-Unis à dépeindre les cybermenaces comme un enjeu de sécurité (1997). Enfin, elle établit la protection des infrastructures essentielles comme une priorité sécuritaire aux États-Unis et dans d'autres pays (Albele-Wigert et Cavelty, 2006).

Les textes analysés ont été écrits par des experts de la sécurité. Plus spécifiquement, nous avons sélectionné les textes d'experts de la sécurité qui s'intéresse à l'aspect politique de l'enjeu du cyberterrorisme. Ainsi, nous ne nous penchons pas sur le vaste corpus documentaire dédié à la sécurité informatique, car il s'agit de texte technique en science informatique destinée à un public précis et restreint d'administrateurs de réseaux et de programmeurs, car ils se préoccupent peu de l'aspect politique du cyberterrorisme. Une fois cette présélection achevée, nous avons conservé les textes écrits par les experts de la sécurité les plus reconnus. Nous explicitons davantage le concept d'expert retenu dans ce mémoire à la section 1.2.

Nous préférons les monographies parce qu'ils sont plus accessibles au grand public. Toutefois, nous utiliserons également des articles scientifiques et des comptes-rendus de conférence d'experts de la sécurité, car le nombre de monographies à notre disposition, en appliquant notre définition d'expert de la sécurité, est très restreint. Ainsi, ils permettront d'enrichir notre analyse.

Aussi, notre sélection ne s'arrête pas seulement sur les textes dénonçant la menace du cyberterrorisme. En effet, nous emploierons des textes d'experts de la sécurité qui minimisent la menace du cyberterrorisme ou qui ne souhaitent pas nécessairement en faire un enjeu de sécurité. Ce choix est justifié par le dilemme normatif de sécurité développé par Jeff Huysman.

Le dilemme se résume ainsi : en s'intéressant à un enjeu sécuritaire et en parlant, le chercheur utilisant une perspective constructivisme risque de contribuer à sa sécurisation. Le risque est aussi présent s'il tente de désécuriser l'enjeu. Dans cette optique, le chercheur peut alarmer son auditoire sur une problématique précise alors qu'il désirait dénoncer le caractère dangereux de cette problématique. Ainsi, au lieu de banaliser une situation, il peut lui donner un caractère prioritaire et menaçant. Le chercheur accomplit le contraire de ce qu'il voulait. (Huysmans, 1998). Donc, tout expert de la sécurité traitant de cyberterrorisme peut avoir un impact sur les éléments constituant les différents cadrages.

Une fois cette présélection terminée, nous avons conservé les textes d'experts de la sécurité les plus reconnus sur la question du cyberterrorisme pour deux raisons. Premièrement, leurs textes sont les plus diffusés et ont probablement un impact plus important que les autres. Deuxièmement, le seul fait d'être les plus reconnus dans ce domaine leur confère une certaine crédibilité et une légitimité pour examiner l'enjeu du cyberterrorisme.

Plan du mémoire

Ce mémoire est structuré en quatre chapitres. Le premier chapitre présente le cadre théorique et les concepts utilisés. Pour commencer, nous introduisons la théorie de la sécurisation. Par la suite, nous définirons le concept d'expert de la sécurité, d'infrastructures essentielles et de cyberterrorisme.

Le deuxième chapitre établit l'influence des experts de la sécurité sur le cadre diagnostique du cyberterrorisme. Pour commencer, nous ferons ressortir le cadre du gouvernement. Ensuite, nous regardons l'impact des experts de la sécurité sur ce cadre afin de déterminer s'ils l'ont influencé. Finalement, il nous sera possible de vérifier notre première hypothèse secondaire de recherche qui est la suivante : « le cadre diagnostique a été

bien établi par les experts de la sécurité, car ils ont réussi à cibler un ennemi, les cyberterroristes, et ce qu'ils menacent, les services essentiels des États-Unis ».

Le troisième chapitre analyse l'influence des experts de la sécurité sur le cadre pronostique du cyberterrorisme. Pour y parvenir, nous déterminerons les éléments du cadre du gouvernement. Par la suite, nous observerons si les experts de la sécurité l'ont influencé. Finalement, nous testerons notre deuxième hypothèse secondaire de recherche qui est la suivante : « le cadre pronostique n'a pas été bien établi par les experts de la sécurité, car ils n'offrent pas de réelle solution contre la menace qu'ils ont désignée ».

Le quatrième chapitre établira l'influence des experts de la sécurité sur le cadre motivationnel du cyberterrorisme. Pour ce faire, nous ferons ressortir le cadre du gouvernement. Après, nous analyserons l'impact des experts de la sécurité sur ce cadre afin de déterminer s'ils l'ont influencé. Ensuite, il nous sera possible de vérifier notre troisième hypothèse secondaire de recherche qui est la suivante : « le cadre motivationnel n'a pas été bien établi par les experts de la sécurité, car ils ne sont pas capables de rallier l'opinion publique contre la menace du cyberterrorisme, car celui-ci reste une menace théorique ».

En conclusion, nous allons vérifier notre hypothèse principale qui est la suivante : « Les experts de la sécurité ont échoué dans leurs tentatives pour faire du cyberterrorisme un enjeu de sécurité aux États-Unis depuis la fin des années 1990 » avec les résultats obtenus de nos trois hypothèses secondaires. Finalement, nous conviendrons des raisons qui permettent d'expliquer ces résultats.

CHAPITRE I

THÉORIES ET CONCEPTS

Dans ce chapitre, nous allons détailler notre cadre théorique et les concepts utilisés. Dans un premier temps, nous discuterons de la théorie de la sécurisation. Par la suite, nous aborderons la théorie du cadrage. Finalement, nous énoncerons et définirons les concepts employés.

1.1 Le cadre théorique

Nous allons expliciter le cadre théorique que nous utiliserons. Nous avons retenu celui du cadrage tel qu'élaboré par Cavelty (2007). Celui-ci est basé en partie sur la théorie de la sécurisation élaborée par l'école de Copenhague, et plus exactement par Ole Waever. Nous amorcerons alors par un exposé de la théorie de la sécurisation. Par la suite, nous enchaînerons avec la théorie du cadrage.

Il existe trois écoles qui traitent de la sécurisation. L'École de Copenhague s'intéresse à la construction politique d'une menace; l'École de Paris permet d'étudier les relations de pouvoir entre les différents acteurs d'une agence et des agences entre elles lors du processus de sécurisation d'un enjeu; et l'École d'Aberystwyth s'interroge sur la sécurisation d'objet et la perception des menaces sur un espace temporel précis (Waever, 2004). Nous restreignons

notre choix à l'école de Copenhague même si l'École de Paris semble bien adaptée à notre problématique. En effet, l'École de Paris est inspirée par la sociologie notamment de Bourdieu et l'œuvre de Foucault. Elle examine empiriquement les pratiques sociales des agences. Ces examens révèlent souvent des processus et des structures d'actions différents que ceux que l'on retrouve dans les documents officiels. Or, nous ne désirons pas, dans ce mémoire, nous examiner les pratiques sociales des individus dans les agences ou celles entre les agences. Nous désirons observer comment des individus, les experts de la sécurité, qui ne font pas nécessairement partie d'agences, tentent une sécurisation de l'enjeu du cyberterrorisme. Pour atteindre notre objectif, l'École de Copenhague correspond mieux à nos besoins. En effet, cette école analyse le processus politique de la construction d'une menace. Pour ce faire, elle utilise le concept d'acte de langage et le concept de processus de sécurisation. Ce processus de sécurisation est composé de trois éléments interreliés. Premièrement, il tente de démontrer qu'une situation précise est une menace existentielle pour l'État et ses citoyens. Deuxièmement, il propose des solutions pour contrer la menace. Troisièmement, le processus recherche l'appui de la collectivité et sa mobilisation pour lutter contre la menace. Ces trois éléments du processus de sécurisation correspondent aux trois cadres d'analyses élaborés par Cavelty soit le cadre diagnostique, pronostique et motivationnel. Ces derniers correspondent chacun à un des trois chapitres d'analyse de ce mémoire. Dans cette optique, l'utilisation de l'École de Copenhague nous semble plus appropriée que celle de Paris (Waever, 2004).

Il est possible de définir la sécurisation comme une tentative, d'un acteur ou d'un groupe d'acteurs, de transformer une situation non urgente en une situation d'urgence. Celle-ci justifie l'entrave aux règles et normes établies par son caractère d'urgence. Buzan, Waever et Jaap de Wilde le définissent comme : « [...] the move that takes politics beyond the established role of the game and frames the issues either as a special kind of politics or as above politics » (1998, p. 23). En d'autres termes, une tentative de sécurisation est l'identification d'une problématique par un acteur. Ce dernier le conçoit comme une menace à sa survie et qui doit être résolue prioritairement. Ainsi, l'enjeu n'est plus seulement politique, l'acteur sécuritaire souhaite une intervention rapide des autorités. Alors, il tente de les convaincre de la nécessité de passer outre les protocoles établis sans qu'il y ait un débat

public sur les mesures prises. L'acteur essaie de démontrer que la situation présente, qu'elle soit de nature politique ou non, constitue une menace existentielle pour la survie de l'État.

Ce changement de priorité ne se fait pas seul. Le négociateur, l'individu qui entreprend la sécurisation d'un enjeu, doit négocier ce changement de situation avec son auditoire. Nous le définissons comme l'ensemble des individus que le négociateur tente de convaincre. Dans le cadre de ce travail, l'auditoire est la totalité de la population des États-Unis. Pour ce faire, le négociateur emploie l'acte de langage. Cela consiste à utiliser son discours pour influencer la perception de la situation. Toutefois, l'acte de langage est plus que cela. En effet, un problème de sécurité le devient que lorsqu'un acteur énonce un acte de langage. Donc, il le devient que lorsqu'on le nomme ainsi. Comme le souligne Ayse Ceyhan « [...] le mot ¨sécurité¨ n'est pas intéressant comme signe se référent à un objet concret qui existe déjà, mais c'est son énonciation qui constitue l'acte. » (1998). Aussi, l'acte de langage ne s'intéresse pas aux vrais ou aux faux. Ce qui importe est l'effet immédiat que le discours a sur l'auditoire. Afin d'être plus convaincant, l'acte de langage va utiliser un langage symbolique, imagé et métaphorique. Les termes utilisés sont choisis en fonction des caractéristiques socio-culturelles et des images populaires qui sont propres à un auditoire. Ainsi, il est possible pour l'acteur sécuritaire de choisir des images, des symboles et des métaphores qui vont influencer, négativement ou positivement, la perception de l'auditoire au sujet d'une problématique (Ibid.). Hayden White exprime bien ce propos lorsqu'il écrit des métaphores : « [...] *tells us* what images to look for in our culturally encoded experience in order to determine how we *should feel* about the thing represented. » (Campbell, 1998, p. 87).

Dans ce mémoire, nous allons tenter d'examiner les métaphores sur le thème du « corps ». David Campbell affirme que les acteurs sécuritaires, notamment le gouvernement des États-Unis, utilisent la dichotomie du « corps sain » versus le « corps malade » pour souligner l'urgence d'une situation. Ainsi, le « corps sain » équivaut à la santé et à la propreté ce qui représente une logique de stabilité. Pour sa part, le « corps malade » renvoie à l'image de la maladie et de l'insalubre ce qui évoque le désordre (Ibid.).

Nous allons aussi nous attarder sur l'utilisation de deux thèmes de vocabulaire ainsi que sur l'utilisation d'évènement historique pour qualifier le cyberterrorisme. Le premier thème de vocabulaire réfère à l'incertitude de la situation ou de la menace que pourraient faire face les États-Unis. Par exemple, pour celui évoquant l'incertitude, nous essayerons de trouver des mots tels que, *could*, *capability* et *possibility*. Il est très important que ces mots servent à imager ou symboliser la menace du cyberterrorisme. Il nous semble judicieux d'analyser ce thème de vocabulaire, car Ralph Bendrath remarque la grande quantité de mots exprimant l'incertitude utilisée dans le débat sur la protection des infrastructures essentielles aux États-Unis (2001).

Le deuxième thème de vocabulaire renvoie à l'idée que les États-Unis sont entrés dans une nouvelle période. Pour ce thème, nous tenterons de trouver des mots comme *new period*, *new era*, *new age* et *Post-Cold War*. Dans cette optique, les États-Unis seraient maintenant dans une nouvelle période qui est différente de la précédente. Cela implique qu'ils font face à de nouvelles menaces et que les anciennes mesures sécuritaires ne sont pas nécessairement adéquates. Afin d'assurer la sécurité de sa population, le gouvernement doit prendre de nouvelles mesures (Jackson, 2005).

Nous allons aussi regarder l'utilisation d'évènements historiques pour qualifier le cyberterrorisme. Ces deux derniers choix sont justifiés par l'étude de Richard Jackson qui les identifie dans son analyse des déclarations officielles de l'administration états-unienne. Dans son ouvrage, *Writing the War on Terrorism*, il analyse le langage utilisé par le gouvernement états-unien dans les documents officiels pour construire son discours sur la menace du terrorisme et pour justifié ses actions à sa population (Ibid.).

Aussi, la perception est un processus influencé par le milieu social de l'individu; différents acteurs n'auront pas nécessairement la même perception d'une situation. Il est plausible qu'une situation soit bénéfique pour un groupe d'individu et problématique pour un autre. Donc, il existe un problème de perception. Afin de l'atténuer, nous tiendrons compte de l'auditoire (Waever, 1995). En effet, une tentative de sécurisation sera réussie si l'auditoire

accepte la conjoncture comme problématique. L'intégration de l'auditoire permet de réduire, sans les éliminer complètement, les perceptions marginales d'une situation précise. Il est toutefois possible que le négociateur et l'auditoire aient tous les deux une perception erronée de la situation. Une perception est nécessairement subjective et peu importe celles des acteurs, ce qui prime avant tout, c'est que dans une tentative de sécurisation, il y a une négociation entre les différents acteurs. Nous pouvons donc affirmer que la sécurisation est un processus intersubjectif et socialement construit (Buzan, Waever et Wilde, 1998).

Buzan, Weaver et Wilde proposent deux facteurs qui font varier les chances d'une sécurisation réussie. Le premier facteur est la position sociale du négociateur. Plus l'acteur a un rang social élevé, plus il a la légitimité pour examiner un enjeu particulier. Donc, la crédibilité ou la réputation d'un acteur a une influence sur ses chances d'une sécurisation réussie. De base, les experts retenus dans ce mémoire ont tous une certaine crédibilité étant donné que nous avons choisi les plus reconnus dans leur domaine. Néanmoins, il est probable que certains d'entre eux jouissent d'une meilleure réputation auprès de l'administration états-unienne que les autres. Nous pensons notamment à John Arquilla et David Rondfeldt de la RAND Corporation. Ce laboratoire d'idées (*think tank)* est en grande partie financé et est très proche de l'administration états-unienne. En effet, plusieurs de leurs publications sont rédigées à la demande du *Office of the Secretary of Defense*. Dans cette optique, nous affirmons qu'ils ont eu plus d'influence sur les politiques du gouvernement des États-Unis que d'autres experts retenus dans ce mémoire. Alors, nous allons retenir cette variable dans notre analyse. Nous l'utiliserons pour éclairer notre analyse lorsque nous pouvons prouver qu'un expert jouit d'une meilleure crédibilité ou réputation auprès de l'administration états-unienne.

La deuxième variable est la relation entre le négociateur et l'auditoire. Plus cette relation est bonne, plus les chances d'une sécurisation réussie augmentent. L'auditoire a tendance à écouter et à porter plus d'attention au propos d'un individu qu'il lui plait. Inversement, si la relation entre les deux parties est mauvaise, les chances d'une sécurisation réussies sont susceptibles de diminuer. Évidemment, ce rapport n'est pas statique, mais est variable dans le

temps. Alors, nous devons mesurer la qualité de la relation à divers moments (Ibid.). Afin d'évaluer cette relation, nous devrons produire plusieurs sondages nationaux administrés sur plusieurs années et analyser ces données pour obtenir une idée de la nature de la relation entre le négociateur et l'auditoire. Compte tenu de notre sujet d'étude et de nos moyens, il est impossible de mesurer la qualité et la relation entre les experts de la sécurité et la population des États-Unis.

Nous notons que même un acteur sécuritaire qui a une position sociale distinguée et une relation privilégiée avec son auditoire ne garantit en rien le succès d'une tentative de sécurisation. Dans cette optique, il y a d'autres facteurs qui ne sont pas mentionnés et qui permettraient d'expliquer la réussite ou l'échec d'un acte de sécurisation avec plus d'exactitude. Le modèle explicatif de la liste des priorités des menaces de John Erikson et d'Erik Noreen offre six facteurs explicatifs supplémentaires. Ces facteurs sont de nature cognitive, environnementale, identitaire, politique, institutionnelle et l'opinion publique (Eriksson, J. et E. Noreen, 2002).

Nous avons décidé de retenir le modèle de la théorie du cadrage (*framing theorie*) élaboré par Cavelty (2007) au lieu de celui d'Eriksson et Noreen pour deux raisons. Premièrement, celui-ci permet d'intégrer le modèle explicatif de Buzan, Waever et Jaap. Deuxièmement, cette théorie a déjà été employée pour déterminer si le gouvernement des États-Unis avait fait du cyberterrorisme un enjeu de sécurité. Il permet une meilleure comparaison entre notre recherche et celle de Cavelty.

Avant de continuer, nous jugeons qu'il est important d'expliciter la théorie du cadrage comme Cavelty l'a développée. Nous définissons le cadrage comme la sélection de certains éléments d'une situation, considérés comme problématiques par l'acteur sécuritaire, afin d'exposer à l'auditoire la menace à laquelle ils font face. C'est une stratégie de l'acteur sécuritaire pour faciliter une réponse particulière à la menace (Ibid.)[3]. Ainsi, le cadrage

[3] Nous utiliserons le terme de *cadre* et de *cadrage* au lieu des termes d'*encadrement* et d'*encadrage* afin de simplifier le texte.

correspond à la vision et aux intérêts de l'acteur sécuritaire. En d'autres mots, la manière dont un problème est cadré permet d'établir le ou les responsables ainsi que ses implications pour l'ensemble de l'auditoire. De plus, cela leur permet de proposer des solutions. Le tout est fait en utilisant des images, de stéréotypes, de messages et de métaphores.

Nous allons définir le concept de cadre. C'est un schéma d'interprétation qui contient les idées des individus et que ces derniers utilisent pour comprendre et réagir à une situation précise. En d'autres mots, les cadres permettent d'appréhender la perception et la réaction des individus envers un évènement. Ces schémas ne sont pas immuables et peuvent changer selon les expériences vécues. De plus, l'utilisation d'un langage précis qui dramatise l'état des choses, comme les métaphores et les stéréotypes, peut modifier la conception qu'une personne a d'une menace et transformer ses cadres.

La théorie du cadrage octroie des réponses à trois types de questions. Le premier type permet de déterminer comment les cadres influencent l'action sociale. Le deuxième type permet de distinguer la manière dont les cadres peuvent être changés. Le troisième type permet d'établir quel cadre est plus efficace pour effectuer une sécurisation et pour quelles raisons. Nous allons nous intéresser principalement à ce dernier type de question (Ibid.).

Le cadre théorique que nous utiliserons prendra en compte quatre types de cadres. Le premier type est le cadre diagnostique (*diagnostic frame*). C'est un schéma d'interprétation qui permet aux individus d'établir un problème et d'assigner le blâme à un agent ou une agence précis. En d'autres mots, le cadre définit ce qui est menacé et qui le menace. Alors, lorsqu'un acteur sécuritaire effectue un cadrage du cadre diagnostique, il désigne ce qui lui semble constituer un problème et identifie ceux qu'il croit responsables de cette situation. Par la suite, il essaie de convaincre son auditoire du danger qui les guette. Le cadrage du cadre diagnostique est réussi si l'auditoire adopte son cadre, c'est-à-dire qu'il indique le même problème et le même responsable que l'acteur sécuritaire. Dans le cas contraire, la tentative échoue, car l'auditoire ne perçoit pas la situation désignée par l'acteur sécuritaire comme problématique.

Le second type de cadre est appelé cadre pronostique (*prognostic frame*). C'est un schéma d'interprétation qui permet aux individus de trouver des solutions afin de protéger ce qui est menacé. De plus, ce cadre explique la manière dont il faut procéder pour arriver à ces solutions. Alors, lorsqu'un acteur sécuritaire effectue un cadrage du cadre pronostique, il offre des solutions à la problématique et il énumère les stratégies, les tactiques et les objectifs pour résoudre le problème. Après, il essaie de convaincre son auditoire de la nécessité d'opter pour ses solutions. Le cadrage du cadre pronostique est réussi si l'auditoire sélectionne son cadre, c'est-à-dire qu'il applique les solutions fournies par l'acteur sécuritaire. Dans le cas contraire, la tentative échoue, car l'auditoire n'a pas arrêté son choix sur une de ces solutions ou il va en choisir une différente.

Le troisième type de cadre est le cadre motivationnel (*motivational frame*). C'est un schéma d'interprétation qui a pour objectif de rallier la population à la lutte contre la menace. Aussi, il appelle souvent la prise d'action concrète par la population. Conséquemment, lorsqu'un acteur sécuritaire effectue un cadrage du cadre motivationnel, il justifie la nécessité d'un regroupement de la population et qu'elle agisse contre la menace. Le cadrage du cadre pronostique est réussi si l'auditoire adopte son cadre, c'est-à-dire qu'il va se rassembler et qu'il va consentir à intervenir contre la problématique. Dans le cas contraire, la tentative échoue, car l'auditoire n'est pas disposé à se réunir et vouloir réagir par rapport à la situation désignée par l'acteur sécuritaire.

Le dernier type est le cadre de résonance (*frame resonance*). Lors du processus de cadrage, l'acteur sécuritaire va transmettre certaines croyances et valeurs à travers son discours. Celles-ci sont acheminées à l'aide du cadre de résonance élaboré par l'acteur sécuritaire. Afin que les cadres soient acceptés par l'auditoire, il faut que les croyances et valeurs transmissent par le cadre de résonance soit désirable ou cohérent avec les croyances et les valeurs existantes de l'auditoire ciblé (Ibid.). Le cyberterrorisme, comme le terrorisme traditionnel, met le mode de vie et la sécurité de la population des États-Unis en danger, nous jugeons que le cadre de résonance du cyberterrorisme est cohérent avec ses valeurs et à ses

croyances. De plus, les solutions proposées par les experts de la sécurité ne briment pas les droits et la liberté de la population, mais tentent de renforcer leur sécurité en protégeant les infrastructures essentielles. Il n'y a donc vraiment pas de débat à savoir s'il faut se protéger contre cette menace. Dans d'autres problématiques, l'étude du cadre de résonnance est primordiale particulièrement lorsque les croyances et les valeurs sont remises en jeu. Normalement, elles provoquent une division entre plusieurs camps dans la population. Nous pensons notamment aux questions éthiques telles que l'avortement ou la peine de mort. Dans de tels cas, une tentative de cadrage peut échouer parce qu'elle va à l'encontre des croyances et des valeurs de l'auditoire ciblé. Pour notre étude, les cadres proposés par les experts de la sécurité visent à conserver les croyances et les valeurs de la population états-unienne. Celles véhiculées par les cadres sont donc désirables et cohérentes avec ceux de la population états-unienne. Dans cette optique, nous postulons que le cadre de résonance est efficace. L'utilité d'analyser ce cadre se trouve réduite. Dans ces circonstances, nous allons nous concentrer sur les trois premiers cadres pour déterminer le résultat des tentatives pour faire du cyberterrorisme un enjeu de sécurité aux États-Unis.

Il est important de distinguer ces cadres les uns des autres parce que cette distinction nous laisse mieux évaluer leurs impacts sur une tentative de sécurisation. Elle permet de déterminer si une tentative a réussi, car il faut que l'ensemble des cadres soit accepté. Dans le cas d'un échec, nous pouvons cerner le ou les cadres qui n'ont pas été approuvés par l'auditoire et les raisons de ce refus.

Nous utiliserons cette théorie pour trois raisons. En premier lieu, la théorie du cadrage est basée, en grande partie, sur celle de la sécurisation. Cela nous permet d'employer le concept d'acte de langage. Cela nous permet d'analyser d'une manière différente les tentatives de faire du cyberterrorisme un enjeu de sécurité aux États-Unis.

En second lieu, elle permet d'intégrer le modèle explicatif de Buzan, Waever et Jaap (1998). Cela nous donne une analyse plus complète des différents cadres utilisés lors de la tentative de sécurisation.

En dernier lieu, la théorie du cadrage a déjà été utilisée pour traiter des tentatives pour faire du cyberterrorisme un enjeu de sécurité aux États-Unis. Cette étude de Cavelty s'intéresse principalement au gouvernement des États-Unis comme acteur sécuritaire (2007). Nous procédons aux mêmes types d'analyse que Cavelty, mais nous remplaçons le gouvernement des États-Unis par les experts de la sécurité comme acteur sécuritaire.

Pour nous permettre de faire la distinction entre les nombreuses stratégies employées par les experts de la sécurité pour influencer le gouvernement, nous utiliserons la théorie des entrepreneurs politiques développée par Ralph Carter et James Scott dans leur ouvrage *Choosing to Lead* (2009). Dans un premier temps, nous justifierons ce choix. Dans un second temps, nous explorons les stratégies utilisées par l'entrepreneur politique.

Premièrement, ils appliquent leur théorie aux membres du Congrès, mais celle-ci peut très bien s'appliquer à toutes sortes d'experts différents. En effet, l'entrepreneur politique est un « expert » (Carter et Scott, 2009, p.26) et il est persistant dans son intérêt pour la problématique. Aussi, nous constatons que cette théorie emploie le concept de cadrage ce qui justifie d'autant plus la pertinence de notre choix. De plus, il a le même objectif que l'acteur sécuritaire : il désire que le gouvernement modifie ou développe de nouvelles politiques par rapport un enjeu spécifique. Pour y arriver, il tente de :

- Mettre en place son cadre pour diriger la discussion sur l'enjeu et mobiliser la population et les groupes d'intérêts.
- Diriger l'agenda politique du Congrès pour qu'une attention particulière soit accordée à cette problématique.
- Structurer et influencer le gouvernement dans sa formulation de ses politiques.
- Modifier, préciser ou reformuler les politiques du gouvernement.
- Combler les vides législatifs avec leur proposition de politique.

