La gestion du risque cyber à l'OTAN

Britanie Bernard

Thèse soumise à la

Faculté des Études Supérieures et Postdoctorales

Dans le cadre des exigences du programme de

Maîtrise ès arts en science politique

École d'Études Politiques

Faculté des Sciences Sociales

Université d'Ottawa

Remerciements

J’aimerais tout d’abord remercier mon directeur de recherche, le Professeur David Grondin, pour sa disponibilité et ses précieux conseils tout au long de ce parcours. La confiance qu’il m’a accordée et ses encouragements pour réaliser ce travail ont été cruciaux, particulièrement dans ces dernières semaines. Merci pour ta générosité et merci d’avoir cru en moi.

Je tiens à exprimer toute ma gratitude au Professeur Miguel de Larrinaga pour sa disponibilité et sa sympathie. Merci pour ta réactivité et tes recommandations bienveillantes qui m’ont permis de trouver ma voie malgré des débuts difficiles.

Un grand merci à Adib Benchérif, mon ami et mentor, qui a nourri ma réflexion tout au long de mes deux années passées à l’Université d’Ottawa. Merci de m’avoir initiée au monde passionnant de l’analyse de risque, qui a inspiré cette thèse et m’a donnée une motivation particulière à toutes les étapes de ma recherche.

Enfin, je tiens à remercier mes parents pour leur soutien indéfectible ainsi que pour m’avoir permis de venir étudier à l’Université d’Ottawa, et à plus forte raison de découvrir le Canada et son peuple si chaleureux. Cette expérience a profondément changé ma vie.

J’exprime ici ma plus sincère reconnaissance aux personnes mentionnées ici, qui ont toutes participé, à leur façon, à ce que cette thèse voit le jour.

Résumé

L'omniprésence des nouvelles technologies de l'information et de la communication (NTIC), dont la plus emblématique est sûrement Internet, est la caractéristique majeure de ce que Myriam Dunn Cavelty qualifie d' « âge de l'information ». Si les innovations sont très largement pensées et développées au sein d'entreprises privées, les gouvernements et les organismes publics ne sont toutefois pas désintéressés et l'on a assisté à une sécurisation du cyber, notamment par les États-Unis et l'OTAN. Cette recherche se veut être une contribution critique à la littérature sur la cyberdéfense de l'OTAN. Elle cherche à montrer que l'adaptation de l'OTAN au contexte stratégique post-guerre froide est passée par une mutation vers la gestion de risque comme mode de gouvernement. À travers l'étude de la doctrine de l'OTAN en matière de cyber défense, cette recherche se veut être l'occasion de réfléchir au rapport que l'OTAN entretien avec le concept de risque. Nous soutenons l'idée que cette doctrine est héritière de la gestion du risque terroriste conçue par l'Administration Bush au lendemain des attaques du 11 septembre 2001, mais également que l'OTAN semble avoir des difficultés à sortir de la logique de dissuasion. Grâce aux travaux du sociologue Ulrich Beck mais également des poststructuralistes en relations internationales, nous cherchons à montrer que la stratégie préemptive en place se caractérise entre autres par une perception disproportionnée des risques, ce qui a comme conséquence la création de plus de risques et l'aggravation du sentiment d'insécurité. Il est donc attendu que l'un des objectifs que nous poursuivons dans cette recherche est le décryptage de pratiques sécuritaires qui engendrent des dérives et qui sont néfastes à la création, à la mise en place et à l'exécution de solutions efficaces de cyber défense.

Table des matières

Mr. Marks, by mandate of the District of Columbia Precrime Division, I'm placing you under arrest for the future murder of Sarah Marks and Donald Dubin that was to take place today, April 22 at 0800 hours and four minutes.