Deuxièmement, l'entrepreneur politique utilise une multitude de stratégies pour influencer les politiques du gouvernement. Elles sont divisées en deux types. Le premier type est les stratégies dites législatives. Dans la mesure où les experts retenus dans notre analyse n'ont aucun pouvoir législatif, il n'est pas pertinent de se pencher sur celle-ci. Le deuxième type de stratégie englobe celles non législatives. Elles sont au nombre de quatre.

La première consiste à visiter et à regarder en personne les conséquences d'une politique pour par la suite en discuter. Celle-ci n'est pas retenue dans notre analyse, car il est impossible, pour le moment, de voir les conséquences du cyberterrorisme, car ça ne s'est jamais produit.

La deuxième stratégie employée est de communiquer personnellement avec un des membres de l'administration au sujet de la problématique. Cette option est intéressante. Toutefois, nous sommes souvent dans l'impossibilité de confirmer s'il y a eu une correspondance entre un expert et un membre de l'administration. Dans ces circonstances, nous n'allons pas négliger cette stratégie et nous allons en tenir compte, mais ce ne sera pas la stratégie privilégiée.

La troisième et la quatrième stratégie nous semblent les plus prometteuses. Elles sont la publication de recherche et la participation dans des médias. Plus précisément, cette dernière stratégie consiste à publier des articles dans des revues ou journaux et à apparaitre dans des émissions de télévisions et de radios. Ces deux stratégies sont complémentaires. En effet, elles accordent de la visibilité à la problématique et permettent aux experts d'exprimer leurs idées à la population et aux membres de l'administration états-unienne.

1.2 Définitions des concepts

Nous jugeons qu'il est nécessaire de définir certains concepts essentiels à notre travail. Le premier concept est celui de la sécurisation. Nous utilisons la définition que nous avons explicitée précédemment.

Le deuxième concept est celui d'experts de la sécurité. Nous le définissons comme un individu qui possède un savoir et une expertise dans le domaine de la sécurité. Ce dernier a développé ses compétences à l'aide de son expérience professionnelle ou par sa formation théorique. Son bagage de connaissance lui donne une légitimité pour fournir son opinion ou son expertise sur les questions de sécurité. Aussi, il communique ses acquis aux dirigeants et à l'ensemble de la population; il participe donc au débat public sur les questions de sécurité.

La définition ci-dessus est trop large. Afin de l'opérationnaliser, nous rajoutons des critères supplémentaires à cette définition. Premièrement, le domaine de la sécurité étant très vaste, nous restreignons notre définition des experts de la sécurité spécialisée dans le sous-domaine des cybermenaces.

Deuxièmement, dans ce sous-domaine, nous distinguons deux types d'experts. Le premier type a une expertise technique en informatique. Il s'intéresse uniquement à la composante informatique des cybermenaces. Ce sont généralement des administrateurs réseau, des programmeurs et des ingénieurs en génie informatique. Le second type d'expert est celui qui nous intéresse. Ce sont ceux qui se préoccupent peu de l'aspect informatique, leur champ d'expertise est dans le domaine des conséquences et des implications sociales et politiques des cybermenaces. En fait, ils s'intéressent aux conséquences des cybermenaces pour l'État, la société et les individus ainsi qu'aux politiques pour lutter et contrer cet enjeu. Ce type d'expert peut englober une pluralité de profession. En effet, ils peuvent être des journalistes, des membres de groupes d'intérêts, des présidents d'entreprise, des chercheurs dans des laboratoires d'idées (*think tanks*) ou des professeurs d'université.

Troisièmement, comme nous allons étudier des monographies et des articles scientifiques d'experts de la sécurité, nous ne tiendrons pas compte des membres de groupes d'intérêts et des présidents d'entreprise, car ils ne produisent pas ce type de document.

En résumé, les experts de la sécurité retenus sont des journalistes, des chercheurs dans des laboratoires d'idées (*think tanks*) et des professeurs d'université qui ont une expertise en matière de cybermenace et sont les plus reconnus dans ce domaine. Ils écrivent des monographies ou des articles scientifiques qui traitent des conséquences, des implications sociales et des politiques de cet enjeu. Ils utilisent ces médias afin de transmettre leur opinion d'expert à la population et d'influencer le gouvernement dans son écriture des politiques en lien avec le cyberterrorisme.

Le troisième concept est celui des infrastructures essentielles (*Critical Infrastructure*). Elles sont définies aux États-Unis par la *Presidential's Commission on Critical Infrastructure Protection* (PCCIP) et sont divisées divisent en cinq catégories (États-Unis, 1997): l'information et la communication, les réseaux de transport, l'énergie, les services financiers et bancaires et les services vitaux à la personne (Ashley, 2003). Chacune de ces catégories approvisionne les services essentiels à la société autant pour la sécurité physique des citoyens que pour l'économie de la nation.

Le dernier concept est celui du cyberterrorisme. Nous utilisons cette définition :

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attack that disrupt nonessential services or that are mainly a costly nuisance would not (Deening, 2000, p. 29).

Nous l'avons choisi parce qu'elle contient les trois éléments traditionnels du terrorisme soit la violence et l'usage de la force, la motivation politique de l'acte et la création d'un état de terreur dû à l'attentat (Schmid et Jongman, 2005). De plus, l'intégration de ces trois composantes permet de différencier le cyberterrorisme des autres activités comme le cybercrime, le piratage informatique et l'« Hacktivisme », soit l'utilisation du piratage à des fins politiques sans violence (Conway, 2002; Denning, 1999; Yar, 2006).

Toutefois, Gordon et Ford soutiennent que cette définition contient deux problèmes. Le premier problème est qu'elle ne considère pas l'usage de la haute technologie dans le but de préparer ou de financer illégalement des actes de terrorisme. L'inclusion, de l'utilisation de l'électronique ou des ordinateurs, pour ces fins, nous ramène aux difficultés reliées à la différenciation du cybercrime et du cyberterrorisme. Par conséquent, cette critique est insatisfaisante. Le deuxième problème est que la définition de Denning est différente de celle utilisée par les médias, et la population en général (Gordon et Ford, 2002). Cette critique est aussi faible dans la mesure où diverses études ont démontré la confusion des médias et du grand public à discerner les diverses activités sur internet et à l'usage excessif du préfixe « cyber » pour distinguer toutes nouvelles choses (Weimann, 2005).

Selon cette définition, il n'y a eu, à ce jour, aucun attentat cybertorriste. Il nous semble judicieux de donner quelques exemples de cyberattaques qui sont considérés comme du cyberterrorisme. Par exemple, une cyberattaque par un groupe terroriste sur des installations électriques d'une région urbaine. Cette attaque causerait une panne de courant pour plus d'une semaine ce qui entraînerait des pertes économiques importantes et la possibilité de décès humains. Une autre illustration serait la modification des groupes sanguins dans les ordinateurs d'un centre hospitalier par un groupe terroriste. Cette action aurait pour conséquence de mettre la vie en danger des patients qui recevraient une transfusion sanguine. Le dernier exemple serait l'infiltration du système de la tour de contrôle d'un aéroport et de causer la collision entre deux avions (Denning, 2000).

CHAPITRE II

L'ÉVOLUTION DU CADRE DIAGNOSTIQUE DU CYBERTERRORISME AUX ÉTATS-UNIS

Dans ce chapitre, nous analysons l'évolution du cadre diagnostique du cyberterrorisme aux États-Unis afin de déterminer si les experts de la sécurité ont réussi à influencer le gouvernement. Pour ce faire, nous utilisons le cadre diagnostique, c'est-à-dire un schéma d'interprétation qui permet aux individus de définir un problème et d'assigner le blâme sur un agent ou une agence précis.

Également, nous soutiendrons que le gouvernement et les experts de la sécurité n'ont pas le même cadre diagnostique du cyberterrorisme malgré qu'ils distinguent les infrastructures essentielles comme ce qui est menacé. En effet, les experts de la sécurité ont tenté de limiter la menace au cyberterrorisme tandis que le gouvernement a inclus l'ensemble des cybermenaces. Selon ce dernier, le cyberterrorisme est une cybermenace parmi tant d'autres. Toutefois, nous relevons que certains experts de la sécurité ont participé, de concert avec le gouvernement, à déterminer ce qui est menacé, c'est-à-dire les infrastructures essentielles.

2.1 L'influence du boom technologique et la Révolution dans les affaires militaires sur le cadre diagnostique du gouvernement des États-Unis

Dans cette section, nous soutenons que le boom technologique des années 1990 a inscrit les cybermenaces dans les préoccupations politiques du gouvernement. De plus, nous croyons que la Révolution dans les affaires militaires a élargi la perception de la vulnérabilité des États-Unis par rapport aux cybermenaces.

Le concept de réseau informatique n'était pas très bien connu de la majorité de la population dans les années 1980. Nous pensons qu'il est nécessaire d'expliquer comment les cybermenaces sont devenues un sujet d'actualité dans les années 1990. Nous distinguons deux raisons. La première est le boom technologique. En fait, une partie importante des entreprises états-uniennes ont intégré les systèmes informatiques comme outils de travail. Comme le souligne Dan White, directeur de la sécurité de l'information chez Ernst & Young, l'adoption rapide des nouvelles technologies a dépassé la capacité de la plupart des compagnies à protéger convenablement leurs ordinateurs (Alexander, 1990). De nombreuses brèches de sécurité existent et les compagnies ne protègent pas leur réseau informatique adéquatement. La revue *Network World* a évalué que seulement 17 % des mille plus grosses compagnies aux États-Unis ont une sécurité informatique adéquate (Network World, 1990). Ces compagnies s'exposent à différents types de problèmes, car les pirates informatiques ont la possibilité de lire, voler, changer et détruire des informations sur un système informatique (Allen-Tonar, 1989).

La deuxième raison est la Révolution dans les affaires militaires (RAM). Nous la définissons comme :

> une transformation radicale de la nature de la guerre, conséquence des percées technologiques qui, associées à des changements profonds de la doctrine militaire et des concepts organisationnels, modifient fondamentalement le caractère et la conduite des opérations militaires. [...] pour qu'il y ait « révolution », il faut que les nouvelles technologies conduisent à un changement profond de la doctrine et de l'organisation, ou qu'elles y trouvent leur répercussion (Gagnon, 2009, p. 23).

Cette RMA se caractérise par l'apparition d'un avantage technologique utilisé pour la conduite de la guerre. En d'autres mots, l'arrivée et l'utilisation de systèmes informatiques connectés en réseau permettant l'échange d'information quasi instantanément auraient changé la façon de diriger la guerre (Braillard et Maspoli, 2001). Selon la théorie d'Alvin Toffler dans *The third wave* (1980), l'Histoire serait constituée de trois vagues, la vague agraire, la vague industrielle et la vague post-industrielle qui est aussi appelée la vague informationnelle. Elles seraient le résultat de grandes transformations technologiques et

niveau du type d'organisation de la production. Actuellement, nous serions en transition vers la vague post-industrielle. Celle-ci met l'accent sur la connaissance et sa qualité. L'information deviendrait l'attribut primordial de l'organisation complète de la société. Le domaine militaire serait affecté, car l'information deviendrait l'élément décisif dans la conduite de la guerre. La théorie de Leonard Dudley dans *The word and the sword* (1991), nous mène à la même conclusion. Les progrès technologiques et techniques donneraient un avantage concurrentiel à un parti et modifieraient la conduite de la guerre et influencent la société en général.

La Révolution dans les affaires militaires bouleverse l'organisation traditionnelle de la conduite de la guerre en rajoutant la sphère du cyberespace (Lonsdale, 1999). Nous tenons à expliquer ce terme. Il est dérivé de l'anglais *Cyberspace*. Il est une contraction des mots *cyber* et *espace*. Il est un néologisme apparu en 1982 dans une nouvelle de William Gibson, *Burning Chrome* (2003). Il l'explicite dans sa plus célèbre œuvre *Neuromancer* (Gibson, 1984). L'expression a été longtemps considérée comme un terme fourre-tout à la mode pour décrire des univers virtuels. William Gibson a lui-même avoué qu'il l'a inventé parce qu'elle n'a pas de réelle valeur sémantique, c'est-à-dire qu'elle n'a pas de véritable signification (Neale, 2000). Aujourd'hui, cette expression est présente dans le lexique des dictionnaires. Par conséquent, nous utiliserons la définition du *Nouveau Petit Robert 2009*, qui le définit comme : « Espace de communication créé par l'interconnexion mondiale des ordinateurs. » (Société Dictionnaire le Robert, 2009, p. 605).

Deux autres concepts issus de la guerre de l'information ont été proposés par Julie Horn (2004). Il s'agit de la cyberguerre (*Cyberwar*) et la guerre du Net aussi appelée guerre de la toile (*Netwar*)[4]. Avant de les définir, il est important de mentionner que ces deux concepts sont souvent considérés comme synonymes. En fait, la majorité des auteurs les définissent comme « une agression informatisée dans le cyberespace » (Ibid., p. 42). Toutefois, Arquilla et Ronfeldt affirment qu'ils n'ont pas la même signification. Selon eux, la cyberguerre, est une guerre de l'information dans les conflits de haute ou moyenne intensité. Elle est

[4] Nous utilisons la traduction libre de Julie Horn.

normalement une guerre dans le sens traditionnel du terme. Le concept cyberguerre n'a donc pas de lien avec le cyberterrorisme. Le second concept, la guerre du net, est défini par le type d'agresseur et non pas par l'utilisation de la technologie (Arquilla et Ronfeldt, 1993). Comme le résume Horn, « *Netwar* est la conséquence d'une révolution de l'information ou les nouvelles technologies de communication renforcent les conflits de basse intensité. » (2004, p.42). Internet devient le lieu d'affrontement de ces conflits de basse intensité. Le cyberterrorisme étant une forme de conflit de basse intensité sur le cyberespace, il correspond à la définition de *Netwar*.

La guerre du Golfe Persique de 1991 est le premier exemple de l'intégration du cyberespace dans la conduite de la guerre. Cette guerre a démontré les avantages de maîtriser l'information grâce à des systèmes informatiques. Toutefois, cet avantage crée une dépendance par rapport à ces systèmes, car une partie peut avoir des systèmes informatiques supérieurs à l'autre, il reste qu'il ne domine pas l'autre pour autant. Comme le précise Martin C. Libicki, la guerre informationnelle n'est pas un jeu à somme nulle comme la guerre navale (1995). Lors d'une guerre navale, l'armée la plus puissante peut contenir son adversaire. Il y a un gagnant et un perdant. Pour ce qui est de la guerre informatique, le protagoniste qui possède les meilleurs systèmes informatiques ne maîtrise pas l'information de son ennemi. L'opposant est toujours en mesure de recueillir, d'analyser et de transmettre de l'information. De plus, la dépendance à des systèmes informatiques engendre une nouvelle vulnérabilité soit le piratage informatique.

L'exemple le plus couramment cité de cette tactique a eu lieu pendant cette guerre alors que des pirates hollandais ont réussi à exécuter une cyberattaque sur 34 ordinateurs du Département de la défense et ont volé des informations sur l'emplacement des troupes états-unienne en Irak (États-Unis. General Accounting Office, 1996). Cet exemple démontre que l'avantage informationnel peut devenir un désavantage informationnel.

La Guerre du Kosovo vient appuyer les conclusions de la Guerre du Golfe Persique. En fait, un rapport du GOA remarque que le brouillard de la guerre n'a pas été dissipé malgré

l'avantage informationnel de l'OTAN (États-Unis, 1997). Bien au contraire, ce conflit a été marqué par l'incertitude, car les forces armées serbes ont réussi à pirater et à modifier une base de données informatiques de l'OTAN. Cet évènement a occasionné des difficultés lors de l'opération de l'OTAN au Kosovo (Thomas, 2000).

Nous concluons que la guerre du Golfe Persique a mis en place une nouvelle peur des technologies de l'information, et par le fait même, des cybermenaces. La guerre du Kosovo a réaffirmé cette vulnérabilité. En somme, le boom technologique et la Révolution dans les affaires militaires ont créé un élargissement de la perception de la vulnérabilité des États-Unis à l'égard des cybermenaces (Cavelty, 2007).

2.2 L'influence de l'attentat d'Oklahoma City sur le cadre diagnostique du cyberterrorisme

Dans cette section, nous soutenons l'attentat d'Oklahoma City a propulsé l'enjeu de la protection des infrastructures essentielles. Aussi, nous remarquons que le gouvernement et les experts de la sécurité ont mis en place un cadre diagnostique des cybermenaces et non du cyberterrorisme. Nous croyons qu'ils définissent les infrastructures essentielles comme menacées et qu'ils tentent de les protéger contre une multitude de menaces physiques et virtuelles.

Un événement majeur le 19 avril 1995 va pousser les décideurs à prioriser la protection des infrastructures essentielles aux États-Unis : L'attentat d'Oklahoma City. Ce dernier effectué par Timothy McVeigh et Terry Nichols, deux citoyens états-uniens qui ont placé un camion chargé d'explosif dans le stationnement du bâtiment fédéral Alfred P. Murrah. L'explosion de l'édifice a fait 168 morts et plus de 800 blessés.

Cet attentat a été un choc pour la nation. Le gouvernement des États-Unis a décidé de réaffirmer son désir de prévenir et de lutter contre le terrorisme. Ce désir s'est exprimé dans le *Presidential Decision Directive 39* (PDD 39) du 21 juin 1995. La directive met à l'avant la

protection des infrastructures essentielles (États-Unis, 1995b). Elle demande au ministre de la Justice, Janet Reno, de mener une enquête gouvernementale afin d'examiner la protection des infrastructures essentielles du pays. Selon Sarah Jane League, vice-présidente de l'*Infrastructure Protection Task Force*, le rapport partiel de février 1996 indique qu'il y a un manque d'attention accordée à la protection des systèmes et des réseaux informatiques des infrastructures essentielles. De plus, il exprime que cette situation crée des vulnérabilités au niveau des systèmes et des réseaux informatiques qui pourraient être utilisés par des terroristes pour conduire des attaques traditionnelles plutôt que des cyberattaques. La possibilité d'un attentat cyberterroriste n'est donc pas écartée (League et coll., 1997). Par conséquent, le rapport lie le concept de cybermenaces à celui de la protection des infrastructures essentielles et du terrorisme. Le lien sera consolidé par le Presidential Commission on Critical Infrastructure Protection.

Du point de vue du cadre diagnostique, le PDD-39 affirme que le gouvernement des États-Unis désire lutter contre le terrorisme sous toutes ses formes. Conséquemment, il inclut le cyberterrorisme implicitement. En deuxième lieu, l'identification de ce qui est menacé par les terroristes a changé. Il distingue les infrastructures essentielles, car elles sont maintenant vulnérables tant physiquement que virtuellement. Ces changements sont perceptibles parmi certains experts de la sécurité.

La protection des infrastructures essentielles n'est pas nouvelle aux États-Unis. Pendant la dernière partie de la Deuxième Guerre mondiale, les théoriciens de la puissance aérienne des États-Unis ont craint les effets d'une attaque sur ces infrastructures. Ils ont conclu que, si les États-Unis pouvaient utiliser des bombardements stratégiques afin de détruire les infrastructures de l'ennemi, d'autres entités pourraient tenter cela sur le territoire états-unien (Collier et Lakoff, 2008). Voyant l'efficacité de cette méthode, certaines organisations gouvernementales ont essayé de réduire la vulnérabilité de leur installation. Un des moyens a été la création du *Defense Electric Power Administration* (DEPA) au début des années 1950. Aussi, ils ont commandé, durant les années 1960, plusieurs études pour effectuer des

évaluations internes des vulnérabilités de leurs systèmes sans s'attarder sur les effets d'un événement particulier (Light, 2002).

Il faut attendre jusqu'au milieu des années 1970 pour que la thématique de la protection infrastructures essentielles refasse surface. Dans ces mêmes années, une minorité d'experts de la sécurité ont affirmé que la protection des infrastructures essentielles pourrait être difficile. Selon eux, des groupes non gouvernementaux hostiles, dont des groupes terroristes, pourraient s'attaquer à ces infrastructures et causer des dommages importants aux États-Unis (Collier et Lakoff, 2008). Robert H. Kupperman, un de ces experts, soutient que le terrorisme est devenu un outil stratégique dans les conflits de faible intensité. Dans cette optique, les terroristes tenteraient d'exploiter les vulnérabilités des infrastructures essentielles des États-Unis, car c'est déjà arriver ailleurs. Il écrit : « Attacks on society's infrastructure have already occurred. » (Kupperman et coll., 1982, p. 28).

Dans cette lignée, un autre texte, *America's Hidden Vulnerabilities : Crisis Management in a Society of Networks*, rédigé par l'équipe de Woolsey en 1984, exprime son inquiétude par rapport aux nouvelles menaces et propose des politiques pour y faire face. Par contre, ce texte a été marginalisé par le gouvernement des États-Unis de l'époque (Collier et Lakoff, 2008).

Il faut attendre le début des années 1990 et l'apparition des réseaux informatiques pour que la protection des infrastructures essentielles redevienne un sujet d'actualité. Celui-ci regagne sa popularité à l'aide d'une étude du gouvernement intitulé *Computer at Risk* (États-Unis. National Research Council, 1991). Elle conclut que les réseaux informatiques du gouvernement et du secteur privé ne sont pas protégés suffisamment. Ils les qualifient de *defenseless*. Selon elle, les États-Unis sont dans une posture où une attaque informatique d'envergure contre eux est très probable. Celle-ci pourrait être commise par un large éventail d'acteurs comme des États, des criminels et des terroristes. Dans cette étude, le concept de cyberterrorisme et d'infrastructure essentielle est présent.

Nous devons préciser que ce texte a été influencé, en partie, par Winn Schwartau. Ce dernier affirme qu'il a témoigné devant le *United States Congress* le 22 juin 1991 (Schwartau, 1994). Selon ses dires, il a soutenu que les systèmes informatiques du gouvernement des États-Unis sont à peu près sans protection. De plus, il a employé le terme *computer terrorist* pour désigner des groupes terroristes qui utiliseraient la composante informatique pour commettre des attentats. Il considère que c'est un nouveau concept de guerre électronique à faible coût qui a recours aux hautes technologies pour infliger de la destruction massive (Ibid.). Aussi, il est le créateur de l'expression *Electronic Pearl Harbor*. Celle-ci désigne une attaque informatique sur les infrastructures essentielles de l'État qui provoquerait un effondrement des services de base de la société (Ibid.). Cette expression est reprise dans le document *Computer at Risk*, il a donc influencé son contenu.

Nous allons maintenant nous attarder sur trois termes utilisés dans les deux textes. Ce sont les premiers exemples d'utilisations d'évènements historiques et du vocabulaire exprimant l'entrée des États-Unis dans une nouvelle ère et celui évoquant l'incertitude pour qualifier le cyberterrorisme.

Le premier est *electronic Pearl Harbor*. Cette symbolisation renvoie à l'attaque historique de 1942 : Pearl Harbor. L'emploi de ce terme n'est pas naïf, car il vise à démontrer la capacité destructrice qu'aurait une telle attaque sur le territoire états-unien ainsi que le traumatisme qu'elle causerait à la population. Cette expression a été reprise à maintes reprises par les médias. En fait, Maura Conway affirme qu'elle a été utilisée 105 fois dans les principaux journaux états-uniens pendant la période de 1994 à 2004 (2008). Nous pouvons donc déclarer que cette expression a réussi à marquer l'imaginaire collectif.

Le deuxième terme est en lien avec le second, il s'agit de l'utilisation du mot *defenseless*. Son emploi renvoie à une situation où les États-Unis seraient vulnérables, ou même, sans protection, devant un *electronic Pearl Harbor*. L'usage de ces termes permet définir les infrastructures essentielles comme ce qui est menacé. Aussi, ces termes soulignent le caractère d'urgence de la situation.

Le troisième terme est un énoncé de David Clark, un chercheur du *Massachusetts Institue of Technology's computer science lab,* et du panel d'experts qui ont été consultés lors de la rédaction du rapport *Computers at Risk* (Peterson, 1990). Ce document dit : « Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb» (National Research Council, 1991, p. 7).

Cet énoncé a deux conséquences. Premièrement, il affirme la possibilité de l'utilisation d'ordinateurs par des terroristes pour commettre des attentats. Deuxièmement, il envoie l'idée que la protection virtuelle des infrastructures essentielles est plus urgente que leur protection physique. Cette citation est reprise encore à ce jour autant par les experts de la sécurité que par le gouvernement. Troisièmement, l'utilisation de ces termes nous prouve que les experts de la sécurité, mais aussi le gouvernement, ont tenté de protéger les infrastructures essentielles contre les cybermenaces. Donc, le cyberterrorisme est un des ennemis identifiés. Toutefois, une multitude d'adversaires potentiels peuvent utiliser des ordinateurs pour attaquer les infrastructures essentielles. Dans ces circonstances, c'est la protection de ces infrastructures, et particulièrement leur protection virtuelle, qui les intéressent.

Dans un autre ordre d'idées, le rapport *Computer at Risk* a eu une influence sur les experts de la sécurité. En fait, Winn Schwartau continue de reconnaitre, lui aussi, les infrastructures essentielles comme une cible potentielle pour les terroristes. Selon lui, il est évident que les ennemis des États-Unis vont attaquer les infrastructures économiques essentielles. Ces dernières, qu'il nomme *econotechnical infrastructure*, sont vulnérables au niveau virtuel et sont des objectifs idéaux pour les terroristes (Schwartau, 1994). Un autre exemple est le texte de Martin Libicki intitulé *The Next Enemy*. L'auteur soutient qu'une cyberattaque contre certaines infrastructures essentielles pourrait causer la mort de citoyens états-uniens (1995).

Pour conclure, nous regarderons les changements au cadre diagnostique durant cette période. Nous remarquons que l'identification de l'ennemi a évolué. L'utilisation de termes

comme *computer terrorist* et *cyberterrorist* commence à devenir plus commune. Dans cette optique, nous pouvons déclarer que les experts de la sécurité ont réussi à faire adopter ce terme aux médias et aux gouvernements. Néanmoins, il nous est impossible d'affirmer qu'ils ont prouvé aux gouvernements que le cyberterrorisme est une menace qui nécessite une sécurisation, car aucun document de cette période ne s'attarde à cette menace spécifiquement. Du point de vue de l'informatique, les textes s'intéressent aux cybermenaces en général. Ils ne contiennent que des détails sur les risques que courent les systèmes informatiques gouvernementaux. En ce qui concerne la sécurité nationale, le cyberterrorisme est au même niveau que toutes autres formes de terrorisme, c'est-à-dire qu'ils sont non désirables et qu'ils prendront des mesures identiques, sans faire de distinction sur le type de terrorisme.

Au sujet de l'identification de ce qui est menacé, les experts de la sécurité tentent d'imposer les infrastructures essentielles comme la cible principale des cyberterrorismes. Cette tentative semble partiellement accomplie, car ils ont réussi à convaincre le gouvernement des États-Unis que ces infrastructures sont ciblées. Toutefois, le PDD-39 n'envisage que la protection physique de ceux-ci, le côté virtuel, celui qui intéresse les experts, n'est pas mentionné. De plus, nous estimons que l'attentat d'Oklahoma City a été le facteur principal de ce regain d'intérêt pour les infrastructures essentielles. Dans cette optique, les experts de la sécurité, mais aussi le gouvernement tentent de protéger les infrastructures essentielles contre les cybermenaces.

2.3 L'influence du *Presidential Commission on Critical Infrastructure Protection* sur le cadre diagnostique du cyberterrorisme

Dans cette section, nous soutenons qu'une minorité d'experts ont influencé l'écriture de la *Presidential Commission on Critical Infrastructure Protection*. Cette dernière définit le cyberterrorisme, mais surtout les cybermenaces, comme un danger pour les infrastructures essentielles des États-Unis. Toutefois, les experts de la sécurité ont échoué à imposer le cyberterrorisme comme une menace plus importante que les autres cybermenaces. Par conséquent, la portée du cadre diagnostique du cyberterrorisme est réduite.

2.3.1 Le cas du gouvernement

La *Presidential Commission on Critical Infrastructure Protection* (PCCIP) est une étude sur la protection des infrastructures essentielles (President's Commission on Critical Infrastructure Protection, 1997). Elle explicite les menaces ainsi que les ennemis auxquels les États-Unis sont confrontés. De plus, elle décrit les mesures ainsi que les solutions qui s'offrent aux États-Unis pour assurer une protection adéquate des infrastructures essentielles. Cette étude du gouvernement des États-Unis est la plus importante en ce qui concerne les cybermenaces et le cyberterrorisme.

Elle fournit des précisions majeures sur le cadre diagnostique en explicitant l'identification de l'ennemi. Plus spécifiquement, elle retient les mêmes éléments que le NSDD-145, c'est-à-dire que les États étrangers, les criminels et les terroristes sont identifiés comme les ennemis. Toutefois, la PCCIP va au-delà du NSDD-145, elle mentionne cinq types potentiels d'attaques faites par des terroristes exclusivement, sur le cyberespace.

De plus, le concept de cyberterrorisme y apparaît clairement pour la première fois dans une étude officielle lorsqu'elle mentionne : « Potential cyber threats and associated risks range from recreational hackers to terrorists to national teams of information warfare specialists. » (Ibid., p. 15). Aussi, elle souligne le manque de données pour mettre en place un plan d'action en vue de répondre à un « cyber terrorist incident » (Ibid., p. 29). Alors, nous pouvons affirmer que le cadre des cybermenaces inclut le cyberterrorisme.

Aussi, la PCCIP évoque la possibilité d'une cyberattaque perpétrée à l'intérieur du territoire états-unien, ce qui est une autre distinction entre elle et le NSDD-145 en inscrivant le concept d'ennemi intérieur à la liste d'ennemis potentiels à utiliser le cyberterrorisme.

Elle le mentionne « Repeatedly identified as the most worrisome threat is the *insider*—someone legitimately authorized access to a system or network » (Ibid, p. 15). De plus, elle l'identifie comme le type d'adversaire le plus inquiétant auquel font face les États-Unis.

En ce qui concerne l'identification de ce qui est menacé, la PCCIP constitue un changement important, car elle reprend une partie des conclusions du rapport *Computer at Risk* que nous avons à la section 2.2. Elle précise que les États-Unis sont très dépendants de leurs systèmes informatiques et de leurs réseaux. De plus, la PCCIP indique que ses infrastructures essentielles sont vulnérables parce qu'elles sont administrées par ces mêmes systèmes informatiques et réseaux. Dans cette optique, les infrastructures essentielles sont maintenant considérées comme une composante à sécuriser dans une perspective de sécurité nationale. Elles le deviennent lorsque la commission précise qu'elles sont primordiales à la sécurité économique et sociale des États-Unis. Aussi, la commission rappelle que la sécurité des infrastructures essentielles doit être examinée dans un nouveau contexte : celui de l'émergence des réseaux informatiques. La PCCIP affirme: «These critical infrastructures [...] must be viewed in a new context in the Information Age.» (Ibid., p. ix). L'utilisation de l'expression *Information Age* renvoie à l'idée que les États-Unis sont entrés dans une nouvelle période de leur histoire.

Une autre contribution importante de la PCCIP au cadre diagnostique est l'élargissement des vulnérabilités potentielles auxquelles doivent faire face les États-Unis. Cet élargissement est fait en explicitant de façon très précise, pour la première fois, les secteurs d'infrastructures essentielles des États-Unis[5]. Nous avons identifié et défini ces secteurs dans la partie 1.2. Finalement, la commission propose des rapports sur chacun des secteurs d'infrastructure essentielle afin de démontrer l'interdépendance et la vulnérabilité des infrastructures essentielles.

[5] Il est à noter que la majorité des experts et des documents subséquents vont identifier seulement cinq secteurs d'infrastructures essentielles, car certains se regroupent.

Le document issu de la PCCIP a été écrit par vingt individus, dix d'entre eux proviennent d'agences gouvernementales, les dix autres participants sont des experts de différents milieux en lien avec un secteur précis d'infrastructures essentielles. Ces derniers ont tenu un rôle important dans la création de ce document. Nous pouvons donc affirmer qu'ils ont tous influencé son contenu.

Toutefois, Yvo Desmedt souligne que lors de l'étude peu d'experts ont été interrogés. Il soutient que la commission ne prend pas en compte l'opinion de différents experts sur chacune des problématiques abordées. Plus spécifiquement, elle est basée sur un échange entre un officiel du gouvernement des États-Unis et un expert d'un enjeu précis. Desmedt conclut que la PCCIP ne correspond peut-être pas à l'avis des autres experts et que ses conclusions peuvent être biaisées (2006).

2.3.2 Le cas des experts de la sécurité

Pour débuter, nous nous pencherons sur les experts qui ont collaboré à la PCCIP. Par la suite, nous nous intéresserons aux experts qui n'y ont pas participé, car ils peuvent avoir des idées différentes et ils ont peut-être influencé les prochains documents gouvernementaux. De cette façon, nous prenons en considération la critique de Desmedt à l'égard de la PCCIP.

Nous avons déjà décelé certains experts dans la section 2.2, et en particulier Winn Schwartau (1994). Ce dernier a manifestement influencé l'écriture de la PCCIP. En plus d'avoir été consulté, il considère les infrastructures essentielles comme la cible principale des cyberterroristes. Il le fait principalement en affirmant que la principale force, mais aussi la plus grande vulnérabilité des États-Unis résident dans son économie. Celle-ci est dépendante des nouvelles technologies, en particulier des ordinateurs de même que des réseaux informatiques, et il soutient que si les réseaux ne fonctionnent plus, l'économie des États-Unis s'écroule et « we will literally die. » (Ibid., p.54). Cet énoncé est très intéressant dans la mesure où il constitue un acte de langage. L'utilisation de l'expression *we will literally die*

indique un contexte qui nécessite une réaction immédiate des autorités. L'inaction se solderait par une situation qui mettrait la survie des États-Unis en péril. Malgré qu'il identifie les cyberterroristes comme un des ennemis, nous soutenons qu'il a essayé une sécurisation sur l'ensemble des cybermenaces, car la menace du cyberterrorisme n'est qu'une possibilité parmi tant d'autres. Par conséquent, ce qui importe pour Winn Schwartau ce n'est pas de déterminer qui est une menace pour les infrastructures essentielles, mais de convaincre le gouvernement, mais aussi le reste de la population, de la nécessité de les protéger.

Schwartau semble avoir été entendu par le gouvernement. Alors que nous l'avons déjà souligné dans cette section, la PCCIP identifie l'ennemi et ce qui est menacé de la même manière que le font Winn Schwartau et le rapport *Computer at Risk*. Toutefois, il ne réussit pas dans sa tentative de sécurisation, car le gouvernement ne prend pas d'action à l'extérieur des normes établies. Dans ces circonstances, la protection des infrastructures essentielles va se dérouler selon les procédures normales en vigueur selon la Constitution états-unienne, et non dans l'urgence. Des études ont été commandées, les actes retenus ont été proposés aux organes décisionnels et la problématique a été débattue au grand jour.

Il nous semble important d'examiner la contribution des experts qui n'ont pas collaboré à la PCCIP. Ils ont peu contribué aux thèmes abordés. Effectivement, les termes *cyberterrorism* et *computer terrorism* ont été très peu étudiés dans les publications scientifiques ou les livres, car ils intéressaient principalement les juristes. Ces derniers s'intéressent aux types de crime informatique et aux difficultés légales de mise en accusation (Ciongoli, DeMarrais et Wehner, 1994). Il y a aussi un mémoire traitant du cyberterrorisme intitulé *Information Age Terrorism : Toward Cyberterror* (Littleton, 1995) qui explore l'implication de l'apparition des ordinateurs et d'Internet sur les méthodes employées par les terroristes. Il décrit surtout les outils informatiques que pourraient utiliser les terroristes. Il ne spécifie pas ce que les terroristes pourraient cibler. Ce texte n'a donc pas vraiment de lien avec la PCCIP.

Aussi, il existe une multitude de textes de cette période qui traitent de procédures de cryptage et de transfert de données ainsi que de la protection de systèmes informatiques gouvernementaux ou de grandes entreprises. Toutefois, aucun de ces textes ne mentionne le cyberterrorisme ou le terrorisme traditionnel et ils n'indiquent pas si les systèmes des infrastructures essentielles sont menacés. En fait, ils considèrent que tous les systèmes informatiques sont à risque et désirent apporter des solutions à ce problème. Ces articles ne correspondent pas aux idées stipulées dans la PCCIP.

Walter Laqueur qui est l'un des auteurs les plus prolifiques en ce qui concerne le terrorisme en général, s'intéresse un peu au concept du cyberterrorisme. Selon lui, les cyberattaques pourraient devenir l'arme du futur des terroristes (Laqueur, 1996). Il considère qu'elles pourraient faire plus de dommages qu'une attaque traditionnelle lorsqu'il dit : « Why assassinate a politician or indiscriminately kill people when an attack on electronic switching will produce far more dramatic and lasting results? » (Ibid., p. 35). Aussi, il fait allusion à une source anonyme des services d'espionnage du gouvernement des États-Unis, qui lui a déclaré qu'il serait possible pour un groupe terroriste composé de vingt pirates informatiques et d'un milliard de dollars, de mettre hors fonction l'économie états-unienne. Dans cette optique, il mentionne que les vulnérabilités de l'État et de la société états-unienne sont d'ordre économique et qu'elles intéresseront les criminels plutôt que les terroristes. De plus, ce texte traite en surface le cyberterrorisme, il s'intéresse beaucoup plus à l'utilisation de l'Internet pour obtenir des informations afin d'organiser un attentat terroriste au sens traditionnel du terme. Alors, il mentionne, vaguement ce qui est menacé soit l'économie états-unienne. Donc, il n'indique pas spécifiquement les infrastructures essentielles comme ce qui est ciblé. Dans ces circonstances, il est peu probable qu'il ait influencé directement le contenu de la PCCIP.

En somme, la PCCIP définit le cyberterrorisme comme un danger potentiel. De plus, elle distingue ce qui est menacé par le cyberterrorisme, mais aussi les cybermenaces en général : les infrastructures essentielles. En ce qui concerne les experts de la sécurité, seule une minorité d'entre eux dont fait partie Winn Schwartau a participé et a influencé la rédaction de

la PCCIP. Toutefois, ces experts n'ont pas été en mesure d'imposer le cyberterrorisme comme une menace plus importante que les autres cybermenaces. Par conséquent, la portée du cadre diagnostique du cyberterrorisme est réduite.

2.4 Le cadre diagnostique du cyberterrorisme pendant la période de 1997-2001

Nous allons maintenant nous pencher sur la période de 1997 à 2001, avant les attentats du 11 septembre. Nous soutenons que, durant cette période, le cadre diagnostique du cyberterrorisme de l'administration états-unienne n'a pas été fondamentalement modifié. Aussi, nous croyons que les experts de la sécurité n'ont pas influencé ce cadre.

2.4.1 Le cas du gouvernement

Premièrement, le cadre diagnostique du cyberterrorisme a continué à être réitéré après la PCCIP dans les documents officiels. Ces documents identifient systématiquement les ennemis pouvant utiliser des cyberattaques de façon très large. Par exemple, le cyberterrorisme est toujours présent et cité de pair avec les États étrangers (Etats-Unis, General Accounting Office, 2001b). Aussi, certains documents officiels comme, par exemple, le *National Plan for Information Systems Protection,* affirment que des groupes terroristes ont toujours employé des méthodes physiques lors de leur attentat (États-Unis, White House, 2000b). Donc, l'apparition d'Internet leur permettrait de lancer des cyberattaques. En fait, le gouvernement ne sait pas si les terroristes vont utiliser le cyberespace pour mener des cyberattaques. Il écrit : « *The rise of networks is likely to reshape terrorism in the information age and lead to the adoption of netwar [...]* » (Ibid., p. 9). Le vocabulaire exprimant l'incertitude pour qualifier le cyberterrorisme est encore utilisé ici. Le mot *likely* soutient que l'utilisation du cyberespace par les terroristes n'est pas une certitude. Dans la même ligne d'idée, l'expression *information age* fait référence à l'idée que les États-Unis sont dans une nouvelle époque et une dynamique nouvelle. Ceci vient renforcer l'idée que le terrorisme peut lui aussi avoir évolué et qu'il faut prendre cette menace au sérieux. De plus, nous

remarquons que le gouvernement considère encore la possibilité d'une attaque faite par un individu ayant un accès légitime aux systèmes informatiques des infrastructures essentielles (League et coll., 1997). Nous retrouvons le concept d'ennemi intérieur. Ce dernier n'est pas nouveau, il était présent auparavant dans le *National Security Decision Directive Number 145* (NSDD-145) (États-Unis, National Security Council, 1984).

Avant de continuer, nous désirons expliciter le concept « d'ennemi intérieur ». Ayse Ceyhen spécifie que cette appellation indique : « que l'ennemi est transnational et se déplace de l'extérieur vers l'intérieur et/où qu'il est déjà infiltré soit clandestinement soit de façon légale sur le territoire américain » (2004b, p. 118). Comme le fait remarqué Ayse Ceyhan et Gabriel Périès, cette définition permet d'observer que la catégorisation d'un ennemi intérieur est toujours imprécise et il n'est pas directement identifiable (2001). Elle ne permet pas de discerner spécifiquement où il se situe exactement. Cette indétermination octroie aux politiciens et aux experts la possibilité d'affirmer que l'ennemi est plus menaçant, c'est-à-dire qu'ils peuvent l'exposer comme un plus grand danger pour le pays. Selon le contexte dans lequel cette expression est utilisée, l'adversaire est représenté différemment. Il peut désigner l'immigrant, le terrorisme, le traître et le communiste pour n'en nommer que quelques-uns (Ibid.). Finalement, ce concept n'est pas nouveau. Le sénateur McCarthy, président du comité du Sénat américain sur les opérations gouvernementales, lors de sa croisade contre les communistes, a identifié toutes personnes soutenant le communisme comme un adversaire à la nation. Plus exactement, il a affirmé que ces citoyens étaient des traitres et qu'ils corrompaient la nation de l'intérieur (Viltard, 2001).

Cela nous indique que le concept du cyberterrorisme existe dans les textes du gouvernement des États-Unis. Toutefois, la conceptualisation du cyberterrorisme est plutôt embryonnaire. De plus, le gouvernement ne peut pas affirmer avec certitude que les groupes terroristes ont une réelle volonté d'entreprendre des cyberattaques. Cela ne lui permet pas de distinguer le cyberterrorisme comme une menace prioritaire. C'est donc une cybermenace théorique parmi tous les autres. Dans cette optique, le gouvernement n'a pas mis en place un

cadre diagnostique contenant le cyberterrorisme comme menace précise aux infrastructures essentielles.

Deuxièmement, l'identification de ce qui est ciblé est semblable à la PCCIP. Ces documents réitérèrent ce que la PCCIP a déjà souligné ou ils ne font que dégager de nouvelles vulnérabilités des infrastructures essentielles. Par exemple, les *National Security Strategy* publiées de 1997 à 2000 considèrent toujours les infrastructures essentielles comme menacées, physiquement ou virtuellement, et font de leur protection une priorité nationale (États-Unis, White House, 1997; 1998; 1999; 2000). C'est un changement important dans la stratégie nationale des États-Unis. Dans le *National Security Strategy* de 1995 et celui de 1996, le concept d'infrastructures essentielles est utilisé pour désigner les bases militaires états-uniennes nécessaires pour les opérations à l'étranger (White House, 1995; 1996). À partir du National Security Strategy de 1997, les infrastructures essentielles correspondent à celles identifiées dans la PCCIP (White House, 1997). Aussi, vers la fin du *National Security Strategy* de 1995, il est mention de la nécessité d'étudier les conséquences des nouvelles technologies pour les intérêts des États-Unis (Ibid.). Dans le même ordre d'idées, le *Presidential Decision Directives 62* indique que les terroristes vont peut-être tenter d'atteindre l'économie ainsi que les infrastructures essentielles des États-Unis à l'aide de systèmes informatiques sophistiqués (White House, 1998b).

Nous avons remarqué une différence notable dans les documents de cette période comparativement à la précédente, celle-ci est l'utilisation de scénarios afin de démontrer la vulnérabilité des infrastructures essentielles. Ceux-ci sont très peu explicités et vagues. Pour étayer ce point, citons *le Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* qui affirme: « These groups could damage the system so severely that major cities, or multistate regions, could suffer severe, long-term energy shortages » (États-Unis. Transition President's Commission on Critical Infrastructure Protection et Critical Infrastructure Assurance, 1998, p.28). Ce scénario d'attaque sur une installation électrique n'indique pas la méthode utilisée pour déjouer la sécurité du système électrique. Aussi, il est basé sur des évènements catastrophiques qui ne se sont jamais

produits. Il est donc fondé sur des hypothèses et des incertitudes comme le témoigne l'utilisation du mot *could.*

Dans le même ordre d'idées, plusieurs agences et départements du gouvernement des États-Unis, ainsi que certains fournisseurs d'infrastructures essentielles privées, ont participé à un exercice de sécurité appelé *Eligible Receiver.* Celui-ci avait pour objectif de déterminer si le système informatique des États-Unis était sécuritaire. Bien que les résultats sont, en grande partie, confidentiels, l'exercice a confirmé que l'équipe de pirates avait été en mesure de prendre les commandes de plusieurs ordinateurs, incluant le *U.S. Pacific Command,* ainsi que le réseau 911 et d'électricité de neuf villes principales aux États-Unis (Globalsecurity.org, (n.d.); Hildreth, 2001). Cette simulation a illustré à nouveau la vulnérabilité virtuelle des infrastructures essentielles.

Aussi, le gouvernement affirme que le cyberterrorisme est de plus en plus dangereux, car la disponibilité des outils a augmenté sensiblement (White House. 2000b). Cet argument n'est pas nouveau, puisque nous le retrouvons dans la PCCIP. Il est seulement présenté sous une autre forme, celle du scénario. Toutefois, ceux-ci sont utilisés pour démontrer les dangers que courent les infrastructures essentielles ainsi que ces effets sur la sécurité de l'État et de ses citoyens. D'autant plus que les textes officiels expriment une inquiétude par rapport à l'incapacité des autorités à prévenir les brèches de sécurité de plus en plus nombreuses (Etats-Unis, General Accounting Office, 2001). Finalement, le cadre diagnostique ne change pas, les scénarios ne servent qu'à illustrer ce qui était déjà établi dans le cadre précédent.

En somme, les textes subséquents à la PCCIP amènent peu d'éléments nouveaux. En fait, l'identification de l'ennemi reste identique. Ils mentionnent le cyberterrorisme, mais ils s'intéressent principalement aux cybermenaces dans une perspective de protection des infrastructures essentielles. La seule nouveauté est l'introduction de scénarios afin d'illustrer les risques que courent les infrastructures essentielles et de démontrer leur interdépendance.

2.4.2 Le cas des experts de la sécurité

En ce qui concerne les textes publiés par des experts de la sécurité durant cette période, ils sont un peu plus nombreux. La séparation des experts en deux camps peut être constatée au cœur de ce laps de temps. Avant de continuer, nous allons résumer les arguments de ces deux factions.

Le premier camp soutient que le cyberterrorisme constitue une menace réelle pour les États-Unis. Ils exposent que les États occidentaux sont plus dépendants des technologies. Cette dépendance viendrait du fait que la plupart des services essentiels sont gérés par un amalgame d'ordinateur et de réseaux informatiques (Verton, 2003). Dans ces conditions, ils considèrent que les infrastructures essentielles sont de plus en plus menacées et vulnérables à une cyberattaque terroriste (Ashley, 2003; Nugent et Raisinghani, 2007; Schneidewind, 2007). De plus, ils craignent l'effet domino. Cet effet se produit lorsqu'une catégorie d'infrastructure essentielle est mise hors fonction. En effet, l'arrêt de cette dernière a un effet d'entrainement sur les autres catégories d'infrastructures essentielles. La mise hors fonction d'une catégorie d'infrastructure essentielle provoque l'arrêt de l'ensemble des infrastructures essentielles. Elles sont donc interdépendantes entre elles (Verton, 2003). Par conséquent, la mise hors fonction d'un seul secteur d'infrastructure essentielle constitue un danger pour la totalité du système d'infrastructure, et par la même occasion, menace la santé physique et financière de la nation tout entière.

Le deuxième camp soutient que le cyberterrorisme est faisable théoriquement, mais peu réaliste et que c'est une méthode moins viable que celles utilisées par le terrorisme traditionnel. Ils croient qu'il y a une supervision et une gestion adéquate des opérations des infrastructures essentielles par des êtres humains et que le cyberterrorisme ne pose pas de risque important à ces infrastructures (Denning, 1999; Embar-Seddon, 2002). Giampiero Giacomello, quant à lui, démontre à l'aide d'une analyse économique de type coût-bénéfice que le cyberterrorisme est moins efficace que son homologue traditionnel (2004).

Il est important de retenir qu'aucun expert ne croit que le cyberterrorisme est une menace imaginaire. Certains experts comme Winn Schwartau indiquent que le cyberterrorisme est un danger imminent et viennent renforcer le cadre diagnostique du cyberterrorisme établi par la PCCIP et les documents connexes. D'autres experts, comme Dorothy Denning, ne considèrent pas le cyberterrorisme comme une menace immédiate. Ils croient que le terroriste traditionnel est encore la menace la plus réelle que les États-Unis ont à affronter (Denning, 1999).

La situation est différente en ce qui concerne l'identification de ce qui est menacé. La totalité des experts analysés considère que les infrastructures essentielles sont menacées par divers acteurs incluant les groupes terroristes. La différence réside dans la façon dont elles sont menacées. Les deux courants mentionnés plus haut ont deux visions différentes. Le premier juge qu'ils sont menacés par des attaques exclusivement physiques. Les experts du premier courant de pensée croient que l'utilisation d'Internet par les groupes terroristes se restreint à une méthode de communication et de collecte d'information. Le deuxième estime qu'ils sont menacés par des attaques physiques et virtuelles. La composante informatique devient donc une arme.

Peu importe la position des experts, le fait qu'ils affirment que les infrastructures essentielles sont menacées par des groupes terroristes contribue au renforcement du cadre diagnostique. En effet, ils se retrouvent en face du dilemme normatif de la sécurité tel qu'énoncé par Jef Huysmans, qui écrit : « [...] dire la sécurité n'est jamais un acte innocent ou neutre. » (1998). Il est intéressant de s'attarder un peu à ce dilemme, car tout individu qui dit ou écrit sur le sujet de la sécurité y est confronté. Le dilemme est résumé comme ceci par Huysmans :

> En résumé, le dilemme normatif auquel est confrontée cette position constructiviste repose sur la compréhension des effets de communication au sein d'une formation de règles construites socialement, qui restreignent le discours d'un auteur dans son émission et dans sa réception. L'analyste dépend lui-même du langage de la sécurité, et il doit en tenir compte lorsqu'il souhaite transformer la sécurisation d'un domaine à partir des études de sécurité. Son désir de transformation, de critique, se heurte en effet au risque d'accroître la sécurisation dans un domaine, car la formation discursive de la sécurité est à la fois la contrainte et le pouvoir qui autorise un auteur à émettre des énoncés dans un domaine sécurisé. (Ibid., p. 182).

Donc, le seul fait de parler d'un enjeu sécuritaire risque de contribuer à sa sécurisation, peu importe l'opinion, défendue. Comme le démontre Huysmans, malgré les tentatives de Waever et de Bigo de passer outre ce dilemme, il reste toujours présent. Le chercheur n'a d'autre choix que d'être conscient de son influence sur le champ sécuritaire et de tenter de réduire son influence sur ce dernier (Ibid.) Le seul fait de parler du danger qui guette les infrastructures essentielles contribue à sa sécurisation. Cela a pour conséquence une résurgence de l'intérêt pour la protection physique et virtuelle des infrastructures essentielles entre les experts de la sécurité. Certains ont tenté de démontrer qu'ils sont relativement bien protégés tandis que d'autres ont dénoncé leur vulnérabilité, mais tous ont discuté des infrastructures essentielles.