(Minority Report, Steven Spielberg, 2002*)*

INTRODUCTION

Il y a 10 ans exactement, entre le 26 avril et le 18 mai 2007, les serveurs de grandes institutions publiques et privées estoniennes étaient victimes d'attaques par déni de service, c'est-à-dire qu'un flot très important de demandes de connexion avait été envoyé dans le but de saturer les serveurs et de les rendre inutilisables. Compte-tenu du contexte géopolitique à l'époque, la Russie avait été accusée, mais il est impossible de dire avec certitude qui est à l'origine de ces agressions. En effet, il est particulièrement difficile d'attribuer les attaques dans le cyberespace. À l'OTAN, cet événement a sonné l'alarme appelant à une prise de conscience collective de la vulnérabilité des infrastructures de l'organisation. Progressivement, la cybersécurité a été incluse dans les débats politiques et les réflexions militaires de l'OTAN en tant que nouveau risque à gérer. L'actualité nous rappelle sans cesse que les dynamiques politiques et militaires ont de plus en plus à avoir avec le cyberespace. En ce qui a trait à la sécurité, les nouvelles technologies de l'information et de la communication (NTIC) offrent un nouveau terrain de réflexion stratégique, un nouveau champ des possibles (Kempf 2015, Dunn Cavelty 2008, Dunn Cavelty 2012, Dunn Cavelty et Kristensen 2008). Il n'est donc pas rare d'observer une adaptation des doctrines et la naissance de nouvelles pratiques de sécurité. Nous allons nous intéresser à la gestion de risque en tant que pratique, car, comme le note Michael Williams : « The defining concept in international security today is not that of the threat. International affairs today is about the management of risks – the management of uncertainty that keeps the western world awake at night » (Williams 2009, 9). En effet, la mondialisation a rendu les sociétés interdépendantes, complexes et bien souvent, les

problèmes d'aujourd'hui sont transnationaux, qu'ils soient d'ordre financier ou économique (crise des *subprimes*), sanitaire (« maladie de la vache folle », Ebola), technologique (cyber attaques). En conséquence, les politiques sécuritaires des pays occidentaux ont évolué en délaissant les acteurs adversaires et leurs capacités pour s'intéresser à leurs propres vulnérabilités. Bien que ce changement se soit opéré de façon graduelle, nous allons voir que les attentats du 11 septembre 2001 et les cyberattaques vécues par l'Estonie en 2007 représentent des moment charnières où la vulnérabilité, respectivement des États-Unis et de l'OTAN, s'est matérialisée.

1. La conceptualisation du risque

En sciences sociales, le risque a réellement commencé à être étudié après la sortie de traduction en anglais de l'ouvrage du sociologue allemand Beck, *Risikogesellschaft: Auf dem Weg in eine andere Moderne*, traduit en 1992 sous le titre *Risk Society: Towards a New Modernity.* Dans cet ouvrage, Beck définit le risque de la façon suivante : « A systematic way of dealing with hazards and insecurities induced and introduced by modernization itself » (Beck 1992: 21). Beck (1944-2015) était un sociologue allemand qui a dédié une grande partie de sa carrière académique au concept de risque. Professeur notamment à l'Université de Munich, à la Fondation Maison de l'Homme à Paris et à la London School of Economics, il a tenté de comprendre les changements socio-politiques engendrés par la mondialisation et le changement de paradigme après la chute du Mur de Berlin et la fin de l'Union Soviétique.

La mondialisation constitue le fil rouge de la réflexion de Beck. La thèse de Beck permet de comprendre la transformation des politiques de sécurité occidentales, notamment en embrassant le concept de réflexivité. La réflexivité, selon Beck, se caractérise par un manque de contrôle sur les conséquences des prises de décision, puisque ces dernières sont prises en fonction de

probabilités estimées d'un scénario; par conséquence, « This fact makes you reflect one everything you are doing to others as if it was something you were doing to yourself » (Rasmussen 2001, 294). Par conséquence, le risque principal autour duquel une société postmoderne se construit est la société elle-même (Williams 2009, 18). Le risque est par essence virtuel; s'il se matérialise, ce n'est plus un risque. Une place primordiale est donc accordée à la subjectivité et à l'incertitude, ce qui laisse une grande marge d'interprétation aux décideurs politiques. La stratégie est donc une activité profondément sociale et il est intéressant de la considérer comme telle en adoptant une approche pluridisciplinaire. En effet, comme le rappelle Mythen, « The risk perspective has been pivotal in the evolution of cross-discipline debate between sociology, cultural studies, politics, geography and environmental studies » (Mythen 2004, 6).

Cependant, il est bon de rappeler que le risque n'est pas un concept nouveau. Les auteurs mobilisés pour cette recherche associent à l'unanimité la naissance du risque à l'époque des conquêtes maritimes et à l'exploration au début de l'époque moderne (fin XV^{ème} – début XVI^{ème} siècles). En assurance maritime, le risque représentait la différence entre les dangers potentiels et l'acquisition de nouvelles terres, de nouvelles découvertes. Étymologiquement, *risq* en arabe signifie la richesse et la bonne fortune. Cette conception du risque était largement associée au surnaturel, à la religion, à la magie, à la chance. En ce sens, la responsabilité de l'humain dans le risque était complètement exclue. Par la suite, le concept a pris un tournant économique. En effet, aux XVIII^{ème} et XIX^{ème} siècles, il fût lié au développement de l'industrie et aux risques pris par les entrepreneurs et les banquiers ; c'est à cette époque que l'humain est intégré au risque. De plus, pour la première fois, le risque a été mathématisé et calculé. Au XX^{ème}, il fût associé à la sphère financière et aux spéculations (Mythen 2004, Williams 2009, Coker 2002, Beck 2009, Luhmann 2005, Williams 2008). Le sociologue allemand Ulrich Beck caractérise cette époque, qu'il nomme