Nous identifions un élément redondant durant cette période soit l'utilisation de scénarios. Ces derniers ont plusieurs fonctions. Dans un premier temps, ils permettent de reconnaitre ce qui est menacé par les cyberterroristes, c'est-à-dire les infrastructures essentielles. La différence principale, entre les textes de cette époque et ceux qui les précèdent, est la distinction entre les cinq catégories d'infrastructure soit l'information et la communication, les réseaux de transports, l'énergie, les services financiers et bancaires et les services vitaux à la personne. Les textes de cette époque vont mettre l'accent sur une catégorie d'infrastructures lors de l'élaboration de ces scénarios.

Dans un deuxième temps, cette distinction, entre les différentes catégories d'infrastructures essentielles, va permettre aux experts de la sécurité de bâtir des scénarios

plus réalistes et va établir la priorité à certains secteurs comparativement à d'autres. C'est ce que fait John Arquilla dans *The Great Cyberwar of 2002* (1998). Ce dernier représente une attaque informatique d'un ennemi invisible sur diverses infrastructures essentielles. Premièrement, il décrit un assaut sur le système électrique du pays tout entier. Par la suite, il raconte qu'un accident aérien causant plus de 400 morts serait attribuable à ces pirates. Puis, une bombe à impulsion électromagnétique exploserait dans la ville de Washington rendant inutilisable toute forme d'objet électronique. Tous ces évènements se déroulant à quelques jours d'intervalle démontrent la vulnérabilité et la dépendance des États-Unis vis-à-vis des systèmes informatiques et les infrastructures essentielles. De plus, ce récit illustre le danger qu'occasionne un ennemi invisible et inconnu, voire intouchable. Pour illustrer cette idée, il utilise un vocabulaire évoquant l'incertitude pour qualifier le cyberterrorisme. Par exemple, alors que les protagonistes ne sont pas certains de l'auteur des attentats, il écrit : « All that still murky. » (Ibid., p. 4). Le mot *murky* réfère à l'idée de noirceur, il est impossible de discerner avec certitude ce qu'il regarde. Par la suite, les États-Unis croient que la Chine et la Russie sont derrière ces attentats et veulent utiliser un arsenal nucléaire contre ces derniers. À ce moment, l'auteur s'interroge sur les répercussions des évènements de la journée. Il se demande : « [...] Could this lead to World War III ? » (Ibid., p. 7). Cette phrase renvoie aux deux guerres mondiales et à leurs conséquences désastreuses pour l'humanité. Aussi, le mode de vie des états-uniens serait bouleversé. Dans cette optique, il est primordial que les États-Unis se prémunissent contre les cybermenaces. À la fin de l'histoire, le cumul de tous les évènements amène un sentiment d'insécurité et de terreur chez la population.

Ce scénario n'est pas isolé. D'autres parviennent à des conclusions équivalentes. Un documentaire de la chaîne de télévision Fox intitulé *Dangers on the Internet Highway : Cyberterror* arrive aux mêmes conclusions malgré une différence importante dans l'histoire (Debrix, 2008). En fait, il précise que l'ennemi est des cyberterroristes. Pour le reste, ces scénarios sont à peu près identiques.

Nous relevons dans ces deux scénarios une tentative de sécurisation, car les deux s'efforcent de démontrer la vulnérabilité des infrastructures essentielles. Ils identifient

l'ennemi comme les cybermenaces en général. Les différents documents gouvernementaux, tels que la PCCIP, définissent déjà ces menaces et ses vulnérabilités, ce qui lui donne une légitimité. De plus, ces scénarios sont vulgarisés ce qui offre une meilleure accessibilité pour le reste de la population. Finalement, les médias utilisés permettent de rejoindre une plus importante partie du peuple qu'un rapport officiel du gouvernement. Nous pouvons affirmer que le cadre diagnostique du cyberterrorisme des experts de la sécurité est clair et bien établi.

Pour conclure cette section, les experts de la sécurité n'ont pas apporté, au cours de cette période, de nouveaux éléments importants dans le cadre diagnostique. Ils ont simplement repris les arguments qui se retrouvent dans la PCCIP. Leur apport est au niveau des scénarios possibles d'attaque et des méthodes qui pourraient être utilisées.

2.5 Le cadre diagnostique du cyberterrorisme après les évènements du 11 septembre

Les évènements du 11 septembre 2001 ont ébranlé les États-Unis. La question du terrorisme est devenue un élément central de la majorité des débats. De nombreuses lois ont été proposées et acceptées pour lutter et se protéger contre la menace du terrorisme. Dans cette optique, il est impératif de se questionner sur l'effet de ces évènements sur le cadre diagnostique du cyberterrorisme. Nous soutenons que les attentats du 11 septembre 2001 n'ont pas modifié sensiblement le cadre diagnostique et que les experts de la sécurité, malgré leurs efforts, n'ont pas réussi à l'influencer de manière substantielle.

2.5.1 Le cas du gouvernement

Le président George W. Bush indique que les évènements du 11 septembre ont prouvé la nécessité d'améliorer la protection des infrastructures essentielles et de lutter contre le terrorisme (États-Unis, White House, 2001; 2001b). Le gouvernement des États-Unis a établi donc avec *l'Executive Order 13 228* (EO 13228) intitulé *Establishing the Office of Homeland*

Security and the Homeland Security Council, un nouvel organe pour combattre et protéger les États-Unis contre le terrorisme (White House, 2001). Ce document n'offre aucun apport au cadre diagnostique dans la mesure où il ne cible pas d'ennemi. De plus, la seule mention de ce qui pourrait être menacé est au sujet des infrastructures essentielles. Alors, la spécification de ce qui est menacé est la même que celle mentionnée dans la PCCIP, il n'y a aucun nouvel élément. La situation est identique avec l'*Executive Order* 13 231 (EO 13231), *Critical Infrastructure in the Information Age* (White House, 2001b). Il modifie plutôt l'organisation du gouvernement et continue à spécifier les différents rôles des départements et agences au niveau de la lutte contre le terrorisme. Néanmoins, ces documents sont importants, car ils mettent en place le *Department of Homeland Security* qui devient le nouvel organe principal pour la lutte contre le terrorisme aux États-Unis.

En ce qui concerne la détermination de l'ennemi, la conception de ce dernier apparaît toujours très large. Elle cible les terroristes, peu importe, le lieu de résidence. Ceci inclut donc le terrorisme intérieur. Néanmoins, il y a un nouveau détail qui semble s'ajouter à ce cadre. En fait, le gouvernement Bush, après le 11 septembre, a commandé et rédigé de nombreuses études sur la capacité des groupes terroristes musulmans à commettre des actes de cyberterrorismes (National Infrastructure Protection Center, 2002; Dartmouth College, 2003; Vatis, 2001).

Malgré ces études, nous croyons que la religion musulmane ne fait pas partie du cadre diagnostique du cyberterrorisme, car aucun document officiel ne condamne que les actes terroristes effectués par des musulmans. La ligne directrice du gouvernement des États-Unis a toujours condamné tous les types de terrorisme. Nous estimons que les attentats du 11 septembre ont forcé les autorités à évaluer prioritairement les cybercapacités des groupes terroristes musulmans. Cela s'explique par le fait que les attentats du 11 septembre ont été effectués par eux. De plus, le gouvernement états-unien a une présence militaire en Afghanistan et en Irak, deux pays majoritairement musulmans et qui sont, historiquement, des lieux à haut taux de groupes terroristes. Les États-Unis ont préféré opter pour une politique préventive afin d'analyser leurs capacités.

En ce qui concerne l'identification de ce qui est menacé, les documents officiels considèrent toujours que les infrastructures essentielles sont ciblées et ils réitèrent les mêmes éléments que la PCCIP. Par exemple, le *National Strategy to Secure Cyberspace* de 2003 a pour objectif principal de prévenir les cyberattaques sur les infrastructures essentielles (États-Unis, White House, 2003b). Toutefois, de nouveaux éléments se rajoutent.

Premièrement, la liste des infrastructures essentielles ne cesse de s'accroître. Par exemple, le *Department of Homeland Security* avait identifié 160 infrastructures essentielles avant l'opération *Iraqui Freedom* du 19 mars 2003. En 2006, ce registre atteignait plus de 77 000 sites (Moteff, 2007; Moteff 2008, p.25). Cet exemple prouve que la détermination de ce qui est menacé est toujours très large. Aussi, la croissance de cette liste démontre un changement dans la sélection de ce qu'est une infrastructure essentielle. Au commencement, le gouvernement états-unien les définissait comme toutes installations dont la mise hors d'état à long terme provoquerait des dangers aux plans militaire et économique. Suite aux évènements du 11 septembre, cette définition a changé. Maintenant, elle intègre les monuments nationaux, les lieux qui pourraient occasionner de grandes pertes humaines, ainsi que les sites qui causeraient une baisse importante du moral de la nation (Moteff, 2008).

Deuxièmement, ils mettent l'accent sur la protection physique des infrastructures essentielles par la voie de la protection informatique. En d'autres mots, ils soutiennent qu'une cyberattaque peut être effectuée dans le but de les affecter physiquement. Par exemple, déverrouiller une porte fermée magnétiquement, ou obtenir des informations afin de pouvoir mener une attaque traditionnelle (Moteff, 2007). C'est un changement fondamental dans le cadre diagnostique du cyberterrorisme, mais aussi des cybermenaces en général.

Nous expliquons une partie de ces changements par les attentats du 11 septembre. Ces derniers ont créé un traumatisme national. Presque tous les textes officiels font mentions de cet évènement historique pour justifier des mesures ou recommandations en matière de sécurité. Richard Jackson a remarqué la forte utilisation de cet évènement dans les discours

du gouvernement (2005). Dans cette optique, le renouveau de l'importance de la protection physique des infrastructures essentielles est attribuable à l'attaque physique sur le World Trade Center. De plus, les pertes humaines expliquent la nouvelle importance des lieux où une attaque pourrait en occasionner beaucoup. L'intégration des monuments nationaux est rationnelle dans la mesure où le World Trade Center était un symbole de la puissance économique états-unienne. Sa destruction a causé, pour une courte durée, une baisse de moral dans la population.

Nous avons remarqué que la problématique des cybermenaces est apparue et a progressé presque exclusivement sous l'administration Clinton. À première vue, nous sommes tentés d'affirmer que les attentats du 11 septembre ont participé à la réduction de la priorité des cybermenaces pour le gouvernement Bush. Un bon indicateur de cette conclusion est l'absence du préfixe *cyber* dans le *National Security Strategy* de 2002 (États-Unis. White House). De plus, le gouvernement Bush semble avoir décidé de réduire l'importance accordée à la protection des infrastructures essentielles, car le *National Security Strategy* de 2006 ne mentionne plus la protection des infrastructures essentielles comme une de ses priorités de sécurité nationale (États-Unis. White House).

Toutefois, de nombreux documents gouvernementaux ont été publiés sur le danger des cybermenaces et sur la protection physique et virtuelle des infrastructures essentielles. Deux d'entre eux retiennent notre attention : *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (États-Unis. White House, 2003b) et *The National Strategy to Secure Cyberspace* (États-Unis. White House, 2003b). Ces derniers poussent la réflexion de la protection des infrastructures beaucoup plus loin que l'a fait l'administration Clinton en divisant la problématique. En fait, chaque document va traiter uniquement d'un seul niveau de protection. Dans cette optique, le gouvernement concède que les infrastructures essentielles sont menacées de façon physique, mais aussi de manière virtuelle.

En ce qui concerne le cyberterrorisme, le gouvernement états-unien ne fait pas allusion à ce concept spécifiquement. De plus, les évènements du 11 septembre ont ravivé l'intérêt du

gouvernement à lutter contre le terrorisme. Il est vrai que ce dernier se concentre beaucoup sur la menace du terrorisme conventionnel. En effet, comme le démontre Richard Jackson dans son ouvrage *Writing the War on Terrorism*, le gouvernement a construit une représentation de la menace terroriste en lien avec les évènements du 11 septembre et sa politique de lutte contre le terrorisme. Selon lui, le gouvernement présente les terroristes comme des : « [...] highly sophisticated, cunning and extremely dangerous killers. » (Jackson, 2005, p. 108). Bien qu'ils soient sophistiqués, l'utilisation du cyberespace, à l'exception de son usage pour la communication, n'est pas présente.

Toutefois, les cybermenaces sont encore d'actualité et le gouvernement accomplit des gestes pour réduire les vulnérabilités virtuelles de ses infrastructures. Par conséquent, nous soutenons que le gouvernement continue de porter une grande attention aux cybermenaces et un peu au cyberterrorisme implicitement. Ainsi, nous croyons qu'il n'a pas tenté de faire du cyberterrorisme un enjeu de sécurité. Donc, nous maintenons que le cyberterrorisme est toujours une situation politique traitée de façon normale, c'est-à-dire que le gouvernement continue à gérer la situation en suivant les protocoles établis et en ayant un débat public sur les mesures prises. Nous soutenons que les évènements du 11 septembre n'ont pas eu d'incidence directe sur la menace du cyberterrorisme, mais qu'ils ont permis de réaffirmer la nécessité d'améliorer la protection des infrastructures essentielles.

2.5.2 Le cas des experts de la sécurité

En ce qui concerne les experts de la sécurité, le cadre diagnostique qu'ils proposent est très semblable à celui de la période précédente. Pour cette raison, nous allons nous concentrer sur les différences. Un des éléments que nous avons relevé est l'intérêt accru à l'égard des terroristes d'origine musulmans. Comme le gouvernement, les attentats du 11 septembre ont attiré l'attention des experts sur ces groupes. Toutefois, contrairement au gouvernement, les experts de la sécurité n'ont pas cessé de s'intéresser aux cybermenaces. Nous affirmons que les attentats du 11 septembre leur ont permis de se concentrer sur le cyberterrorisme parce

que la majorité des livres traitants du cyberterrorisme à la disposition de la population ont été écrits après ces évènements. Aussi, nous croyons que le manque d'intérêt du gouvernement Bush au sujet des cybermenaces les a forcés à s'intéresser et à s'exprimer sur cette problématique.

Nous pouvons prendre l'exemple de *Black Ice* de Dan Verton (2003). Il soutient la thèse que les États-Unis, par le biais de leurs infrastructures essentielles, sont menacés par le cyberterrorisme. Ces cyberterroristes peuvent être d'origine musulmane, mais il ne restreint pas son analyse à ces derniers malgré l'intérêt évident qu'il porte à Al-Qaïda. Aussi, Verton essaie de démontrer, à l'aide de scénarios, que l'interdépendance des infrastructures essentielles est une vulnérabilité que les ennemis des États-Unis tenteront d'exploiter. Son argument repose sur l'effet domino que nous avons évoqué dans la section 2.4.2. Il correspond à la mise hors fonction d'une catégorie d'infrastructures essentielles qui aurait pour action la neutralisation de l'ensemble des infrastructures. La conséquence finale est des dommages physiques et économiques importants, un arrêt de tous les services essentiels, un état de panique dans la population ainsi que des décès reliés à cette perturbation.

Black Ice est l'exemple le plus connu et le plus cité dans les médias de l'utilisation de scénarios et de simulations pour pointer la menace du cyberterrorisme. Curieusement, c'est le seul à utiliser des métaphores de phénomènes naturels pour qualifier le cyberterrorisme. Il compare la difficulté et le danger de ne pas être en mesure de voir les changements de tactiques des terroristes à un séisme. En effet, il écrit : « [...] we can be caught by surprise by a massive, life-threatening earthquake when we fail to pick up on the subterranean changes in terrorism. » (Ibid, p. xix). Il désigne une autre cyberattaque en utilisant encore la métaphore du tremblement de terre pour qualifier ces effets négatifs. Il écrit : « *This time, the chaos, confusion, and fear would surge outward from the epicenter of the main attack like a digital shockwave from an earthquake.* » (Ibid., p. 2).

D'autres auteurs comme Bradley Ashley (2003) utilisent des scénarios et des exercices pour démontrer le danger du cyberterrorisme. Les leurs sont construits avec l'objectif de

désigner une situation comme problématique et de tenter de conscientiser la population et le gouvernement. Ils ont réussi en partie. Nous estimons, comme Maura Conway, que les experts de la sécurité, avec l'aide des médias, ont réussi à créer un cadre diagnostique du cyberterrorisme et à ciblé les infrastructures essentielles comme ce qui est menacé (2008). Néanmoins, seule la population a accepté ce cadre. Des sondages nous montrent que près de la moitié des citoyens états-uniens ont peur du cyberterrorisme et qu'ils croient que la cible des cyberterroristes serait les infrastructures essentielles (Ibid.). Aussi, nous soutenons que les experts de la sécurité ont réussi à toucher à l'imaginaire collectif de la population des États-Unis à l'aide de plusieurs productions culturelles comme le film *Live Free or Die Hard* (Wiseman, 2007) et la 7e saison de *24 heures chrono* (Surnow, Cochran, 2008), qui sont basées sur ces scénarios, c'est-à-dire sur des attentats de cyberterroristes faits contre des infrastructures essentielles. Aussi, de nombreux romans de fiction souvent écrits par des auteurs très connus ont fait leurs apparitions. Par exemple, *Cyberterror* de R.J. Pineiro, *Storm* de Dave Pearson, *Power plays : Cutting edge* de Tom Clancy, *Unholy domain* de Dan Ronco, *Early warning* de Michael Walsh et de la série *Deep black* de Stephen Coonts. Finalement, nous avons même trouvé un livre intitulé *Careers as a Cyberterrorism Expert* par Jason Porterfield. Tous ces exemples nous démontrent que certains produits culturels s'approprient le concept de cyberterrorisme.

Toutefois, le gouvernement ne semble pas avoir été influencé par ce cadre, car il conserve la même position sur le sujet. Dans cette optique, il est pertinent de trouver la raison de ce *statu quo*.

Cette raison est que le cyberterrorisme est une cybermenace parmi tant d'autres. L'administration états-unienne était intéressée, avant tout, à la protection physique, mais surtout virtuelle, des infrastructures essentielles. Par conséquent, ce qui le concerne le plus, ce n'est pas ce qui les menace, mais plutôt la façon de les protéger. Ainsi, le cyberterrorisme et les cybermenaces sont intéressants, car ils permettent de déterminer les menaces aux infrastructures, mais ce n'est pas la priorité. Dans cette optique, le gouvernement s'intéresse aux risques qui ciblent le cyberespace (*risks to cyberspace*) c'est-à-dire ceux qui visent les

installations informatiques et de communication ainsi que leurs réseaux. En d'autres mots, les infrastructures essentielles. Selon Ronald J. Deibert et Rafal Rohozinski, pour contrer ce type de risque, les États vont chercher à coordonner et à réguler les politiques pour rendre le cyberespace plus sécuritaire et plus stable ce qui favorise le développement social et économique d'un État (2010). Pour y arriver, la protection des infrastructures essentielles est primordiale. Les nouveaux risques sont ceux qui surgissent ou qui sont favorisés par le cyberespace (risk through cyberspace), mais qui ne ciblent pas nécessairement les infrastructures essentielles. Nous pensons notamment à la désobéissance civile, aux cybermenaces et au cyberterrorisme. Pour ce type de risque, la coopération et la mise sur pied de politiques pour lutter contre ce type de risque sont plus difficiles, car l'intérêt qu'un État leur porte varie selon ses valeurs et son intérêt national. Dans la mesure où le cyberterrorisme est encore une menace théorique et qu'il ne met pas concrètement en danger les infrastructures essentielles, le gouvernement à peu d'incitatifs pour faire du cyberterrorisme un enjeu de sécurité. Il préfère focaliser leur énergie pour mettre sur pied des mesures et des politiques concrètes pour réduire les risques qui ciblent le cyberespace (*risks to cyberspace*).

En somme, les experts ont permis au gouvernement de constater que les infrastructures essentielles étaient menacées. En ce sens, ils ont influencé le gouvernement en partie avec leur tentative de sécurisation. Toutefois, le gouvernement n'a jamais été influencé ou n'a pas tenté de faire du cyberterrorisme un enjeu de sécurité. Ce dernier a continué à être une cybermenace au même titre que le cybercrime et le piratage informatique.

CHAPITRE III

L'ÉVOLUTION DU CADRE PRONOSTIQUE DU CYBERTERRORISME AUX ÉTATS-UNIS

Dans ce chapitre, nous allons analyser l'évolution du cadre pronostique du cyberterrorisme aux États-Unis afin de déterminer si les experts de la sécurité ont réussi à influencer le gouvernement. Pour ce faire, nous utiliserons le cadre pronostique, c'est-à-dire un schéma d'interprétation qui permet aux individus de trouver des solutions pour protéger ce qui est menacé.

Également, nous soutiendrons que la principale stratégie soit la coopération entre le secteur public et le secteur privé présenté par les experts de la sécurité pour contrer le cyberterrorisme et pour protéger les infrastructures essentielles est celle déjà proposée par le gouvernement. De plus, le cadre pronostique n'a pas été bien établi par les experts de la sécurité, car les résultats de cette stratégie sont faibles.

3.1 L'influence de l'attentat d'Oklahoma City sur le cadre pronostique du cyberterrorisme

Nous soutenons que le gouvernement n'a pas tenté d'influencer le cadre pronostique du cyberterrorisme à l'aide du *Presidential Decision Directive 39*. En fait, il s'intéresse surtout au problème du terrorisme traditionnel, car il a été rédigé en réaction à l'attentat d'Oklahoma City. Alors, il n'amène pas de solution pour le cyberterrorisme. En ce qui a trait aux experts de la sécurité, nous n'avons pas été en mesure de mesurer leur influence sur le cadre pronostique.

3.1.1 Le cas du gouvernement

Le *Presidential Decision Directive* 39 (PDD-39) a pour objectif d'énoncer des politiques pour lutter contre toutes formes de terrorisme afin de protéger le territoire, la population ainsi que les infrastructures des États-Unis (White House, 1995). Elles sont au nombre de trois. La première est de réduire la vulnérabilité des États-Unis par rapport à des attaques potentielles en redéfinissant les rôles de certains départements et agences. La seconde est de réaffirmer que les politiques du gouvernement des États-Unis ne seront pas influencées par des menaces ou des actes de terroristes. La dernière politique est de mettre en place un mécanisme de coopération entre les différents départements et agences gouvernementales afin de lutter contre le terrorisme. Nous allons analyser ces politiques plus en profondeur.

La première est de réduire la vulnérabilité des États-Unis sous toutes ces formes, sur son territoire ou à l'étranger. Afin d'y arriver, le document assigne des tâches très précises à diverses entités gouvernementales. Ils devront s'assurer que les organisations sont bien structurées et financées pour lutter contre les actes de terrorisme selon leurs rôles respectifs. Cette politique devait mettre un terme à la lutte entre les différents départements et agences en ce qui concerne l'affectation des budgets pour combattre le terrorisme et les cybermenaces (Ibid.).

Toutefois, cela ne fut pas le cas. En fait, les institutions gouvernementales utilisent certains stratagèmes pour obtenir des budgets plus importants. L'un d'eux est de se doter d'un nouveau rôle. Dans ce cas-ci, c'est de lutte contre le terrorisme. Pour y arriver, elles ont défini le terrorisme selon leurs intérêts et cela leur a permis de justifier leur implication dans ce domaine. Une fois qu'elles ont eu un rôle à jouer dans la lutte contre le terrorisme, ces institutions gouvernementales ont réclamé des budgets supplémentaires. L'exemple du *Federal Bureau of Investigation* (FBI) est assez représentatif de ce propos.

En 1996, le FBI ouvre le *Computer Investigation and Infrastructure Threat Assessment Center*, car les crimes informatiques se multiplient. Il annonce qu'il va lutter contre les cybercrimes. Ce terme est intéressant parce qu'il est imprécis et peut se rapporter à toutes les actions électroniques illégales ou constituants une menace pour l'État. Il peut aussi comprendre le cyberterrorisme et la propagande pour ne donner que quelques exemples. La définition utilisée lui permet donc de dépasser le simple crime informatique pour englober plusieurs phénomènes tout à fait différents. En ce sens, elle enlève toute distinction entre le criminel et le terroriste (Bonditti, 2001).

Cette stratégie a été efficace, car elle a justifié des budgets beaucoup plus importants. Entre 1995 et 1998, le budget antiterroriste a plus que doublé, et ce, en grande partie à cause de la loi antiterroriste de 1996 (Ibid.). À propos de cette situation, le *General Accounting Office* (GAO) a dénoncé, à plusieurs reprises le manque de cohérence dans l'allocation et l'utilisation des budgets dédié à la lutte antiterroriste (États-Unis. White House, 2001c).

La deuxième politique a pour objectif de décourager les actes de terroriste en réaffirmant qu'ils ne modifieront pas les politiques du gouvernement. De plus, la politique précise que les gouvernements s'engagent à lutter vigoureusement contre les terroristes ainsi que leurs commanditaires en espérant ainsi réduire la capacité à commettre des attentats (Ibid.). Celle-ci n'est pas nouvelle, c'est une réaffirmation d'une ancienne politique. Nous la retrouvons dans toutes les stratégies nationales des États-Unis que nous avons analysées (White House, 1996 ; 1997 ; 1998 ; 1999 ; 2000 ; 2002 ; 2006). Par sa nature, l'État se doit de lutter et de se prémunir contre toutes menaces à sa survie. Le terrorisme fait partie de ces menaces.

Pour permettre à cette politique d'être efficace, les États-Unis réaffirment leur volonté de trainer en justice tout individu commettant un acte terroriste. Aussi, il précise qu'il demanderait l'extradition aux États-Unis de tout terroriste ayant violé une loi fédérale (White House, 1995). Dans cette optique, il nous est possible d'affirmer que les cyberterroristes pourraient être extradés et traduits en justice aux États-Unis.

Malgré la volonté des États-Unis de punir les terroristes, les individus commettant des actes de cyberterrorisme ou des cybercrimes en vue de mettre en place un attentat terroriste avaient peu de chance d'être inculpés. August Bequai, un juriste, mentionne que les chances d'être inculpé, dans les années 1990, pour du piratage et d'obtenir une peine de prison étaient de moins d'une chance sur dix mille (1999). Il y avait deux raisons principales expliquant ce faible taux. La première était que les victimes de cyberattaques ne reportaient pas les incidents aux autorités. En fait, plusieurs avaient peur de la mauvaise publicité d'un tel événement, des conséquences légales sur leur compagnie et du manque d'intérêt de la part des autorités. La deuxième était que la préparation d'un dossier de poursuite criminelle et les procès étaient très longs et coûteux pour les entreprises. De plus, à l'aide de petits détails techniques, les avocats de la défense étaient capables de prolonger une affaire judiciaire pendant plusieurs années. Un bon exemple a été le procès sur l'*Equity Funding Computer-Assisted Fraud*[6], qui a pris plus de dix ans, car il a fait plusieurs appels du verdict (Ibid.). Nous voyons que cette politique était inefficace. Elle était plutôt une déclaration visant le terrorisme traditionnel.

La troisième politique a pour objectif de permettre une réaction rapide et efficace contre une attaque terroriste à l'aide de la coopération entre les divers agences et départements gouvernementaux. Plus exactement, le document reflète la volonté, en spécifiant explicitement chacun des rôles des départements en matière de lutte contre le terrorisme, qu'ils respectent les fonctions de chacun (White House, 1995).

Pour ce faire, la troisième politique mentionne un *Federal Response Plan*. Plus spécifiquement, il se nomme le *Robert T. Stafford Disaster Relief and Emergency Assistance Act*. Ce dernier est un plan conçu pour intervenir lors de catastrophes ou de différents évènements qui pourraient survenir sur le territoire ou la population des États-Unis. En d'autres mots, c'est un plan de gestion des conséquences lors d'une catastrophe naturelle ou humaine.

---

[6] Le procès portait sur la vente de faux fond mutuel et d'assurance vie par la compagnie Equity Funding Corporation of America de 1960 à 1973. Le film, *Billion Dollar Bubble*, est basé sur ce procès (Gibson, 1978).

La première version de 1974 était très peu développée. Toutefois, le dirigeant de la *Federal Emergency Management Agency (FEMA)*, James Lee Witts, nommé par le Président Bill Clinton, l'a modifié sensiblement en 1992 en élargissant sa responsabilité à l'ensemble des dangers auxquels pourraient faire face les États-Unis. Par la suite, il a été amendé à plusieurs reprises pour prendre en compte les nouvelles menaces (2007). Par conséquent, il n'a pas été créé par le PDD-39, mais il a été amendé pour répondre à de nouvelles exigences.

Cette idée de la nécessité d'un renouveau de la coopération entre les différentes agences du gouvernement pour protéger les infrastructures essentielles de l'information et de la communication en vue de faire face aux nouvelles menaces a été reprise dans la stratégie nationale de sécurité de 1997. C'est la fin de la guerre froide qui a diversifié les menaces. Les États-Unis sont entrés dans une nouvelle ère. Dans cette stratégie, il est écrit : « [...] with the Cold War's end. Combating these dangers which range from terrorism [...] and intrusions in our critical information infrastructures requires far-reaching cooperation among the agencies of our government as well as with other nations. » (White House, 1997, p. 12).

En somme, le PDD-39 est un document proposant trois politiques. Elles ont pour objectifs d'enrayer la menace du terrorisme sur le territoire états-unien et de protéger les infrastructures essentielles. Nous remarquons que le document s'intéresse surtout aux menaces traditionnelles.

3.1.2 Le cas des experts de la sécurité

En ce qui concerne les experts de la sécurité, il nous est difficile de discerner leurs contributions dans le contenu du PDD-39, car les solutions offertes sont, pour la plupart, des réaffirmations de politiques qui existaient auparavant. Nous désirons aussi noter que le PDD-39 est encore en partie classifié. Cette situation nous cause des difficultés à distinguer leurs

apports au PDD-39. Dans ces conditions, nous ne pouvons pas dégager de conclusion par rapport à l'influence des experts de la sécurité sur celui-ci.

Pour conclure, le gouvernement affirme son intention de lutter contre toutes les formes de terrorisme et il met en place une stratégie pour protéger ses infrastructures essentielles avec la publication du PDD-39. Néanmoins, la stratégie s'adresse aux menaces traditionnelles principalement. Du côté des experts, nous sommes incapables de distinguer leur influence sur le PDD-39.

3.2 L'influence du *Presidential Commission on Critical Infrastructure Protection* sur le cadre pronostique du cyberterrorisme

Nous soutenons que la PCCIP a établi la stratégie de base pour protéger les infrastructures essentielles des États-Unis. Celle-ci est la coopération entre les secteurs public et privé. Pour leur part, certains experts de la sécurité ont participé à l'élaboration et ont influencé la rédaction du document. Toutefois, nous soutenons qu'ils n'ont pas proposé de solution ou de stratégie spécifiquement pour contrer la menace du cyberterrorisme. Ils ont plutôt amorcé une réflexion sur les solutions et les stratégies possibles pour contrer l'ensemble des cybermenaces.

3.2.1 Le cas du gouvernement

La Critical foundations *: protecting America's infrastructures* est l'étude la plus complète en ce qui concerne le cadre pronostique du cyberterrorisme (President's Commission on Critical Infrastructure Protection, 1997). Elle a pour but de permettre au gouvernement des États-Unis de prendre les mesures nécessaires pour protéger physiquement et virtuellement ses infrastructures essentielles. Leur protection virtuelle est un nouveau défi pour le gouvernement États-Unis, car le boom technologique du début des années 1990, comme il a été mentionné à la section 2.1, a autorisé l'intégration des systèmes informatiques

dans les infrastructures essentielles. Ces nouvelles technologies ont apporté divers avantages comme une communication plus rapide ainsi que des frais d'exploitation plus faibles. Toutefois, elles ont aussi amené des inconvénients liés à la sécurité de ses systèmes et des infrastructures qu'ils gèrent. La PCCIP met donc l'accent sur la protection virtuelle des systèmes informatiques des infrastructures essentielles (Ibid.). Afin de justifier son choix et ses propositions, elle utilise une métaphore du « corps ». Elle compare les infrastructures essentielles à quelques choses d'indispensable pour le maintien ou la protection de la vie lorsqu'elle dit : « In short, they are the lifelines on which we as a nation depend. » (Ibid., p. vii). La PCCIP est truffée de métaphores sur ce thème. Ce n'est pas surprenant étant donné le sujet de la commission. Aussi, elle utilise un vocabulaire exprimant l'entrée des États-Unis dans une nouvelle ère. Ce dernier réfère à l'entrée dans une nouvelle ère pour les États-Unis. Elle écrit : « In summary, all of us need to recognize that the cyber revolution brings us into a new age as surely as the industrial revolution did two centuries ago. » (Ibid, p. xi). Cette nouvelle époque implique de nouvelles menaces et de nouveaux défis ainsi que l'élaboration de nouvelles stratégies pour protéger les intérêts des États-Unis.

Aussi, elle précise qu'environ 85 % des infrastructures essentielles sont détenues par le secteur privé. Dans cette optique, la responsabilité du bon fonctionnement et de la protection de ces infrastructures incombe tant aux gouvernements qu'au secteur privé. Le reste de l'étude correspond à des recommandations d'actions pour permettre un partage efficace des rôles reliés aux infrastructures. Elle propose donc une stratégie d'action plutôt qu'une solution aux problèmes de leurs protections. Plus exactement, elle conclut : «In effect, we are not proposing solutions, but offering a step toward posturing our nation more effectively to deal with a new, still evolving world. » (Ibid., p.101). Néanmoins, les recommandations et les politiques que la commission propose sont pertinentes à étudier, car elles influencent, encore aujourd'hui, le cadre pronostique du cyberterrorisme.

Nous mentionnerons les sept recommandations de la commission en ordre d'apparition. La première est de promouvoir un partenariat entre le gouvernement et les propriétaires d'infrastructures essentielles et leurs opérateurs afin d'augmenter le partage des informations

au sujet des menaces, des vulnérabilités ainsi que de l'interdépendance des infrastructures essentielles. Cette recommandation vient d'un constat; le partage de l'information est le plus grand besoin actuel.

La seconde est de s'assurer que les propriétaires des infrastructures essentielles, les opérateurs et les gouvernements sont suffisamment informés et qu'ils ont le soutien nécessaire pour parvenir à les protéger. Pour y arriver, cette recommandation propose de mettre en place des outils comme, par exemple, des procédures de sécurité, afin de faciliter leur protection.

La troisième recommandation est l'établissement des structures nationales qui ont pour objectif de faciliter un partenariat efficace entre les différents paliers de gouvernement et aussi il va permettre aux propriétaires et aux employés des infrastructures essentielles de participer à la construction d'un plan de protection des infrastructures essentielles (*National Infrastructure Assurance Policy*). Pour ce faire, le rapport propose la création d'une multitude de structures au niveau national.

La quatrième consiste à augmenter la vigilance nationale par rapport aux menaces, aux vulnérabilités ainsi qu'aux conséquences de l'interdépendance des infrastructures essentielles à l'aide des programmes d'éducations et autres jugés nécessaires (Ibid.).

La cinquième recommandation est la mise en place d'une série d'activités sur la gestion de la sécurité informatique et des autres programmes connexes afin de démontrer le rôle de chef du gouvernement fédéral. Pour ce faire, le gouvernement doit montrer l'exemple et prendre l'initiative afin que les différents protagonistes utilisent les ressources que le gouvernement national offre.

La sixième est de modifier la législation afin d'augmenter l'efficacité du *National Infrastructure Assurance Policy* et de tous les autres efforts qui ont pour objectif la protection

des infrastructures essentielles. Elle propose de catégoriser les menaces informationnelles comme une information étrangère prioritaire.

La dernière recommandation est de quadrupler l'investissement en recherche et développement sur la protection des infrastructures essentielles. Pour ce faire, le gouvernement va accorder la priorité à l'investissement dans les secteurs à haut potentiel, c'est-à-dire ceux qui amèneront les meilleurs rendements (Ibid.).

En somme, la PCCIP met en place les bases de la protection virtuelle des infrastructures essentielles sans pour autant négliger leur protection physique. Elle tente de réduire leur vulnérabilité par rapport aux cybermenaces. Elle n'est donc pas établie pour lutter spécifiquement contre le cyberterrorisme.

3.2.2 Le cas des experts de la sécurité

Nous remarquons que les experts de la sécurité sont très actifs sur un domaine qui est connexe aux infrastructures essentielles en s'intéressant et en participant activement à la création du *National Information Infrastructure* (NII). Ce dernier est une initiative du Président Clinton qui désire créer un système de communication privée et publique et mettre en ligne, pour la population, des services gouvernementaux interactifs[7]. Ce système a été créé par le *High Performance Computing and Communication Act* de 1991 (États-Unis. Congress, 2007). En termes simples, le NII intègre Internet dans le cadre des activités de l'État. Il permet aux différents départements de communiquer plus efficacement, d'où son surnom d'*Information Superhighway*, mais aussi de communiquer avec la population et rendre plus accessibles certains services. Parmi les experts de la sécurité, Winn Schwartau, a été un des experts chargés de la mise en place du NII (2004). Ce dernier, ainsi que d'autres experts, indique des politiques et des lignes directrices afin de créer un réseau de l'information

[7] Ce sont les mêmes services gouvernementaux déjà offerts à la population. Le citoyen peut avoir accès à ces services par Internet. Il n'est plus obligé d'aller à un bureau gouvernemental ou d'envoyer une demande par la poste. Il peut maintenant effectuer sa requête par le cyberespace.

sécuritaire. De plus, ces experts constatent des problèmes potentiels auxquels le NII pourrait faire face, comme des difficultés rattachées au commerce électronique, à la protection de l'information et des droits civils et ceux reliés à la sécurité des réseaux (Ibid.).

Les problèmes potentiels que les experts de la sécurité ont relevés se sont présentés quelques années plus tard et ils sont toujours d'actualité. Ils ont tenté, au moment de l'écriture du document, de proposer des solutions à ces problèmes. Par leur nature nouvelle, les solutions étaient encore embryonnaires et ils ont plutôt offert des pistes de réflexion au gouvernement et aux experts.

Pour illustrer ce propos, nous allons nous pencher sur l'idée de Schwartau qui est, à notre avis, le plus important contributeur à la réflexion sur les cybermenaces. Il propose l'élaboration d'un *National Information Policy*. Ce dernier a pour objectif de poser des règles de conduite de bases pour les individus dans le cyberespace sans être pour autant une proposition législative. De plus, il fixe comment les États-Unis doivent se comporter par rapport aux autres usagers et aux différents pays qu'il va rencontrer sur le cyberespace. Finalement, il souhaite que les États-Unis deviennent un des principaux contributeurs à la réflexion sur le cyberespace. (Schwartau, 1994).

Pour conclure, le PCCIP établit la stratégie de base du gouvernement pour protéger leurs infrastructures essentielles des cybermenaces, soit la coopération, entre les secteurs public et privé. Bien qu'ils aient participé, le plus souvent indirectement, à la PCCIP, les experts de la sécurité ne proposent pas de stratégie ou de solutions spécifiques au cyberterrorisme. Ils ont offert une réflexion sur les solutions et les stratégies possibles pour contrer les cybermenaces de façon générale.

3.3 Le cadre pronostique du cyberterrorisme pendant la période 1997-2001

Nous soutenons que le cadre pronostique du cyberterrorisme n'a pas fondamentalement changé. Le gouvernement a continué le plan de protection des infrastructures essentielles dicté dans la PCCIP. Pour leur part, les experts ont poursuivi leurs réflexions sur les stratégies à utiliser pour protéger les infrastructures essentielles et contrer le terrorisme. Bien que certains aient critiqué quelques initiatives du gouvernement, ils appuient, dans l'ensemble, sa stratégie. Finalement, leur seule contribution réside dans la création de nouveaux logiciels ou de systèmes informatiques plus fiables pour protéger les infrastructures essentielles. Donc, ils n'ont pas proposé d'innovations pour cette stratégie.

3.3.1 Le cas du gouvernement

La période suivant la PCCIP en est une de continuation des politiques énoncées par ce dernier. Nous pouvons les regrouper en deux volets qui ont pour mission d'enrayer la menace du cyberterrorisme. Afin de mieux analyser le cadre pronostique du cyberterrorisme, nous étudierons séparément chacun de ces volets.

Le premier volet est énoncé principalement dans le PDD-62 (États-Unis. White House, 1998b). Il se veut un énoncé contre toutes formes de terroristes et désire donner les outils nécessaires aux États-Unis pour combattre et se prémunir contre cette menace. Le document réaffirme les déclarations du PDD-39. Néanmoins, il existe une différence, soit la création du *National Coordinator for Security, Infrastructure Protection and Counter-Terrorism* dirigée par Richard A. Clark, le *National Coordinator*. Cette structure a pour mission de superviser les politiques et les programmes gouvernementaux concernant le contre-terrorisme, la protection des infrastructures essentielles et la gestion du risque à l'égard des armes de destruction massive. De plus, cet organe a un rôle de conseillé au sujet du financement des programmes de lutte contre le terrorisme et coordonne le développement des lignes directrices en matière de gestion de crise. Donc, le dirigeant de cette institution a une certaine

influence sur les décisions en lien avec les cybermenaces et la protection des infrastructures essentielles. Nous y reviendrons à la section 4.4.1 lors de la discussion du cadre motivationnel.

Le deuxième volet est érigé principalement par le PDD-63 (États-Unis. White House, 1998c). Il a pour objectif de mettre en place les dispositifs nécessaires afin de protéger les infrastructures essentielles des États-Unis. Plus spécifiquement, il s'intéresse à la protection physique, mais l'accent est placé sur la protection virtuelle des infrastructures. La finalité des mesures prescrites est alors d'éliminer et de prévenir l'apparition de vulnérabilité virtuelle.

Dans la même lignée que la PCCIP, le document considère que la mise en place d'un partenariat public privé est une condition nécessaire pour réussir à les protéger. Dans cette optique, le gouvernement et les entreprises vont contribuer à la construction d'un *National Infrastructure Assurance Plan*. Ce plan vise dix objectifs. Chacun de ces objectifs correspond à une partie de la solution du gouvernement états-unien contre les cybermenaces et le cyberterrorisme.

1. Analyser périodiquement chaque secteur d'infrastructures essentielles afin de trouver des vulnérabilités.
2. Créer un plan de rattrapage pour chaque secteur basé sur l'analyse des vulnérabilités faites précédemment.
3. Mettre en place un centre d'alerte pour prévenir les différentes infrastructures essentielles d'attaque potentielle.
4. Mettre en place un système de réaction en cas d'attaque afin de limiter les dégâts.
5. Créer un système de remise en fonction des systèmes informatiques des infrastructures essentielles en cas d'incident.
6. Créer un programme d'éducation sur la sécurité informatique des infrastructures destiné aux employés gouvernementaux et du secteur privé.
7. Parrainer des études de recherches et développement sur le sujet de la protection des infrastructures essentielles (Ibid.).

8. Planifier une procédure pour améliorer la collecte et l'analyse de l'information concernant les menaces venant de l'extérieur visant les infrastructures (White House, 1998c).
9. Créer un plan pour étendre la coopération internationale en matière de protection des infrastructures entre les alliés des États-Unis.
10. Évaluer les budgets nécessaires en ce qui concerne les infrastructures essentielles (Ibid.).

Nous désirons noter un problème récurrent pour le gouvernement. Celui du manque d'incitatifs pour le secteur privé pour coopérer activement contre le cyberterrorisme. En fait, il serait faux d'affirmer que le secteur privé ne s'intéresse pas à se protéger contre le cyberterrorisme ou toutes autres formes de cybermenaces. Néanmoins, il va continuer à préférer une gestion du risque en fonction des coûts des mesures sécuritaires. Se rallier représente, pour lui, un coût supplémentaire et non fondé. Aussi, il faut que les informations transmises au gouvernement par les entreprises soient rendues publiques en conformité avec le *Freedom of Information Act* (Stohs, 2002). Toutefois, cette contrainte sera levée avec le *Homeland Security Act of 2002* qui protège l'information divulguée par les infrastructures essentielles privées (États-Unis. United States Congress, 2002). Finalement, l'entreprise prend un risque lorsqu'elle échange des informations avec le gouvernement. En effet, ces informations peuvent être utilisées contre cette entreprise si elle enfreint une loi (Kristensen, 2008).

Nous concluons que le PDD-63 propose ou vise sensiblement les mêmes politiques pour lutter contre le cyberterrorisme que la PCCIP. La seule différence est que ce dernier ne demeure qu'une commission à titre consultatif alors que le PDD-63 constitue une déclaration des actions qui ont été prises par le gouvernement états-unien.

Le gouvernement est conséquent avec la PCCIP et le PDD-63 lorsqu'il crée, au moyen de l'*Executive Order* 13130 (États-Unis. White House. 1999b), le *National Infrastructure Assurance Council* (NIAC). Ce nouvel organe a pour objectif de promouvoir le partenariat

entre les secteurs public et privé au sujet de la protection des infrastructures essentielles. Il reste un organe consultatif sans pouvoir de décision. Toutefois, il a un accès au Président grâce au *National Infrastructure Assurance Council*, ce qui démontre l'importance que porte le gouvernement à l'opinion et aux recommandations du secteur privé (Michel-Kerjan, 2003). Il présente, lorsqu'il le juge nécessaire, des rapports et des suggestions aux gouvernements.

Le *National plan for Information Systems Protection* a eu comme but de réaffirmer le plan d'action du PDD-63 (White House, 2000b). Ce document n'offre aucun élément nouveau de solution en ce qui concerne la protection des infrastructures essentielles et la lutte contre le terrorisme. Néanmoins, il est intéressant, car il s'intéresse à une problématique récente, qui semblait avoir échappé au gouvernement, soit la protection des droits et de la vie privée. Dans les faits, l'apparition des nouvelles technologies de communications, principalement Internet, a demandé des ajustements dans la législation, comme l'*Electronic Communications Privacy Act* (États-Unis. United States Congress, 1986b) et le *Privacy Act* (Etats-Unis. United States Congress, 1974), afin de faire respecter ces droits. Malgré cela, les nouvelles mesures pour protéger virtuellement les infrastructures essentielles, telles qu'une surveillance plus accrue de l'activité sur leurs réseaux informatiques, peuvent constituer une menace pour la vie privée et les libertés individuelles. Le gouvernement répond à cette question en soutenant que la protection des infrastructures essentielles ne doit pas se faire au détriment des droits et de la vie privée. Par conséquent, les systèmes de contrôle informatique doivent être conçus pour respecter ces droits. De plus, les employées responsables de ses systèmes doivent honorer un code d'éthique. Lors de ses formations du secteur public et du secteur privé, le gouvernement veut mettre l'accent sur l'importance de l'éthique. Finalement, le gouvernement respectera une politique de confidentialité lors de l'échange d'information du secteur privé au secteur public (White House, 2000b).

Ce regain d'intérêt pour cette problématique est dû, en grande partie, aux nombreuses voix qui se sont élevées à propos de la possibilité d'individus qui seraient lésés dans leurs droits. Nous avons remarqué que certains spécialistes et militants de la protection des droits privés avaient déjà dénoncé ces risques (Beeson, 1996 ; Schwartz, 1999). Toutefois, les

experts de la sécurité n'ont pas abordé cet enjeu. Alors, nous ne nous attarderons pas sur ce dernier.

3.3.2 Le cas des experts de la sécurité

En ce qui concerne les experts de la sécurité, un élément récurrent de leur analyse est qu'il est impossible de sécuriser toutes les vulnérabilités et d'obtenir un système informatique invulnérable. Ils ont conclu que les infrastructures essentielles ne peuvent pas être totalement protégées (Ellision et coll., 1997 ; Denning, 2000 ; Fuhrman, 1998). Cette impossibilité s'explique par différentes raisons. Premièrement, il n'est pas possible de sécuriser une vulnérabilité si elle n'est pas connue. Deuxièmement, l'évolution dans ces technologies est souvent trop rapide comparativement aux efforts de mise à jour et de réparation des brèches de sécurité. L'ajout d'équipements neufs ou de protocoles peut occasionner de nouvelles vulnérabilités. Troisièmement, l'ouverture de *port* pour permettre la communication entre les différents ordinateurs dans un réseau informatique amène nécessairement des possibilités de vulnérabilités. Finalement, les travaux de Gödel offrent une explication convaincante de cette impossibilité, car ils sont les fondations de la logique formelle utilisée en sciences informatiques.

Godel a aussi développé les théorèmes d'incomplétude[8] qui est la base de sérieux problèmes pour la science informatique. Il prouve que, pour tout système axiomatique capable de décrire les nombres naturels, on peut affirmer deux conclusions. Premièrement, le système ne peut pas être en même temps cohérent et complet (Paty, 1988). Deuxièmement, « ¨la cohérence d'un système ne peut pas être prouvée à l'intérieur de ce système lui-même.¨ » (Ibid., p. 145). Ces conclusions résultent de l'apparition d'un problème fondamental en science informatique, le problème de l'arrêt de Turing. Ce dernier est de savoir si le programme informatique va finir par s'arrêter ou continuer indéfiniment son opération en boucle (donc de savoir si la proposition est démontrable ou non). Dans le dernier cas, un

[8] Ce terme réfère à l'état de ce qui est incomplet.

bogue apparaît (Dawson, 2006). Nous arrivons à la conclusion qu'il est impossible de déterminer la fiabilité d'un programme informatique.

En ce qui concerne l'efficacité du plan d'action du gouvernement au sujet de la protection virtuelle des infrastructures essentielles, les experts de la sécurité sont divisés sur la question. Toutefois, le gouvernement et les experts de la sécurité, présents lors de la conférence *Cyber-Terrorism and Information Warfare*, considèrent qu'il ne faut pas traiter la menace du cyberterrorisme différemment du reste des cybermenaces. Selon eux, les méthodes utilisées par les belligérants seront identiques. La différence réside dans les raisons justifiant leurs actes. Ainsi, nous pouvons affirmer que les experts proposent, en général, des politiques et des solutions pour contrer les cybermenaces qui serviront aussi contre le cyberterrorisme.

De son côté, Rathmell croit qu'une cyberattaque terroriste est peu probable. Néanmoins, il juge qu'il est nécessaire de façonner un mécanisme de recensement des vulnérabilités informatiques. Ce dernier devra transmettre ces informations aux entités concernées (Rathmell, 1997). Cette proposition est très semblable au premier et au deuxième objectif du *National Infrastructure Assurance Plan*. Plus spécifiquement, ce rôle est effectué par le *National Infrastructure Protection Center* (NIPC), un sous-programme du FBI.

Le NIPC est critiqué vigoureusement par les spécialistes en sécurité informatique en raison de ses alertes de sécurité, car ils considèrent que les informations qu'il transmet par courriels sont insuffisantes pour permettre aux opérateurs de réseaux informatiques de prendre les mesures nécessaires pour protéger leur réseau (Forno, 2000). Aussi, lorsque l'envoi contient suffisamment de données techniques, il arrive que ceux-ci soient erronés. Finalement, la critique la plus sévère s'élève au niveau de la coopération entre le secteur public et le secteur privé, un des piliers du *National Infrastructure Assurance Plan*, parce que le NIPC ne dévoile pas toujours la totalité des informations qu'il possède. Selon Richard Forno, le NIPC se doit de réévaluer son processus de transmission de ses informations afin de créer un véritable dialogue entre le secteur public et privé (Ibid.).