première modernité, par le fait d'assurer les risques liés à la modernisation économique. Ensuite, avec la mondialisation, les risques sont devenus difficiles à localiser et n'ont plus eu de limites spatio-temporelles : c'est la seconde modernité chez Beck qui a vu l'émergence de la société du risque, un concept sur lequel nous allons longuement revenir. Désormais, nous avons à faire à un concept du risque assez vague, qui contient de nombreuses définitions : « Multiple meanings from probability (risk of terrorism), to consequences (risks to security produced by ethnic cleansing), to describing perilous situations (Saddam Hussein poses risks or is a risk to peace) » (Heng 2006, 43). Cependant, comme le rappelle Furedi, aucune définition ne peut saisir le risque, car il évolue sans cesse et il est à mettre en lien avec des contextes et des sociétés qui sont différentes ; selon cet auteur, le point central à retenir c'est la distinction entre réalité et possibilité (Furedi 2002, 17) ; C'est également la différence établie entre une menace et un risque, respectivement.

2. *Le cyber à l'OTAN*

La gestion du risque cyber à l'OTAN présente plusieurs particularités qui rendent ce sujet pertinent. Tout d'abord, c'est un sujet intéressant, car jusqu'à présent, les chercheurs ont extensivement étudié l'OTAN sous l'angle de sa doctrine de dissuasion, de ses campagnes en Yougoslavie et en Libye, de son élargissement, etc. Le cyber est un sujet récent et, par conséquent, il n'a pas encore beaucoup été étudié même s'il existe de très bonnes contributions académiques (Hansen et Nissenbaum 2009, Rasmussen 2001, Coker 2013, Kempf 2014, Pomarède 2014). Il faut souligner que c'est un sujet qui n'est arrivé que récemment sur l'agenda politique de l'OTAN, une des organisations internationales ayant érigé la cybersécurité au rang de priorité (cf. Résolution 387). Jusqu'à présent, l'OTAN s'est concentrée sur la défense de ses propres systèmes d'information et de communication grâce aux principes de prévention et de résilience, ce qui

signifie respectivement que l'OTAN cherche à gérer les risques de façon proactive et qu'elle se prépare à réagir en cas d'attaque. Ce qui marque avant tout lorsque l'on cherche à étudier la cyber défense de l'OTAN, c'est l'ambiguïté stratégique ainsi que la complexité de la gouvernance : « NATO will maintain strategic ambiguity as well as flexibility on how to respond to different types of crisis that include a cyber component » (Hunker 2013, 159). C'est à partir de 2007 que les choses s'accélèrent sur le plan politique et militaire en ce qui concerne le cyber.

Étymologiquement, « cyber » signifie gouverner, diriger. Il est donc très pertinent de s'intéresser à ce sujet dans le cadre de recherches en science politique. Toutefois, c'est un thème technique et complexe. D'abord, le cyberespace n'est pas aisément définissable. Nous devons ce terme à l'auteur américain et canadien William Gibson qui, en 1984, inventa le terme dans *Neuromancien*, une fiction dystopique. Alix Desforges tente de donner une définition du cyberespace : « si l'Internet est aisément définissable et identifiable, le cyberespace apparaît plus englobant et plus virtuel. Il évoque tout à la fois un "monde" virtuel, dématérialisé, sans frontières, anonyme, de libertés, de partage et de communication, mais également un "espace" dangereux et nébuleux dans lequel des comportements réprimés en société peuvent s'exprimer sans répression » (Desforges 2014, 67). Typiquement, deux visions s'affrontent à propos de cet univers virtuel et dématérialisé qu'est le cyberespace : « Certains y voient la promesse d'un accroissement de la démocratie, du progrès économique et d'un monde pacifié, mais il annonce aussi l'avènement d'une surveillance généralisée, un Big Brother ultime et un outil absolu pour le contrôle des foules et leur manipulation – une représentation réveillée par la publication des documents d'Edward Snowden quant aux pratiques de la NSA en matière de renseignement » (Desforges 2015, 67-68). Nous allons nous attacher à mettre en lumière les caractéristiques du cyberespace afin de montrer

comment cet espace, qui est à l'origine exclusivement technique, est devenu un espace social, politique, militaire et stratégique (Kempf 2014b).