Certains experts critiquent l'approche du gouvernement pour lutter contre les cybermenaces comme le fait Rathmell dans un texte écrit en 1998. Il soutient que l'approche du gouvernement des États-Unis pour contrer les cybermenaces est inefficace. Il considère qu'une démarche qui se concentre sur la capacité informatique des groupes hostiles au gouvernement d'infliger des dégâts n'offre que de résoudre une partie du problème de la protection des infrastructures essentielles et que ce type d'approche ne permet que d'obtenir les risques et vulnérabilités du moment. Étant donné le caractère évolutif des technologies, cette approche ne permet pas de prédire les prochains vulnérabilités ou types d'attaques. Alors, la planification à long terme de la sécurité virtuelle des infrastructures essentielles est un exercice futile. Il propose une approche basée sur la structure et la culture organisationnelle des groupes belligérants. Selon lui, il est possible de déterminer si les groupes en ont la capacité et s'ils ont une volonté d'employer ces méthodes. Il considère que la culture d'une organisation a un impact important sur le type d'attaque utilisé ainsi que les cibles visées. Dans cette optique, une organisation qui opère au moyen des attentats suicides à la bombe a développé une culture du martyr. Un changement de moyen d'attaque ne devrait pas se faire instantanément. Rathmell soutient qu'il leur faudra un certain temps pour que les organisations terroristes modifient leurs méthodes parce que les cyberattaques sont trop récentes. Il est donc possible, à l'aide d'étude de cas, de déterminer si un groupe va utiliser les cyberattaques et cerner leurs méthodes d'attaques informatiques. Le problème de l'utilisation de l'étude de cas est assez évident. Il faut une information de qualité et de premier plan de l'organisation et de son mode d'opération. Cette information est difficile à obtenir et il y a toujours une possibilité qu'un nouveau groupe se soit formé et que les autorités l'ignorent. Dans cette situation, cette approche n'est pas efficace. Finalement, Rathmell observe une limite à sa propre approche. Il note que le nombre d'organisations ayant effectué des cyberattaques, de 1990 à 1998, est limité. Par ce faible nombre de cas, il juge qu'il est difficile, au moment de l'écriture de son texte, de tirer des conclusions de ces cas (Rathmell, 1998).

Pour sa part, Gideon Frieder avait remarqué que le concept et les idées se rattachant au cyberterrorisme étaient relativement nouveaux (1998). Il considérait qu'il n'existait pas encore quelqu'un, à sa connaissance, avec une formation spécialisée sur le sujet au niveau universitaire et une expérience de carrière suffisante pour analyser et ériger des politiques sécuritaires adéquates. Selon lui, une relève devait bientôt être en mesure de se spécialiser dans ce domaine.

Nous notons que certains experts préconisent des solutions, pour lutter contre le cyberterrorisme, semblables à celles du gouvernement. Par exemple, Thomas Furhman met l'accent sur la gestion du risque, car elle permet des décisions mieux informées. Cette méthode se base sur le postulat qu'il est impossible de tout sécuriser pour des raisons financières. Dans ces circonstances, les organisations doivent décider du niveau de risque qu'ils considèrent comme acceptable. Pour ce faire, ils établissent leurs secteurs vitaux, les menaces à leurs intérêts et la probabilité et les conséquences si une attaque a lieu. Une fois cette étape franchie, les gestionnaires quantifient les menaces et vont utiliser les outils à leur disposition pour maîtriser leur risque (Furhman, 1998). Cette théorie est inspirée de l'économie et de la théorie des choix rationnelles. Cette théorie est bien résumée par cette citation : « All of this is done in the context of cost. Because if the cure is more costly than the problem itself, then maybe it's not worth correcting at all. » (Ibid., p. 13).

De plus, il considère qu'une panne des infrastructures essentielles devra être assez importante, pour affecter significativement la société. Il cite l'exemple de la perte de service électrique au Québec en 1998. Selon lui, bien qu'une partie de la province n'ait pas eu accès à de l'électricité pour une longue période, cela n'a pas eu d'impact sur la sécurité nationale. Il suggère donc que le gouvernement et le secteur privé développent un sens de proportion à l'égard des dégâts que pourrait causer la perte d'une des cinq catégories d'infrastructure essentielle. Ainsi, ils pourront focaliser leurs ressources à la protection des infrastructures essentielles à la société et à l'État (Ibid.).

Aussi, Furhman préconise la mise en place de mesures de sécurité et d'organisations destinées à réduire l'interdépendance des infrastructures essentielles. Dans cette optique, il sera plus difficile de leur infliger des dommages considérables et il sera moins tentant pour les groupes belligérants de planifier une attaque et les mesures de sécurité supplémentaires augmenteront la difficulté de réussite d'une telle attaque (Ibid.).

Comme nous pouvons le constater, l'approche de Tom Furham est sensiblement la même que celle du gouvernement. En effet, la gestion du risque fait partie intégrante du *National Infrastructure Assurance Plan*, elle est basée sur les six premiers objectifs de ce dernier. Ainsi, le plan est fondé sur une identification des menaces et des vulnérabilités (*Vulnerability Analysis*). Par la suite, les gestionnaires suggèrent un plan de rattrapage (*Remedial Plan*). Une structure d'alerte, une d'intervention et différents systèmes de sauvegarde sont proposés (*Warning*, *Response* et *Reconstitution*). Finalement, la formation des employés gouvernementaux et du secteur privé permet d'éliminer des risques simples de sécurité (*Education and Awareness*).

Nous notons que l'utilisation de la gestion du risque comme stratégie par le gouvernement états-unien n'est pas nouvelle. En fait, la gestion du risque a été employée la première fois en 1838 lorsque le Congrès des États-Unis, après avoir débattu pendant plusieurs années le rôle du gouvernement sur la législation des moteurs à vapeur, a établi le *Steamboat Inspection Service*. Un autre exemple est la recommandation du *U.S. Nuclear Regulatory Commission* d'utiliser des analyses de probabilité pour déterminer la sécurité des installations (Vesper, 2006). Nous pouvons donc affirmer que les experts de la sécurité n'ont pas influencé le gouvernement au niveau de l'utilisation de la gestion du risque au niveau des infrastructures essentielles.

Finalement, la conférence *Cyber-Terrorism and Information Warfare* démontre qu'il y a des échanges d'idées entre le gouvernement, le secteur privé et les experts de la sécurité. Toutefois, nous constatons que les experts de la sécurité n'ont pas amené de nouvel élément

de stratégie pour contrer le cyberterrorisme et protéger les infrastructures essentielles. Ils ont repris les mêmes stratégies élaborées auparavant par le gouvernement.

Néanmoins, il y a un consensus entre les experts au sujet des infrastructures essentielles. Ils reconnaissent leurs nécessités pour conserver le niveau de vie des États-Uniens. D'ailleurs, Dorothy Denning, une experte qui ne croit pas à la faisabilité du cyberterrorisme, qualifie les infrastructures essentielles de : « national life support system » (2000, p.3). Cette métaphore du « corps » illustre la même idée que la PCCIP. Elle renvoie à l'idée que protéger la santé des infrastructures essentielles est nécessaire pour que les États-Unis puissent conserver leur stabilité et leur mode de vie actuel. Le succès de la protection des infrastructures essentielles nécessite une défense contre tous les types de menace. Donc, ce n'est pas encore une stratégie de protection contre le cyberterrorisme, mais contre les cybermenaces en générales.

Pour conclure, le gouvernement a continué le plan de protection des infrastructures essentielles dicté dans la PCCIP. Pour leur part, les experts ont poursuivi leurs réflexions sur les stratégies à utiliser pour protéger les infrastructures essentielles et contrer le terrorisme. Certains ont critiqué quelques initiatives du gouvernement, mais, dans l'ensemble, ils soutiennent la stratégie du gouvernement. La gestion des risques et la coopération entre le secteur public et le secteur privé semblent être des stratégies qui plaisent aux experts. Néanmoins, leur seule contribution réside dans la création de nouveaux logiciels ou systèmes informatiques fiables pour les infrastructures essentielles.

3.4 Le cadre pronostique du cyberterrorisme après les évènements du 11 septembre

Nous soutenons que le gouvernement a continué à préconiser la stratégie établie par la PCCIP afin de protéger les infrastructures essentielles des États-Unis. Nous remarquons qu'il n'y a pas eu de transformation importante de cette stratégie malgré le changement de gouvernement et les changements organisationnels comme suite aux évènements du 11 septembre 2001. Du côté des experts de la sécurité, nous croyons qu'ils n'ont pas influencé le

cadre pronostique du cyberterrorisme. Nous l'expliquons par le fait qu'ils n'ont pas proposé d'innovation pour contrer le cyberterrorisme. De plus, nous avons remarqué que les stratégies et solutions qu'ils offrent ne sont pas propres au cyberterrorisme. Ce qu'ils ont recommandé concerne le terrorisme ou les cybermenaces en général. Ils n'ont pas créé un cadre pronostique du cyberterrorisme.

3.4.1 Le cas du gouvernement

Comme nous l'avons mentionné précédemment dans la section 2.5.1, le gouvernement a créé l'*Office of Homeland Security* en réaction aux attentats du 11 septembre 2001. La mission de ce dernier est de développer et d'implanter une stratégie nationale afin de prémunir les États-Unis contre des attaques terroristes. Cette mission est identique à celle du PDD-39. Toutefois, une différence fondamentale existe entre les deux documents. Le PDD-39 les a délégués à plusieurs autres départements selon leurs compétences; L'EO 13228 prévoit une réorganisation de la distribution des rôles et accorde la totalité des rôles à l'*Office of Homeland Security*. Cette particularité a deux conséquences. Premièrement, il devient le principal responsable meneur de la lutte contre le terrorisme aux États-Unis. L'intégralité de l'effort sera supervisée et coordonnée par ce bureau. La coordination et la mise en œuvre des mesures devraient être plus aisées. Deuxièmement, sa mise sur pied va mettre fin aux guerres pour les budgets de la lutte contre le terrorisme entre les différentes agences et départements du gouvernement des États-Unis (White House, 2001). Elle va alors remodeler son organisation pour faciliter la lutte contre le terrorisme et ils continueront leur combat contre le cyberterrorisme avec le même intérêt que pour toutes les formes de terrorismes.

Du point de vue de la protection des infrastructures essentielles des États-Unis, le plan d'action est identique à celui de la PCCIP. En fait, l'*executive order* 13231, *Critical Infrastructure in the Information Age*, n'offre aucun élément nouveau (White House, 2001b). Ce plan est encore basé sur le principe de la gestion du risque, et ce, en partenariat avec le secteur privé. Une des seules particularités notables est la création d'une entité, le *President's*

Critical Infrastructure Protection Board. Ce dernier a comme tâche de développer et coordonner la mise en place des politiques en lien avec la protection des infrastructures essentielles. Ces politiques sont explicitées dans l'*Executive Order*. Elles sont exactement les mêmes que celles du *National Infrastructure Assurance Plan* à une exception près; il doit coordonner ces activités avec *l'Office of Homeland Security*. Cette dernière tâche est logique dans la mesure où *l'Office of Homeland Security* doit prémunir les États-Unis contre de futures attaques terroristes. Pour ce faire, il doit être en mesure de délimiter et protéger les infrastructures essentielles. Cela nécessite un travail de coordination entre les deux entités (Ibid.).

Comme il est coutume lors de la création d'une nouvelle organisation, celle-ci commence en publiant son plan d'action. L'*Office of Homeland Security* ne fait pas autrement, il publie le *National Strategy for Homeland Security* (États-Unis. Office of Homeland Security, 2002). Son objectif est de protéger les citoyens états-uniens de toutes attaques terroristes. Pour ce faire, il prévoit réduire ses vulnérabilités et il va établir un plan d'action en cas d'incident. Il est à noter que le document est très général. En fait, il met en place des politiques pour contrer le terroriste traditionnel et des formes moins traditionnelles comme le terrorisme nucléaire, biologique, chimique ou informatique. Il est intéressant, car il nous montre que l'administration états-unienne s'intéresse toujours au cyberterrorisme. Par sa nature très large, il nous est impossible de déterminer des politiques ou des solutions propres à la menace du cyberterrorisme. Nous arrivons à la même conclusion au sujet du *National Strategy for Homeland Security* de 2007 (États-Unis. Homeland Security Council).

Cependant, il a permis la rédaction de deux documents de stratégie nationale de sécurité plus explicite. Le premier est le *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Il s'intéresse à la sécurité nationale au niveau physique (États-Unis. White House. 2003). Il prévoit des stratégies et des politiques en vue de protéger la population et le territoire des États-Unis des menaces plus traditionnelles comme le terrorisme traditionnel. Il n'a pas d'intérêt pour nous, alors nous n'étudierons pas sur ce document plus en profondeur.

Le deuxième document, le *National Strategy to Secure Cyberspace,* se concentre sur toutes les menaces provenant du cyberespace ce qui inclut le cyberterrorisme (États-Unis. White House. 2003b). Comme toute stratégie nationale de sécurité, elle désire protéger l'espace virtuel états-unien de toutes formes d'attaques et de menaces. Elle est audacieuse, car c'est la première du genre. Aucune autre ne s'est concentrée exclusivement sur le cyberespace. Bien qu'il soit original, le document propose un plan qui est une reproduction de la PCCIP. En fait, le document suggère toujours de protéger virtuellement les infrastructures essentielles.

La seule différence est que le document utilise à profusion un nouveau terme, celui de « debilitating ». Ce dernier réfère à un affaiblissement. Il est très utilisé en médecine pour décrire les effets d'une maladie ou d'un parasite sur le corps. Le document l'utilise pour décrire les effets d'une attaque sur les infrastructures essentielles. Par exemple, il écrit : « [...] helps reduce our Nation's vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them. (Ibid., viii). Nous pouvons encore trouver la comparaison entre les infrastructures essentielles et le corps humain.

Pour protéger virtuellement les infrastructures essentielles, il préconise la participation du secteur privé dans l'élaboration des stratégies, ainsi que la coopération et l'échange d'information entre le secteur privé et public. De plus, il recommande d'améliorer et d'analyser les systèmes informatiques pour trouver des vulnérabilités et incite le gouvernement fédéral à poursuivre l'élaboration et la mise en pratique des plans de protection de ses systèmes informatiques. Aussi, il doit continuer à agrandir sa capacité à alerter les opérateurs d'infrastructures essentielles des menaces virtuelles et à perfectionner sa capacité à gérer des incidents potentiels (Ibid.). Nous pouvons conclure que cette stratégie ne change en rien les politiques énoncées auparavant dans la PCCIP.

Nous remarquons que l'incapacité des plans du gouvernement à parvenir à des résultats concrets diminue la force du cadre pronostique. Nous observons que, depuis la PCCIP, le gouvernement préconise le même plan d'action pour lutter contre les cybermenaces. Or, les objectifs fixés dans ces plans sont, encore aujourd'hui, loin d'être atteints. Pour illustrer ce propos, nous allons prendre l'exemple de la coopération entre le secteur public et privé. Celle-ci est la pierre angulaire du plan d'action du gouvernement des États-Unis en ce qui concerne les cybermenaces et la protection des infrastructures essentielles. Malgré des efforts soutenus, la coopération entre les deux secteurs est relativement faible, en grande partie par le manque d'incitatif pour le secteur privé à collaborer à ces programmes et à échanger de l'information. L'exercice *Cyberstorm* de 2006 souligne bien ces propos (États-Unis. Department of Homeland Security, 2006). Cet exercice a été créé pour vérifier la protection des systèmes informatiques des infrastructures essentielles. Le gouvernement et le secteur privé ont participé à celle-ci. La presque totalité des conclusions concerne les difficultés de communication, d'échange d'information et de coopération en général entre les différentes entités. Ce problème ne touche pas seulement la coopération entre le secteur public et privé. Il porte également sur la collaboration entre deux organes du secteur public. Sur ce sujet, le rapport affirme que l'*Interagency Incident Management Group* (IIMG) et le *National Cyber Response Coordination Group* (NCRCG) ont encore besoin de peaufiner leur coopération. De plus, ce dernier conçoit que le gouvernement des États-Unis a besoin de développer un programme politique permettant d'échanger de l'information avec le secteur privé au niveau national et international. Aussi, le rapport conclut que le gouvernement se doit de créer une stratégie de communication pour le public en général et les autorités locales afin qu'ils puissent prendre les actions nécessaires pour remédier à la situation (Ibid.).

Ces conclusions ne sont pas isolées. Plusieurs autres rapports du GOA démontrent que le gouvernement n'a toujours pas été en mesure d'atteindre ses objectifs fixés dans la PCCIP et les textes subséquents. Le constat du rapport du GAO, *Critical Infrastructure Protection : Multiple Efforts to Secure Control Systems,* est que le DHS doit développer et mettre sur pied une stratégie de coordination entre les secteurs public et privé afin d'améliorer la protection des systèmes informatiques des infrastructures essentielles (2004).

Le rapport *Critical Infrastructure Protection : Multiple Efforts to Secure Control Systems Are Under Way but, Challenges Remain* juge que les systèmes informatiques des infrastructures essentielles sont encore vulnérables à des attaques informatiques (États-Unis. General Accounting Office, 2007). Afin de réduire ces vulnérabilités, il recommande que le *Department of Homeland Security* améliore la coopération ainsi que l'échange d'information entre le secteur public et le secteur privé. Il pointe du doigt l'absence d'une réelle stratégie de coopération entre le secteur public et le secteur privé et propose l'élaboration d'une telle stratégie.

En somme, nous affirmons que le cadre pronostique du cyberterrorisme tel qu'élaboré par le gouvernement des États-Unis après le 11 septembre reste sensiblement identique à celui suggéré par la PCCIP en 1997. En effet, la création du DHS et sa prise en charge de la protection des infrastructures essentielles n'ont fondamentalement rien changé à la protection des infrastructures essentielles aux États-Unis.

3.4.2 Le cas des experts de la sécurité

En ce qui concerne les experts de la sécurité, nous aborderons les solutions proposées par ceux qui ont effectué une tentative de faire du cyberterrorisme un enjeu de sécurité. Nous soutenons qu'ils n'ont pas apporté de nouvelles solutions aux problèmes et leur manque d'innovation est la raison qui explique l'échec de leur cadre pronostique du cyberterrorisme.

La protection des infrastructures essentielles est toujours au cœur des préoccupations des experts de la sécurité. Ils utilisent toujours la métaphore du « corps » pour justifier les mesures qu'ils proposent. Parmi les experts utilisant le plus ce type de métaphore, il y a Dan Verton. Ce dernier qualifie les infrastructures essentielles de : « *digital nervous system* » (2003, p16) et de « vital organs of the digital infrastructure » (Ibid. p.19). Encore une fois, une comparaison est faite entre les infrastructures essentielles et le corps humain.

L'idée d'urgence est toujours présente dans le discours des experts. Par exemple, Dan Verton écrit : « [...] that digital heartbeat began to flat-line. » (Ibid. p.148) pour expliquer la perte de service téléphonique occasionné par les attentats du 11 septembre. La métaphore du corps est forte. Si le cœur ne bat plus, il y a décès. Alors, il est primordial que cette situation ne se reproduise plus.

Parmi les solutions proposées par les experts de la sécurité, nous retrouvons l'amélioration de la protection des infrastructures essentielles. Pour y arriver, ils prônent un perfectionnement des programmes de protection des systèmes informatiques et ils mettent l'accent sur la nécessité de vérifier la fiabilité des systèmes informatiques en les soumettant à divers tests. Aussi, ils préconisent la coopération entre le secteur public et le secteur privé au niveau de l'échange de l'information. Finalement, ils encouragent le secteur privé à prendre les mesures nécessaires pour garantir la protection de leurs infrastructures (Verton, 2003 ; Zanini et Edwards, 2001).

Zanini et Edwards vont un peu plus loin dans leur analyse en préconisant une étude périodique des cybercapacités des groupes terroristes afin d'être en mesure de déterminer lequel constitue un risque non négligeable. Dans la même ligne d'idées, ils indiquent le besoin d'intercepter et d'analyser les conversations et les opérations auxquelles se livrent les groupes terroristes (Ibid.).

Nous avons remarqué que les experts en sécurité informatique proposent des méthodes informatiques pour réduire les vulnérabilités des systèmes informatiques. Bien qu'elles soient nouvelles, elles ne constituent pas une innovation pour lutter contre le cyberterrorisme et protéger les infrastructures essentielles (Chakrabarti et Manimaran, 2002 ; Igure, Laughter et Williams, 2006). En fait, le gouvernement avait déjà une politique de recherche et de développement et il avait déjà des mises à jour de sécurité et, lorsqu'elle coïncide avec leur politique de gestion des risques, elles vont intégrer de récentes techniques pour renforcer leurs sécurités informatiques.

Pour conclure, nous soutenons que le gouvernement a continué à préconiser la stratégie établie par la PCCIP afin de protéger les infrastructures essentielles des États-Unis. Nous remarquons qu'il n'y a pas eu de transformation importante de cette stratégie malgré le changement de gouvernement et ceux de nature organisationnelle en réponse aux évènements du 11 septembre 2001. Du côté des experts de la sécurité, certains d'entre eux ont participé à l'élaboration du PCCIP. Les autres ont promu cette stratégie et n'ont pas apporté d'innovation à cette dernière. De plus, ils n'ont pas tenté d'établir une solution propre au cyberterrorisme. Les solutions qu'ils ont proposées touchent soit le terrorisme en général, soit les cybermenaces. Par conséquent, ils n'ont pas été en mesure de créer un cadre pronostique du cyberterrorisme.

CHAPITRE IV

L'ÉVOLUTION DU CADRE MOTIVATIONNEL DU CYBERTERRORISME AUX ÉTATS-UNIS

Dans ce chapitre, nous allons analyser l'évolution du cadre motivationnel du cyberterrorisme aux États-Unis afin de déterminer si les experts de la sécurité ont réussi à influencer le gouvernement. Pour ce faire, nous utiliserons le cadre motivationnel, c'est-à-dire un schéma d'interprétation qui a pour objectif de regrouper la population pour qu'il lutte et qu'il entame des actions concrètes contre la menace.

Également, nous soutiendrons que les citoyens n'ont pas appuyé les experts de la sécurité dans leur tentative de faire du cyberterrorisme un enjeu de sécurité parce que le gouvernement avait déjà identifié cette menace, parmi l'ensemble des cybermenaces. De plus, il avait amorcé une réflexion et il avait entrepris des décisions directes pour les contrer. Il n'y avait pas de raison pour la population de se rallier et de mettre sur pied des mesures exceptionnelles contre le cyberterrorisme.

4.1 L'influence de l'attentat d'Oklahoma City sur le cadre motivationnel du cyberterrorisme

Le gouvernement et les experts de la sécurité n'ont pas tenté de bâtir un cadre motivationnel du cyberterrorisme durant cette période. Nous verrons que les deux parties chercheront à rallier la nation, soit la population et les institutions politiques et législatives, autour de la problématique de la protection des infrastructures essentielles. Cet essai de rassemblement est capital, car il prouve que l'intérêt du gouvernement et des experts de la sécurité est de protéger ses infrastructures essentielles de l'ensemble des cybermenaces et pas

spécifiquement du cyberterrorisme. Afin de démontrer ce point, nous examinerons deux évènements cruciaux de cette période. Par la suite, nous discuterons de l'apport de Winn Schartau et du rapport *Computer at Risk*, sur le cadre motivationnel de la protection des infrastructures essentielles.

Le premier évènement important est l'attentat d'Oklahoma City en 1995. Nous soutenons que le gouvernement et les experts de la sécurité ne chercheront pas à mettre en place un cadre motivationnel du cyberterrorisme parce que la population était déjà convaincue de la menace du terrorisme. Par ailleurs, cet attentat ne comporte aucun lien avec le cyberterrorisme, il est alors illogique que le gouvernement ou les experts de la sécurité tentent d'imposer un cadre motivationnel sur cette menace précisément.

Le deuxième évènement est la guerre du Golfe Persique. Celle-ci a démontré au gouvernement et à l'ensemble de la population les carences de sécurité par rapport aux cybermenaces, des systèmes informatiques du Département de la Défense des États-Unis, mais aussi de tous les autres en général. Cet évènement va forcer le gouvernement à entamer des préparatifs pour améliorer la sécurité de ses ordinateurs. (Cavelty, 2007). Finalement, il n'y a pas de cadre motivationnel du cyberterrorisme, car le gouvernement s'intéresse aux cybermenaces et pas au cyberterrorisme spécifiquement. Toutefois, cet événement dévoile les risques que constituent les cybermenaces au gouvernement et la population des États-Unis.

Cette idée est réitérée par Winn Schwartau et le rapport *Computers at Risk*. Bien qu'ils constatent le danger que pourrait représenter le cyberterrorisme, ils considèrent avant tout que les États-Unis se doivent de protéger virtuellement leurs infrastructures essentielles. Ainsi, le danger du cyberterrorisme constitue une cybermenace parmi tant d'autres. Un exemple révélateur de cette situation est l'*electronic Pearl Harbor*. Ce terme ne s'intéresse pas à la partie belligérante, celle qui menace. Il examine la cible, soit les infrastructures essentielles, et à ses conséquences pour la nation (Schwartau, 1994 ; États-Unis. National Research Council. 1991.). Dans cette optique, Schwartau et le rapport *Computers at Risk* espèrent rallier et obtenir le soutien de la population des États-Unis par rapport à la nécessité de mettre

sur pied des mesures pour protéger virtuellement les infrastructures essentielles. Pour arriver à cette fin, ils ont aussi recours au vocabulaire exprimant l'entrée des États-Unis dans une nouvelle ère. Par exemple, il écrit : « However, in this period of rapid change, significant damage can occur if one waits to develop a countermeasure until after an attack is manifest. » (Ibid., p. 11). Selon leur logique, cette nouvelle période amène de nouvelles menaces et les États-Unis doivent développer de nouvelles politiques pour se protéger. Il est donc nécessaire, pour la population, d'appuyer les actions du gouvernement en vue de protéger virtuellement les infrastructures essentielles.

Schwartau va au-delà du document *Computers at risk* en proposant son *National Information Policy*. Sa proposition est très significative pour notre analyse du cadre motivationnel et comme nous l'avons déjà souligné à la section 3.2.2, il ne désire pas écrire un texte de loi, mais amorcer une discussion sur les diverses problématiques reliées au cyberespace. Parmi ces problématiques se trouvent celle des cybermenaces et de la protection des infrastructures essentielles. Néanmoins, malgré ses suggestions, ce qu'il souhaite, avant tout, c'est d'indiquer les obstacles et de les élucider en tant que nation, c'est-à-dire avec l'aide des citoyens, du gouvernement et des industries. Nous pouvons affirmer que cela constitue une tentative d'imposition d'un cadre motivationnel lorsqu'il dit : « With luck the following outline will be a call for action [...] ». (Ibid., p. 320). Pourtant, il ne tente pas d'établir un cadre motivationnel du cyberterrorisme. C'est un appel à l'action pour résoudre une multitude de difficultés touchant le cyberespace comme nous l'avons souligné à la section 3.2.2.

Aussi, il désire commencer une discussion collective sur la problématique très générale du cyberespace lorsqu'il affirme : « [...] then let the debate begin ! » (Ibid., p. 353). Cette dernière phrase reste intéressante. Elle permet de soutenir que Schwartau n'a pas tenté de sécurisation, car il demande un débat public. En fait, il sollicite une action politique qui se conforme aux règles et aux normes établies par le système législatif états-unien ce qui n'est pas le cas lors d'une tentative de sécurisation.

En somme, le gouvernement et les experts de la sécurité n'ont pas cherché à mettre en place un cadre motivationnel du cyberterrorisme pour faire du cyberterrorisme un enjeu de sécurité aux États-Unis. Nous soutenons qu'ils ont essayé de rallier le public états-unien sur les menaces qui peuvent émaner du cyberespace et qui peuvent nuire aux infrastructures essentielles. Dans cette optique, ce cadre ne se réduit pas seulement au cyberterrorisme, mais à l'ensemble des cybermenaces.

4.2 L'influence du *Presidential Commission on Critical Infrastructure Protection* sur le cadre motivationnel du cyberterrorisme

Dans cette section, nous soutenons que le gouvernement et les experts de la sécurité n'ont pas développé un cadre motivationnel du cyberterrorisme en lien avec la PCCIP. Nous considérons qu'ils ont construit un cadre motivationnel pour la protection des infrastructures essentielles.

4.2.1 Le cas du gouvernement

Le gouvernement et les experts de la sécurité n'ont pas cherché à mettre en place un cadre motivationnel du cyberterrorisme en lien avec la PCCIP. Nous verrons que les deux parties tenteront de rallier la nation autour de la problématique de la protection des infrastructures essentielles et plus précisément, ils essayeront de bâtir une coopération entre le secteur privé et public sur cette problématique.

Nous constatons que malgré que la PCCIP et certains experts de la sécurité définissent le cyberterrorisme comme une des menaces, ce n'est pas la seule qu'ils entrevoient. Comme nous l'avons mentionné à la section 2.3.1, la menace identifiée est représentée de manière très large et comprend les États, les criminels et les terroristes. Dans cette optique, si le cadre motivationnel désire rallier la population contre un ennemi, il le fera contre l'ensemble des acteurs pouvant constituer une cybermenace pour les États-Unis.

Toutefois, nous constatons que la période de la PCCIP se concentre sur la protection des infrastructures essentielles. Cette dernière constitue le prolongement logique de la réflexion entamée après le rapport *Computers at Risk*, la révolution militaire et l'attentat d'Oklahoma City. Les documents de la période précédente, comme nous l'avons mentionné dans la section 2.2, soutiennent que la protection de ces systèmes informatiques demeure déficiente et que ces infrastructures essentielles sont menacées. C'est pour cette raison que la PCCIP et des spécialistes de toutes sortes de domaines ont tenté d'analyser les vulnérabilités et de mettre sur pied une stratégie permettant d'améliorer la protection virtuelle de ces infrastructures. Cette stratégie est principalement basée sur une coopération entre le secteur public et le secteur privé. L'argument principal réside dans le constat que 80 % à 85 % des infrastructures essentielles des États-Unis sont détenues par le secteur privé. Alors, si ce dernier ne se munit pas des mesures adéquates pour diminuer les vulnérabilités de ses infrastructures, la majorité de celles-ci seront vulnérables, ainsi que la sécurité de la nation. Donc, la PCCIP représente un cri de ralliement pour tous les propriétaires d'infrastructure essentielle. Elle désire leur montrer l'importance des infrastructures essentielles privées et les motiver à prendre des dispositifs pour en améliorer la défense par rapport aux cybermenaces. Cette citation de cette commission illustre bien ce propos : « Waiting for disaster is a dangerous strategy. Now is the time to act to protect our future. » (President's Commission on Critical Infrastructure Protection, 1997, p. 6). Par conséquent, nous soutenons que la période de la PCCIP et précisément, la commission contient un cadre motivationnel à propos de la protection virtuelle des infrastructures essentielles.

4.2.2 Le cas des experts de la sécurité

Nous constatons que la plupart des experts de la sécurité sont satisfaits de cette stratégie. La raison principale de cet accord est qu'une partie importante de ces derniers ont participé à son élaboration. De plus, ils représentent de grandes firmes, comme Microsoft, IBM ou Cisco, détenant un intérêt marqué pour ce sujet. Alors, ils souhaitent que les propriétaires

d'infrastructures essentielles utilisent leurs nouveaux produits afin de diminuer leurs vulnérabilités par rapport aux cybermenaces.

En ce qui concerne les autres experts, aucun ne nie la nécessité de continuer à améliorer, lorsqu'il est nécessaire, la protection virtuelle des systèmes informatiques. Leurs désaccords se situent, surtout, au niveau des risques que courent les infrastructures essentielles. Selon eux, les dangers auxquels ils font face sont surestimés. Ils mettent l'accent sur la sous-évaluation de la résilience des installations et ils soutiennent que la présence de protocoles de sécurité et la supervision humaine sont adéquates pour leur permettre de résister à la majorité des attaques. Donc, ils ne sont pas convaincus de la nécessité de grands travaux d'amélioration de la sécurité des infrastructures essentielles. Ils appuient les mesures existantes, soit des analyses de sécurité et des mises à jour périodiques des infrastructures (Embar-Seddon, 2002; Denning, 1999; Dunnigan, 2002).

En somme, le gouvernement et les experts de la sécurité n'ont pas tenté de mettre en place un cadre motivationnel du cyberterrorisme autour de la PCCIP. Ils ont bâti un cadre motivationnel pour la protection des infrastructures essentielles basé sur une coopération entre le secteur privé et public.

4.3 Le cadre motivationnel du cyberterrorisme pendant la période de 1997-2001

Dans cette section, nous soutenons que le gouvernement n'a pas tenté de mettre en place un cadre motivationnel du cyberterrorisme. Quant à eux, les experts de la sécurité ont mis sur pied un cadre motivationnel du terrorisme. Ils ont été en mesure de toucher l'imaginaire collectif de la population états-unienne, mais ils n'ont pas été capables d'influencer le gouvernement.

4.3.1 Le cas du gouvernement

Nous commencerons par examiner la situation du gouvernement durant cette période et nous traiterons par la suite de celui des experts de la sécurité. Comme nous l'avons déjà mentionné dans les sections 2.4 et 3.3, les documents subséquents à la PCCIP demeurent relativement identiques en ce qui concerne le cadre diagnostique et pronostique. Ces derniers définissent toujours la menace à laquelle font face les infrastructures essentielles de manière très large en incluant le cyberterrorisme, mais en n'oubliant pas la possibilité de cyberattaque menée par un État étranger ou un groupe criminel. De plus, la stratégie pour protéger les infrastructures essentielles des cybermenaces est basée sur une coopération entre le secteur privé et public. Nous remarquons que le gouvernement utilise la même stratégie afin de protéger ses installations. Alors, il est logique de constater que le cadre motivationnel est le même. En effet, il désire rallier la nation, mais surtout le secteur privé, à l'enjeu de la protection des infrastructures essentielles (États-Unis. White House, 2001c). Le *National Plan for Information Systems Protection* illustre bien cette idée lorsqu'il écrit : « This effort will only succeed if our Nation as a whole rises to this challenge. » (White House, 2000b, p. iii).

4.3.2 Le cas des experts de la sécurité

Le point de vue des experts de la sécurité sur la problématique du cyberterrorisme est divisé comme nous l'avons décrit dans la section 2.4.2. Une partie des experts conçoit la possibilité d'attentat cyberterrorisme, mais juge qu'elle est peu probable. Ils estiment alors que les efforts devraient être concentrés sur d'autres aspects de la sécurité de la nation. Certains préconisent une amélioration de la protection des infrastructures essentielles. Ils croient que le gouvernement ne doit pas canaliser son ardeur sur la menace du cyberterrorisme. Dans ces conditions, ils ne cherchent pas à imposer un cadre motivationnel du cyberterrorisme. Au contraire, ils tentent de conserver ce statu quo, c'est-à-dire qu'ils définissent le cyberterrorisme comme une cybermenace parmi tant d'autres. Ils envisagent

donc qu'elle puisse être gérée de manière traditionnelle comme c'est le cas des armes de destruction massive (Denning, 1999; 2001).

L'autre camp est constitué d'experts de la sécurité considérant qu'il faut agir immédiatement contre la menace du cyberterrorisme. Dans cette optique, ils pressent le gouvernement et le secteur privé à se parer contre le cyberterrorisme en réduisant la vulnérabilité virtuelle des infrastructures essentielles. Leur principal argument est que les États-Unis ne doivent pas attendre de subir une attaque pour déployer des efforts en prévision de se prémunir contre une telle menace. Afin de promouvoir ce message, les experts de la sécurité ont eu recours à l'utilisation de simulation comme *Eligible Reicever 97* et de scénarios de fiction, comme ceux des pannes de courant, pour démontrer le danger que constitue le cyberterrorisme pour les infrastructures essentielles, mais aussi pour l'ensemble de la nation (Arquilla, 1998). Malgré les critiques qu'ont reçues ces simulations et scénarios, ils ont obtenu une importante propagation médiatique. Nous notons que certaines des expressions utilisées telles qu'*Electronic Pearl Harbor* et *Weapons of mass disruption*, ont réussi à toucher l'imaginaire collectif (Conway, 2008). Un excellent exemple est la diffusion du documentaire *Dangers on the Internet Highway : Cyberterror* par le réseau Fox en 1999 (Debrix, 2008). Nous affirmons que ces experts ont proposé un cadre motivationnel du cyberterrorisme et qu'il a été présenté aux citoyens. Toutefois, nous ne pouvons pas déterminer si la population a accepté ce cadre et nous n'avons pas noté de modification sur la question du cyberterrorisme par le gouvernement.

En somme, le gouvernement n'a pas imposé un cadre motivationnel du cyberterrorisme. Pour leur part, les experts de la sécurité ont posé un cadre motivationnel du cyberterrorisme, mais ils n'ont pas réussi à influencer le gouvernement.

4.4 Le cadre motivationnel du cyberterrorisme après les évènements du 11 septembre

Après les attentats du 11 septembre 2001, nous soutenons que le gouvernement n'a pas développé un cadre motivationnel du cyberterrorisme malgré tous ses efforts pour lutter contre le terrorisme. De plus, nous maintenons que les experts de la sécurité ont modifié leur cadre motivationnel après les attentats du 11 septembre, mais que ce cadre n'a pas réussi à influencer le gouvernement. Nous débuterons avec la situation du gouvernement pour ensuite passer aux experts de la sécurité.

4.4.1 Le cas du gouvernement

À première vue, les attentats du 11 septembre 2001 auraient dû raviver l'intérêt du gouvernement pour le cyberterrorisme vu la proximité entre ce concept et celui du terrorisme traditionnel. Néanmoins, ça n'a pas été le cas. Nous avions déjà remarqué à la section 3.4.1 que le gouvernement a augmenté son intérêt et ses efforts pour lutter contre le terrorisme traditionnel et que son attention pour les cybermenaces a diminué. Il est vrai qu'ils ont commandé des études sur les capacités informatiques de groupes terroristes musulmans. Toutefois, ils considèrent qu'une cyberattaque terroriste serait effectuée dans le but de nuire physiquement aux infrastructures essentielles comme nous l'avons mentionné à la section 2.5.1. De plus, nous croyons que l'omission du terme *cyber* dans les *National Security Strategy* à partir de 2002, démontre une certaine perte d'intérêt du gouvernement des États-Unis pour les cybermenaces (White House, 2002).

Nous avons aussi constaté que Richard Clarke n'a pas réussi à imposer le cyberterrorisme comme un enjeu de premier plan aux États-Unis. Ce dernier a été nommé par le Président Clinton comme le premier *National Coordinator for Security, Infrastructure Protection, and Counterterrorism* en mai 1998 et a continué à occuper ce poste sous le Président George W. Bush jusqu'en mars 2003. Il est un des seuls fonctionnaires états-uniens à avoir ouvertement déclaré la nécessité pour les États-Unis de se prémunir spécifiquement

contre le cyberterrorisme (Cavelty, 2007). Les évènements du 11 septembre viennent mettre définitivement un terme à son objectif. En fait, au début et après la commission sur les attentats du 11 septembre 2001, les défenseurs du gouvernement Bush, ont mené une campagne de diminution de la crédibilité de Richard Clarke. Cette dernière a été sans pitié. L'éditorialiste Paul Krugman la qualifie comme : « a campaign of character assassination » (2004, p. A11). Aussi, ses multiples déclarations lors de cette commission sont porteuses de contradictions qu'il explique par la demande du gouvernement Bush de tenter de minimiser l'importance de sa responsabilité dans les évènements du 11 septembre. À la suite de ces évènements, il a perdu beaucoup de crédibilité. Ceci peut expliquer, en partie, son échec à imposer le cyberterrorisme comme un enjeu de premier plan aux États-Unis. De plus, il a démissionné en 2003.

4.4.2 Le cas des experts de la sécurité

En ce qui concerne les experts de la sécurité, la situation a peu changé depuis la dernière période étudiée. Ils sont toujours divisés sur la question du cyberterrorisme comme nous l'avons mentionné dans la section précédente. La différence fondamentale entre les deux périodes est l'impact des évènements du 11 septembre. Alors que le gouvernement a réduit son intérêt pour les cybermenaces au profit du terrorisme traditionnel, les experts de la sécurité ont tenté de les réintroduire dans la liste de priorité du gouvernement. Nous notons que leur tentative a échoué.

Aussi, nous constatons que, depuis les évènements du 11 septembre, le nombre de livres publiés sur le cyberterrorisme augmente rapidement. Une recherche sur le site *Worldcat.org*, un site qui compile des milliers de catalogues de bibliothèque majoritairement universitaire à travers le monde, avec comme mot clé « cyberterrorism », nous indique que 33 livres ont été publiés en 2000 sur le sujet du cyberterrorisme comparativement à 80 livres pour l'année 2001. Par la suite, il y a eu 90 livres publiés en 2002 comparativement à 100 livres en 2003 sur ce même sujet.

Nous avons aussi remarqué que les auteurs de ces publications ont continué à exiger une intervention du gouvernement contre le cyberterrorisme en utilisant les mêmes justifications que durant la période de 1997-2001. Il y a une différence et elle réside dans l'ajout de la nécessité de l'action du gouvernement et du secteur public pour contrer le cyberterrorisme. Les évènements du 11 septembre pourraient, selon eux, se reproduire dans le cyberespace (Verton, 2003 ; Ashley, 2003). Il y a, donc, une plus grande urgence. En effet, l'ouvrage de Dan Verton, Black Ice, est une métaphore de ce danger. Il compare le danger du cyberterrorisme à la glace noire qui se forme sur les routes. Cette glace est dangereuse pour les automobilistes, car elle est difficile à apercevoir et lorsqu'un automobiliste roule dessus, elle peut causer une perte de contrôle de son véhicule et causer un accident. Ainsi, Dan verton écrit :

> «We must look closely for the warning signs that exist in the ether, and in our own vulnerabilities, and ensure that the high-tech future of terrorism does not become like black ice stretched across the information superhighway - alerting us to its presence only after we are spinning out of control.» (Ibid., p. xxviii).

Ainsi, il lance un avertissement contre la menace du cyberterrorisme et de ces conséquences. Cet énoncé est surtout un appel à l'action à l'attention du gouvernement.

De plus, ils croient que les groupes terroristes musulmans, spécialement Al-Qaïda, se préparent à utiliser le cyberterrorisme contre les infrastructures essentielles des États-Unis (Ibid.). Les experts de la sécurité ont tenté d'employer les évènements du 11 septembre pour justifier une action du gouvernement et du secteur public contre la menace du cyberterrorisme.

Nous remarquons que cette tentative de ralliement contre le cyberterrorisme a échoué, bien qu'ils ont réussi à démontrer, surtout à la population, les risques du cyberterrorisme. En effet, un sondage effectué en 2001 dans les dix-neuf villes les plus importantes au monde relève que 75 % des usagers d'Internet ont peur du cyberterrorisme. Un autre sondage fait

en 2003 par le *Federal Computer Week*, le *Pew Internet* et l'*American Life Project*, conclut que plus de 50 % des États-Uniens ont peur que des terroristes effectuent des cyberattaques sur les infrastructures essentielles (Conway, 2005). Avec de tels résultats, il nous semble pertinent de s'interroger sur la raison qui fait en sorte que les citoyens et le gouvernement n'ont pas soutenu l'effort des experts de la sécurité.

Nous arrivons à la conclusion que le gouvernement n'a pas été influencé par les experts de la sécurité et n'a pas tenté de rallier l'opinion publique contre le cyberterrorisme, car il avait ultérieurement indiqué cette menace, ainsi que l'ensemble des cybermenaces. Aussi, il avait déjà entrepris une réflexion et il avait amorcé des actions directes pour contrer les cybermenaces en général. Étant donné qu'il avait pris des mesures préventives et qu'aucune situation d'urgence n'est survenue, il pouvait continuer sa réflexion et la mise en place de ses dispositions de façon traditionnelle, c'est-à-dire en respectant les règles et les normes du système politique états-unien.

CONCLUSION

Dans ce mémoire, nous avons entamé une réflexion exploratoire sur l'enjeu du cyberterrorisme aux États-Unis. Nous avons remarqué que la documentation sur ce sujet est mince et qu'elle consiste à donner des conseils pratiques. Aussi, nous avons relevé que les experts de la sécurité semblaient très préoccupés par cet enjeu et que nous n'avions pas une bonne compréhension du processus de sécurisation. Dans cette optique, nous avons noté qu'un texte, de Myriam Cavelty, s'intéressait aux tentatives du gouvernement des États-Unis pour faire du cyberterrorisme un enjeu de sécurité, mais elle ne traitait pas de la prépondérance des experts sur cette problématique. Croyant qu'ils ont eu une influence et qu'ils ont peut-être cherché à sécuriser cet enjeu, nous avons décidé d'explorer cette avenue. Par conséquent, nous nous sommes résolus à déterminer leur importance sur cette problématique. Plus spécifiquement, nous nous sommes posé la question suivante : comment les experts de la sécurité tentent-ils de faire du cyberterrorisme un enjeu de sécurité aux États-Unis depuis la fin des années 1990 et quelles sont les variables qui influencent la réussite ou l'échec de ces tentatives?

Pour parvenir à répondre à cette question, nous avons décidé d'utiliser la même approche théorique que Cavelty. Celle-ci se nomme la théorie du cadrage. Elle intègre la théorie de la sécurisation de l'école de Copenhague et va au-delà. Cette théorie postule qu'une tentative de sécurisation est réussie lorsqu'un enjeu est perçu par l'ensemble de la population comme une menace importante à leur existence et nécessite des actions qui passent outre les normes et les lois établies par le système politique. Pour ce faire, l'acteur tentant la sécurisation fera un cadrage. Nous le définissons comme le choix subtil de certains

aspects d'un problème dans le but d'obtenir une réponse particulière à celui-ci. Pour ce mémoire, nous avons retenu trois types de cadres pertinents pour notre analyse.

Le premier type de cadre est appelé cadre diagnostique. Il consiste à déterminer clairement un problème et à assigner le blâme sur un agent ou une agence précis. En d'autres mots, le cadre définit ce qui est menacé et qui le menace.

Le second type de cadre est appelé cadre pronostique. Ce cadre a pour fonction d'offrir des solutions afin de protéger ce qui est menacé. De plus, ce cadre explique la manière dont il faut procéder pour arriver à ces solutions.

Le troisième type de cadre est le cadre motivationnel. Il a pour objectif de rallier la population à la lutte contre la menace et, souvent, il incite à la prise d'action concrète par ce dernier.

L'utilisation de cette théorie nous permet de déterminer si les experts de la sécurité ont tenté de faire du cyberterrorisme un enjeu de sécurité. De plus, elle nous laisse établir s'ils ont influencé le gouvernement sur cet enjeu. Dans un dernier temps, elle nous permet d'observer les variables qui influencent l'échec ou la réussite dans une tentative de sécurisation et donc, d'améliorer notre compréhension du processus de sécurisation.

Pour opérationnaliser notre cadre théorique, nous avons analysé les trois types de cadres par rapport aux textes d'experts de la sécurité sur la question du cyberterrorisme. De cette façon, nous avons exposé les cadres explicités par les experts de la sécurité. Par la suite, nous avons déterminé s'il y a eu sécurisation, car une fois qu'un cadre est accepté par un auditoire, il influence l'action des acteurs et en définit le sens pour le reste de la population (Cavelty, 2007). L'acceptation du cadre par les acteurs décisionnels et le reste de la population reste un critère qui a guidé notre démarche.

Avant de passer au second critère, il est important de spécifier comment nous déterminons qu'un auditoire accepte, ou non, un cadre. Nous avons utilisé des sondages états-uniens sur le terrorisme en général, mais aussi sur le cybercrime et les cybermenaces. Néanmoins, l'utilisation de sondage n'est pas toujours nécessaire. En fait, lorsque nous établissons que les experts de la sécurité n'ont pas influencé le gouvernement, il n'est pas capital de connaître l'opinion du public états-unienne, car la tentative de sécurisation a échoué.

Le second critère est temporel. En réalité, il est important que le cadre présenté par les experts de la sécurité soit confectionné avant celui des acteurs décisionnels. Aussi, si ces derniers ont déjà créé des cadres sur le sujet avant les experts de la sécurité, il est probable que ce soit eux qui sont influencés. Il est primordial de suivre l'évolution de ces cadres afin de déterminer si les experts de la sécurité se sont trouvés en mesure d'influencer les cadres retenus par les acteurs décisionnels.

Finalement, le dernier critère est que le cadre élaboré par les experts de la sécurité soit identique ou très semblable à celui des acteurs décisionnels. Nous ne pourrons parler de sécurisation réussie par les experts de la sécurité si leur cadre diffère de celui des acteurs décisionnels dans la mesure où celui-ci ne serait pas parvenu à être accepté comme cadre principal.

Notre démarche a été faite dans une perspective historique afin de nous assurer que les experts de la sécurité ont eu une influence sur les décisions en lien avec le cyberterrorisme. Plus précisément, nous avons analysé ces textes dans une perspective temporelle aux déclarations officielles du gouvernement des États-Unis. Cette étape nous a permis de nous donner l'assurance que ce sont bien les experts de la sécurité qui ont eu un effet sur les choix du gouvernement états-unien en matière de cyberterrorisme. Par conséquent, si nous avons retrouvé les cadres des experts de la sécurité dans les documents officiels du gouvernement états-unien a priori des textes des experts de la sécurité, il nous sera difficile d'établir leurs

influences sur les politiques touchant le cyberterrorisme. Finalement, nous avons procédé cadre par cadre afin de déterminer leur efficacité propre.

Maintenant, nous allons dévoiler nos résultats. Nous procéderons en examinant nos trois hypothèses de recherche secondaires. Par la suite, nous vérifierons notre hypothèse principale de recherche.

Notre première hypothèse concerne nos résultats du premier chapitre de ce mémoire. Elle est la suivante : « Le cadre diagnostique a été bien établi par les experts de la sécurité, car ils ont réussi à cibler un ennemi, les cyberterroristes, et ce qu'ils menacent, les services essentiels des États-Unis ». Elle n'est pas vérifiée. En fait, les experts de la sécurité ont bel et bien tenté d'identifier les cyberterroristes comme l'ennemi. Toutefois, le gouvernement ne les a pas identifiés spécifiquement. Ils ont défini le cyberterrorisme comme une cybermenace parmi tant d'autres. Néanmoins, les infrastructures essentielles ont été définies comme des cibles potentielles. En d'autres mots, elles sont considérées comme menacées. Cette identification a été effectuée par certains experts de la sécurité en concert avec le gouvernement. Dans cette optique, le gouvernement a ciblé les cybermenaces comme l'ennemi et les infrastructures essentielles comme ce qui est menacé. Donc, les deux cadres sont différents.

Notre seconde hypothèse concerne nos résultats du deuxième chapitre de ce mémoire. Elle est la suivante : « Le cadre pronostique n'a pas été bien établi par les experts de la sécurité, car ils n'offrent pas de réelle solution contre la menace qu'ils ont désignée ». Cette hypothèse n'est pas vérifiée. En fait, nous avons remarqué que les politiques, les stratégies et les solutions proposées par les experts de la sécurité pour contrer le cyberterrorisme et protéger les infrastructures essentielles sont celles avancées auparavant par le gouvernement. Nous observons que quelques experts ont participé à la création de la stratégie de base du gouvernement, soit la PCCIP. Toutefois, ils n'ont pas apporté d'amélioration ou d'innovation à cette stratégie. Les seules améliorations que nous avons constatées sont de nouveaux logiciels ou de récentes techniques de protection de système informatique. Alors, nous

concluons que le cadre pronostique n'a pas été bien établi par les experts de la sécurité, car la stratégie proposée pour protéger les infrastructures essentielles, soit la coopération, entre le secteur public et le secteur privé convient aux experts malgré leurs faibles résultats.

Notre troisième hypothèse concerne nos résultats du troisième chapitre de ce mémoire. La troisième est la suivante : « Le cadre motivationnel n'a pas été bien établi par les experts de la sécurité, car ils ne sont pas capables de rallier l'opinion publique contre la menace du cyberterrorisme, car celui-ci reste une menace théorique ». Cette hypothèse n'est pas vérifiée. En fait, nous avons constaté qu'ils ont tenté d'utiliser les évènements du 11 septembre pour justifier une action du gouvernement et du secteur public contre la menace du cyberterrorisme. Cet essai n'a pas réussi avec le gouvernement. Toutefois, nous observons qu'ils sont parvenus à toucher à l'imaginaire politique du reste de la population. Aussi, nous avons remarqué que le cyberterrorisme est maintenant présent dans les produits culturels états-uniens.

Nous arrivons à la conclusion que la population n'a pas appuyé les experts de la sécurité dans leur tentative de faire du cyberterrorisme un enjeu de sécurité parce que le gouvernement avait déjà défini cette menace, parmi l'ensemble des cybermenaces. De plus, il avait déjà amorcé une réflexion et il avait entrepris des actions directes pour contrer les cybermenaces en général. Étant donné qu'il avait implanté des dispositifs préventifs et qu'aucune situation d'urgence n'est survenue, il pouvait continuer sa réflexion et la mise en place de ses mesures de façon traditionnelle, c'est-à-dire en respectant les règles et les normes de leur système politique.

Nous pouvons maintenant vérifier notre hypothèse de recherche principale. Elle est la suivante : « Les experts de la sécurité ont échoué dans leurs tentatives pour faire du cyberterrorisme un enjeu de sécurité aux États-Unis depuis la fin des années 1990 ». Cette hypothèse est vérifiée. Nous constatons que les experts de la sécurité ont échoué dans leurs tentatives de sécurisation, car l'analyse du cadre diagnostique, pronostique et motivationnel nous indique qu'ils n'ont jamais été en mesure d'influencer le gouvernement des États-Unis.

Bien que d'autres études plus approfondies soient requises, nous croyons avoir trouvé deux variables qui expliquent l'échec de ces tentatives. La première est le manque d'innovation des experts de la sécurité pour lutter contre le cyberterrorisme et protéger les infrastructures essentielles. Nous soutenons que ce manque d'innovation à diminuer leur chance d'une sécurisation réussit, car il s'avère plus difficile de convaincre un auditoire de la nécessité de réagir à une menace lorsqu'ils ne proposent pas de nouvelles solutions.

La seconde variable est l'absence d'attentat de cyberterrorisme et d'accident grave relié aux cybermenaces. Étant donné que le gouvernement a pris des mesures préventives et qu'aucune situation d'urgence n'est survenue, ils ont pu continuer leur réflexion et la mise en place de leurs mesures de façon traditionnelle, c'est-à-dire en respectant les règles et les normes de leur système politique. Alors, la nécessité d'entreprendre un processus de sécurisation diminue.

Nous terminons en offrant trois pistes de réflexion sur cette problématique. Premièrement, nous croyons que l'enjeu du cyberterrorisme est à son début. Dans cette optique, il serait intéressant d'observer l'impact d'une cyberattaque d'envergure sur les infrastructures essentielles. Ainsi, il nous serait possible d'étudier l'influence de cette attaque sur les politiques du gouvernement. De plus, il serait captivant d'étudier les discours des experts de la sécurité à la suite de cette attaque.

Notre seconde piste de réflexion vise la théorie de la sécurisation. Nous croyons qu'il serait judicieux de continuer son développement théorique. En effet, une meilleure compréhension du processus de sécurisation pourrait nous aider à mieux cerner les problématiques qui sont ciblées par ce processus et les raisons de ses choix.

Notre dernière piste de réflexion concerne l'énoncé du Président Barack Obama. Le 29 mai 2010, il a affirmé qu'il souhaite rendre sécuritaires les ordinateurs les plus vitaux pour la

sécurité économique et la sécurité nationale. Il serait intéressant d'analyser s'il utilisera une stratégie identique à la PCCIP ou s'il tentera une nouvelle approche et d'observer les réactions des experts de la sécurité sur ce dossier.

BIBLIOGRAPHIE

Albele-Wigert, Isabelle et Myriam Dunn. 2006. *An inventory of 20 national and 6 international critical information infrastructure protection policies*. T. 1 de *The international CIIP handbook 2006*. Zurich: Center for Security Studies.

Alexander, Michael. 1990. «High-Tech Boom Opens Security Gaps». *Computerworld*, vol. 24, no 14, p. 118-119.

Allen-Tonar, Larry. 1989. «Networked Computers Attract Security Problems' Abuse». *Networking Management*, vol. 7, no 12, p. 48-53.

Arquilla, John, et David Ronfeldt. 1993. «Cyberwar is Coming!». *Comparative Strategy*, vol. 12, no 2, p. 141-165.

Arquilla, John. 1998. «The Great Cyberwar of 2002». *Wired*, vol. 6, no 2. [En ligne]. [http://www.wired.com/wired/archive/6.02/cyberwar.html] (18 novembre 2009).

Ashley, Bradley. K. 2003. «Anatomy of Cyberterrorism: is America Vulnerable ?». Séminaire 10, Maxell (AL), Air War College. [En ligne]. [http://www.au.af.mil/au/awc/awcgate/awc/ashley.pdf] (6 avril 2010).

Bendrath, Ralph. 2001. «The cyberwar debate: Perception and politics in US critical infrastructure protection», *Information&Security: An International Journal*, vol. 7, p. 80-103.

Bequai, August. 1999. «Cyber-crime the US experience». *Computers & Security*, vol. 18, no 1, p. 16-18.

Beeson, Ann. 1996. «Top Ten Threats to Civil Liberties in Cyberspace». *Human Rights*, vol. 23, no 2, p. 10-13.

Bonditti, Philippe. 2001. «L'organisation de la lutte anti-terroriste aux États-Unis». *Cultures & Conflits*, vol. 44, p. 65-76.

Braillard, Phillippe, et Gianluca Maspoli. 2001. *La «Révolution dans les affaires militaires»: Paradigmes stratégiques, limites et illusions*. Paris: Ministère des affaires étrangères et européennes, p. 630-645. [En ligne]. [http://www.diplomatie.gouv.fr/fr/IMG/pdf/FD001464.pdf] (6 avril 2010).

Buzan, Barry, Ole Waever et Jaap de Wilde. 1998. *Security: A New Framework for Analysis*, Boulder, Lynne Rienner.

Campbell, David. 1998. *Writing Security: United States foreign policy and the politics of identity*. Minneapolis: University of Minnesota Press.

Carter, Ralph et James Scott. 2009. *Choosing to Lead*. Durkham: Duke University Press.

Cavelty, Myriam Dunn. 2007. «Cyber-Terror—Looming Threat of Phantom Menace? The Framing of the US Cyber-Threat Debate». *Journal of Information Technology Politics*, vol. 4, no 1, p. 19-36.

Ceyhan, Ayse. 1998. «Analyser la sécurité: Dillon, Waever, Williams et les autres». *Cultures & Conflits*, no 31-32. [En ligne]. [http://conflits.revues.org/index541.html] (6 avril 2010).

Ceyhan, Ayse et Gabriel Périès. 2001. «Introduction. L'ennemi intérieur: une construction discursive et politique». *Cultures & Conflits*, no 43, p. 100-112.

Ceyhan, Ayse. 2004. «Sécurité, frontières et surveillance aux Etats-Unis après le 11 septembre 2001». Cultures & Conflits, no 53, p. 113-145.

Chakrabarti, Anirbam et G. Manimaran. 2002. «Internet Infrastructure Security: A Taxonomy». *IEEE Network*, vol. 16, no 6, p. 13-21.

Ciongoli, Adams G., Jennifer A. DeMarrais et James Wehner. 1994. «Computer-Related Crimes : Ninth Survey of White Collar Crime. ». *American Criminal Law Review*, vol. 31, no 3, p. 425-454.

Collier, Stephen J. et Andrew Lakoff. 2008. «The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem». In *Securing 'the Homeland'. Critical infrastructure, risk and (in)security*, sous la dir. de Myriam Dunn et Kristian Soby Kristensen, p. 17-39. Abingdon (NY): Routledge.

Conway, Maura. 2002. «Cyberterrorism: The Story so Far». In *Proceedings of the European Conference on Information Warfare and Security*, sous la dir. de Bill Hutchinson, p. 49-57. Kidmore End (Angl.): MCIL.

Conway, Maura. 2005. «The Media and Cyberterrorism: A Study in the Construction of 'Reality'». In The First International Conference on the Information Revolution and the Changing Face of International Relations and Security (Lucerne, 23-25 mai 2005). Lucerne (Suisse). [En ligne]. [http://se2.isn.ch/serviceengine/Files/CRN/46731/ieventattachment_file/F6C4C67B-787E-49CD-82DD-102705970C60/en/MConway_Terrorism.pdf] (24 mars 2009).

Conway, Maura. 2008. «Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures». In *Securing 'the Homeland'. Critical infrastructure, risk and (in)security*, sous la dir. de Myriam Dunn et Kristian Soby Kristensen, p. 109-129. Abingdon (NY): Routledge.

Dartmouth College, Institute for Security Technology Studies, Technical Analysis Group. 2003. *Examining the Cyber Capabilities of Islamic Terrorist Groups*. Hanover (NH): Dartmouth College. [En ligne]. [http://www.ists.dartmouth.edu/docs/ITB_032004.pdf] (24 mars 2009).

Dawson, John W. 2006. «Gödel and the origins of computer science». Note de cours, Pennsylvania: Pennsylvania State University. [En ligne]. [*www.cs.swan.ac.uk/cie06/files/d14/SwanseaAddress.ppt] (18 novembre 2009.*

Debrix, François. 2008. *Tabloid Terror: War, Culture and Geopolitics*. New York: Routledge.

Deibert, Ronald J. et Rafal Rohozinski. 2010. «Risking Security: Policy and Paradoxes of Cyberspace Security». *International Political Sociology*, vol. 4, no 1, p. 15-32.

Denning, Dorothy. 1999. «Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy». In *Networks and Netwars: The Future of Terror, Crime and Militancy*, sous la dir de John Arquilla et David Ronfeldt, p. 239-288. Santa Monica (CA): Rand Corporation.

Denning, Dorothy. 2000. «Cyberterrorism: The Logic Bomb versus the Truck Bomb». *Global Dialogue*, vol. 2, no 4, p. 29-37. [En ligne]. [http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc] (18 novembre 2009).

Desmedt, Yvo. 2006. «Robust Operations Research I: Introduction & Communication Networks». Londres: University College London. [En ligne]. [http://www.cs.ioc.ee/yik/schools/win2006/desmedt/communication-networks.pdf] (9 novembre 2009).

Dudley, Leonard M. 1991. *The word and the sword: how techniques of information and violence have shaped our world*. Cambridge (Mass.): Blackwell.

Embar-Seddon, A. 2002. «Cyberterrorism: are we under siege?». *American Behavioral Scientist*, vol. 45, no 6, p. 1033-1043.

États-Unis, Department of Homeland Security, National Cyber Security Division. 2006. *Cyber Storm. Exercise Report*. Washington: U.S. Government Printing Office.

États-Unis, Federal Emergency Management Agency. 2007. *Robert T. Stafford Disaster Relief and Emergency Assistance Act*. PL 100-707. Washington: U.S. Government Printing Office.

États-Unis, General Accounting Office. 1991. *Computer security hackers penetrate DOD computer systems: statement of Jack L. Brock, Jr., Director, Government Information and Financial Management, Information Management and Technology Division, before the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, United States Senate*. GAO/T-IMTEC-92-5 Washington: U.S. Government Printing Office.

États-Unis, General Accounting Office. 1996. *Operation Desert Storm: Evaluation of the Air War*. GAO/PEMD-96-10. Washington: U.S. Government Printing Office.

États-Unis, General Accounting Office. 2001. *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. Report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate*. GAO-01-323. Washington: The White House.

États-Unis, General Accounting Office. 2001. *Combating Terrorism, Comments on Counterterrorism Leadership and National Strategy*, GAO-01-556T. Washington: The White House.

États-Unis, General Accounting Office. 2004. *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems*. GAO-04-628T. Washington: The White House.

États-Unis, General Accounting Office. 2007. *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way but, Challenges Remain*. GAO-08-119T. Washington: The White House.

États-Unis, Homeland Security Council. 2007. *National Strategy for Homeland Security*. Washington: U.S. Government Printing Office.

États-Unis, National Security Council. 1984. *National Security Decision Directive Number 145: National policy on telecommunications and automated information systems security*. Washington: The White House.

États-Unis, National Research Council, Computer Science and Telecommunication Board, System Security Study Committee. 1991. *Computers at risk: safe computing in the information age*. Washington: National Academy Press.

États-Unis, Office of Homeland Security. 2002. *National Strategy for Homeland Security*. Washington: The White House.

États-Unis, President's Commission on Critical Infrastructure Protection. 1997. *Critical foundations: protecting America's infrastructures. The report of the President's Commission on Critical Infrastructure Protection*. Washington: U.S. Government Printing Office.

États-Unis, Transition President's Commission on Critical Infrastructure Protection et Critical Infrastructure Assurance. 1998. *Preliminary research and development roadmap for protecting and assuring critical national infrastructures*. Washington: U.S. Government Printing Office.

États-Unis, United States Congress. 1974. *Privacy Act of 1974*. Public Law 93-579. Washington: U.S. Government Printing Office.

États-Unis, United States Congress. 1986. *Electronic Communications Privacy Act of 1986*. Public Law 99-508. Washington: U.S. Government Printing Office.

États-Unis, United States Congress.1996. *Antiterrorism and Effective Death Penalty Act of 1996*. Public Law 104-132. Washington: U.S. Government Printing Office.

États-Unis, United States Congress. 2002. *Homeland Security Act of 2002*. Public Law 107-296. Washington: U.S. Government Printing Office.

États-Unis, United States Congress. 2007. *The High-Performance Computing Act of 1991 (Public Law 102-194) as amended by the Next Generation Internet Research Act of 1998 (P.L. 105-305) and the America COMPETES Act of 2007 (P.L 110-69)*. Washington: U.S. Government Printing Office.

États-Unis, White House, Office of the President of the United States. 1995. *A National Security Strategy of Engagement and Enlargement*. Washington: The White House.

États-Unis, White House, Office of the President of the United States. 1995. *Presidential Decision Directives 39: U.S. policy on counterterrorism*. Washington: The White House.

États-Unis, White House, Office of the President of the United States. 1996. *A National Security Strategy of Engagement and Enlargement*. Washington: The White House. [En ligne]. [http://www.fas.org/spp/military/docops/national/1996stra.htm] (18 novembre 2009).

États-Unis, White House, Office of the President of the United States. 1997. *A National Strategy for a New Century*. Washington: The White House. [En ligne]. [http://osdhistory.defense.gov/docs/nss1997.pdf] (18 novembre 2009).

États-Unis, White House, Office of the President of the United States. 1998. *A National Security for a New Century*. Washington: The White House.

États-Unis, White House, Office of the Press Secretary. 1998. *Combating Terrorism: Presidential Decision Directive 62*. Washington: The White House.

États-Unis, White House. 1998. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63*. Washington: The White House.

États-Unis, White House. 1999. *A National Security for a New Century*. Washington: The White House.

États-Unis, White House. 1999. *Executive order 13130. National Infrastructure Assurance Council*. Washington: The White House.

États-Unis, White House. 2000. *A National Strategy for a Global Age*. Washington: The White House.

États-Unis, White House. 2000. *National Plan for Information Systems Protection, Version 1.0: an Invitation to a Dialogue*. Washington: The White House.

États-Unis, White House. 2001. *Executive order 13228. Establishing the Office of Homeland Security and the Homeland Security Council*. Washington: The White House.

États-Unis, White House. 2001. *Executive order 13231. Critical Infrastructure Protection in the Information Age*. Washington: The White House.

États-Unis, White House. 2001. *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities. Washington*: The White House.

États-Unis, White House. 2002. *The National Strategy of the United States of America*. Washington: The White House.

États-Unis, White House. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington: The White House.

États-Unis, White House. 2003. *The National Strategy to Secure Cyberspace*. Washington: The White House.

États-Unis, White House. 2006. *A National Strategy of the United States of America*. Washington: The White House.

Eriksson, Johan. et Erik Noreen. 2002. *Setting the agenda of threats: An explanatory Model*. Document de recherche, Uppsala (Suisse), Université d'Uppsala. [En ligne]. [http://www.pcr.uu.se/pcr_doc/uprp/uprp_no_6.pdf] (12 juillet 2008).

Forno, Richard. 2000. *NIPC - A Failure To Communicate*. The Information Warfare Site. [En ligne]. [http://www.iwar.org.uk/cip/resources/nipc/2000-06.html] (10 novembre 2009).

Frieder, Gideon. 1998. «Panel 1». In *Cyber-Terrorism and Information Warfare : Threats and Responses* (Arlington, 16 avril 1998), sous la dir. de Yonah Alexander et Edgar H. Brenner, p. 9-10. Arlington: Potomac Institute for Policy Studies.

Fuhrman, Thomas A. 1998. «Panel 1». In *Cyber-Terrorism and Information Warfare : Threats and Responses* (Arlington, 16 avril 1998), sous la dir. de Yonah Alexander et Edgar H. Brenner, p. 12-14. Arlington: Potomac Institute for Policy Studies.

Gagnon, Benoît. 2009. *Cyberterrorisme, infoguerre et cyberorganisation* (Montréal, 10 juillet 2009). [En ligne]. [http://www.cerium.ca/IMG/pdf/GAGNON_-_PDF.pdf] (9 novembre 2009).

Giacomello, Giampiero. 2004. «Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism». *Studies in Conflict & Terrorism,* vol. 27, no 5, p. 387-408.

Gibson, Brian. 1978. *The Billion Dollar Bubble*. Coul., 60 min. Angleterre: British Broadcasting Corporation.

Gibson, William. 1984. *Neuromancer*. New York: Ace Books.

Gibson, William. 2003. *Burning chrome*. New York: HarperCollins Publishers.

Globalsecurity.org. (n.d.). *Eligible Receiver* [En ligne]. [http://www.globalsecurity.org/military/ops/eligible-receiver.htm] (4 janvier 2010).

Gordon, Sarah et Richard Ford. 2002. «Cyberterrorism?». *Computers & Security*, vol. 21, no 7, p. 636-647.

Hildreth, Steven A., Congressional Research Service, Report for Congress. 2001. *Cyberwarfare*. RL30735. Washington: U.S. Government Printing Office.

Horn, Julie. 2004. «Vers l'élaboration d'un régime international de contrôle du cyberterrorisme». Mémoire de maîtrise, Montréal, Univesité du Québec à Montréal.

Huysmans, Jef. 1998. «Dire et écrire la sécurité : le dilemme normatif des études de sécurité». *Cultures & Conflits*, no 31-32, p. 177-202.

Igure, Vinay M., Sean A. Laughter et Ronald D. Williams. 2006. «Security issues in SCADA networks». *Computers & Security*, vol. 25, no 7, p. 498-506.

Jackson, Richard. 2005. Writing *the War on Terrorism*. Manchester: Manchester University Press.

Kristensen, Kristian Soby. 2008. «The Absolute Protection of our Citizens: Critical Infrastructure Protection and the Practice of Security». Chap. In *Securing 'the Homeland'. Critical infrastructure, risk and (in)security*, p. 63-83. Abingdon (NY): Routledge.

Krugman, Paul. 2004. «This isn't America. The Bush team's form of rebuttal: character assassination». *Pittsburgh Post-Gazette* (New York), 3 avril, p. A11.

Kupperman, Robert H., Debra van Opstal et David Williamson Jr. 1982. «Terror, the Strategic Tool: Response and Control». *Annals of the American Academy of Political and Social Science*, vol. 463, p. 24-38.

Laqueur, Walter. 1996. «Postmodern Terrorism». *Foreign affairs*, vol. 75, no 5, p. 24-36.

League, S., D. Keyes, D. Knauf et M. Woods. 1997. «Plenary Panel Session: Critical Infrastructure Protection-The Cyber/Information Dimension: Report on National Infrastructure Coordination Initiatives». In *13th Annual Computer Security Applications Conference* (San Diego, 8-12 décembre 1997).

Libicki, Martin C. 1995. «The Next Enemy». *Strategic Forum 34* (février). [En ligne]. [http://www.ndu.edu/inss/strforum/SF_35/forum35.html] (Consulté le 11 novembre 2009).

Light, Jennifer S. 2002. «Urban security from warfare to welfare». *International Journal of Urban and Regional Research*, vol 26, no 3, p. 607-613.

Littleton, Matthew J. 1995. «Information Age Terrorism: Toward Cyberterror». Mémoire de maîtrise, Monterey, Naval Postgraduate School.

Lonsdale, David J. 1999. «Information Power: Strategy, Geopolitics and the Fifth Dimension». *Journal of Strategic studies*. vol. 22, no 2-3, p. 137-157.

Michel-Kerjan, Erwann. 2003. «New Challenges in Critical Infrastructures: A US Perspective». Working paper #03-25, Philadelphie:
Center for Risk Management and Decision Processes Center. [En ligne]. [http://opim.wharton.upenn.edu/risk/downloads/03-25-EMK.pdf] (18 novembre 2009).

Moteff, J., Congressional Research Service, Report for Congress. 2007. *Critical Infrastructure*: *The National Asset Database*. RL33648. Washington: U.S. Government Printing Office.

Moteff, J., Congressional Research Service, Report for Congress. 2008. *Critical Infrastructures*: *Background, Policy, and Implementation*. RL30153. Washington: U.S. Government Printing Office.

National Infrastructure Protection Center. 2002. *Terrorist Interest in Water Supply and SCADA Systems*. Information Bulletin 02-001. [En ligne]. [http://lists.jammed.com/crime/2002/01/0053.html] (14 décembre 2009).

Neale, Mark. 2000. *No Maps for These Territories : on the road with William Gibson*. Digital, coul., 89 min. États-Unis: Docurama.

Network World. 1990. «Network security stills lack». *Network World*. vol. 7, no 6, p. 33.

Nugent, J. H. et M. Raisinghani. 2007. «Bits and Bytes vs. Bullets and Bombs:A New Form of Warfare». In *Cyber Warfare and Cyber Terrorism*, sous la dir. de Janczewski, L. et A. M. Colarik, p. 26-34. Hershey: Idea Group Inc.

Paty, Michel. 1988. «Sur la nation de complétude d'une théorie physique». In *Leite Lopes Feschrift. A pioneer physicist in the third world*, sous la dir. de A. Troper, p. 143-164. Singapore: World Scientific Publishers.

Peterson, I. 1990. «Risky Business: Tackling Computer Security». *Science News*, vol 138, no 24, p. 373.

Rathmell, Andrew. 1997. «Cyber-Terrorism: The Shape of Future conflict?». *The RUSI Journal*, 142, no 5, p. 40-45.

Rathmell, Andrew. 1998. «Information warfare and sub-state actors: An organisational approach». *Communication & Society*, vol. 1, no 4, p. 488-503.

Roy, Simon N. 2003. «L'Étude de cas», In *Recherche sociale: de la problématique à la collecte des données*, sous la dir. de Benoît Gauthier, p. 159-184. Sainte-Foy (Qué.): Presses de l'Université du Québec.

Schmid, Alex Peter et Jongman, A. J., 2005, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature*. New Brunswick (NJ): Transaction Publisers, 726 p.

Schneidewind, N. 2007. «USA's View on World Cyber Security Issues». In *Cyber Warfare and Cyber Terrorism*, sous la dir. de Janczewski, L. et A. M. Colarik, p. 446-452. Hershey: Idea Group Inc.

Schwartau, Winn. 1994. *Information Warfare: Chaos on the electronic superhighway*. New York: Thunder's Mouth Press.

Schwartz, Paul M. 1999. «Privacy and Democracy in Cyberspace». *Vanderbilt Law Review*, vol. 52, no 6, p. 1607-1702.

Société Dictionnaire le Robert. 2009. «Le Nouveau Petit Robert. Dictionnaire Alphabétique et analogique de la langue française». Paris: Le Robert.

Stohs, Brett. 2002. «Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 Will Degrade the Freedom of Information Act». *Duke Law & Technology Reviews*, 18. [En ligne]. [http://www.law.duke.edu/journals/dltr/articles/pdf/2002DLTR0018.pdf] (4 octobre 2009).

Surnow, Joel et Robert Cochran. 2008. *24 heures chrono: Saison 7*. Coul., 1008 min. États-Unis: 20tth Century Fox.

Thomas, Timothy. 2000. «Kosovo and the Current Myth of Information Superiority». *Parameters*. vol. 30, no 1, p. 13-29.

Toffler, Alvin. 1980. *The third wave*. New York: Morrow.

Vatis, Micheal. A. 2001. *Cyber Attacks During the War on Terrorism: A Predictive Analysis*. Document de travail, Hanover (NH), Institute for Security Technology Studies, 27 p. [En ligne]. [http://www.ists.dartmouth.edu/library/221.pdf] (24 mars 2009).

Verton, Dan. 2003. *Black ice*: *the invisible threat of cyber-terrorism*. New York: McGraw-Hill/Osborne.

Vesper, James L. 2006. « A Incomplete History of Risk Management ». Chap. In *Risk Assessment and Risk Management in the Pharmaceutical Industry: Clear and Simple*, p. 1-8, Bethesda: PDA/DHI. [En ligne]. [https://store.org/bookstore/TableOfContents/Risk_Assessment_Ch01.pdf] (8 décembre 2009).

Wæver, Ole. 2004. «Aberystwyth, Paris, Copenhagen - New 'Schools' in Security Theory and their Origins between Core and Periphery». In *Geo-cultural Epistemologies in IR: Thinking Security Differently*: Actes de la 45ème Convention Annuelle de l'*International Studies Association* (Montréal, 17-20 mars 2004). [En ligne]. [http://www.allacademic.com/meta/p74461_index.html] (14 décembre 2009).

Weimann, Gabriel. 2005. «Cyberterrorism: the Sum of All Fears ?». *Studies in Conflict and Terrorism*, Vol. 28, No 2, p. 129-149.

Wiseman, Len. 2007. *Live Free or Die Hard*. Coul., 130 min. États-Unis: 20th Century Fox.

Yar, Majid. 2006. «Political Hacking: From Hacktivism to Cyberterrorism». Chap. in *Cybercrime and Society*, p. 45-62. Londres: Sage Publications Inc.

Yves Viltard. 2001. «Le cas McCarthy. Une construction politique et savante». *Cultures & Conflits*, no 43, p. 13-59.

Zanini, Michele et Sean J. A. Edwards. 2001. «The Networking of Terror in the Information Age». In *Networks and Netwars*: *The Future of Terror, Crime and Militancy*, sous la dir de John Arquilla et David Ronfeldt, p. 29-60. Santa Monica (CA): Rand Corporation.