Premièrement, le cyberespace est composé de plusieurs couches : la couche physique englobe toutes les infrastructures matérielles physiques, comme par exemple les ordinateurs, les câbles sous-marins et terrestres. Cette couche peut être assez facilement cartographiée, mais il est très difficile d'atteindre la couche physique par une cyberattaque (Geers 2010). Ensuite, nous trouvons la couche logique ou logicielle, qui représente toutes les technologies qui permettent que des informations se transportent ou soient stockées. Enfin, la couche sémantique ou cognitive est la plus difficile à appréhender, parce qu'elle concerne l'information, les idées, les échanges (Kempf 2015, Douzet 2014). Le cyberespace est universel : « Chaque point du globe atteint n'importe quel autre » (Kempf 2014, 56). Cela sous-tend également que les réseaux sont interconnectés entre eux, et qu'il est difficile de faire la distinction entre des réseaux nationaux et des réseaux internationaux. En ce sens, il est possible d'affirmer que jusqu'à un certain point, le cyberespace ne connaît pas de frontières, ou en tout cas, pas les frontières entre les États-Nations telles que nous les connaissons. Nous le verrons, il existe tout de même des frontières dans le cyberespace et elles tendent à se renforcer (Kempf : 33). Le thème de la territorialisation et des frontières amène nécessairement à parler de souveraineté, et plus exactement de souveraineté numérique. Selon Kempf, le cyberespace représente l'opportunité pour les Etats d'être davantage autonomes : « la cyberdéfense appartient avec le nucléaire et le renseignement au cœur de la souveraineté des Etats » (Kempf : 138). Nous voulons montrer que le cyber a en fait été militarisé dans l'optique de faire partie intégrante de cette souveraineté, mais qu'en aucun cas la cybersécurité est inhérente à la défense des États.

Ensuite, nous devons dresser un bref portait des différents acteurs. Nous pensons que la typologie proposée par Dorothy Denning (2003) est la plus à même de saisir la différence de nature et d'intention entre les acteurs. L'experte propose 6 catégories :

- Tout d'abord, nous trouvons ce que Denning appelle les « insiders », c'est-à-dire les gens de l'intérieur, qui sont des individus qui ont des accès à des documents ou des procédures. Selon Denning, cela représente 80% des incidents de cybersécurité. Sans donner de statistique, Hunker (2013) affirme que la cyberattaque dont il faut se méfier le plus vient de l'intérieur ;
- Ensuite, les hackers sont des individus qui essayent de s'introduire dans les systèmes ou d'en gagner l'accès, contrairement aux *insiders*. Cette catégorie est très vague et peut s'appliquer aux catégories suivantes ;
- Puis viennent les espions, qu'ils agissent pour des motifs économiques ou politiques, leur but est de subtiliser des données en restant invisibles ;
- Denning distingue ensuite les criminels qui agissent dans le seul but d'obtenir de l'argent, que ce soit par rançon, en vendant des informations ou bien en subtilisant des données de cartes bancaires ;
- Les terroristes entrent dans cette catégorisation, car ils utilisent le cyberespace en soutien à leurs opérations physiques sur le terrain. Ce cas, que nous étudierons en détail, montre la limite d'une telle catégorisation puisque dans la majorité des cas, les terroristes utilisent le cyberespace pour financer leurs opérations (on pourrait donc les classer dans les « criminels ») et pour recruter ;

- Enfin, les États-nations, dont Denning juge qu'il faut s'en méfier le plus car certains d'entre eux, une vingtaine dont la Russie, la Chine et la Corée du Nord, auraient des capacités de cyberguerre.

Par ailleurs, il existe différentes cyberattaques. Hunker en identifie 2 types : les attaques passives qui cherchent à copier ou voler des données sans perturber le système, le réseau voire même sans que cela soit remarqué (cyber crime type vol de données bancaires, cyberespionnage). D'autre part, il y a les attaques dites disruptives dont le but est de perturber les réseaux et systèmes, voire de les bloquer dans un but de revendication (vandalisme, revanche, demande de rançon, hacktivisme) (Hunker 2013, 155). Les nations comme la Russie et la Chine sont très actives dans l'espionnage et dans le développement d'outils disruptifs.

Enfin, la caractéristique la plus importante dans l'étude de la cybersécurité est l'opacité qui résulte dans la difficulté d'attribution des attaques. En d'autres termes, il est techniquement difficile d'identifier son agresseur. L'OTAN reconnaît que cela pose un problème dans l'élaboration de sa stratégie : « L'aspect le plus inquiétant du cyberespace est que l'attaquant a l'avantage sur le défenseur. Il suffit aux attaquants d'un seul maillon faible pour pénétrer dans le réseau, alors que les défenseurs doivent parer à toutes les failles. Ces attaques par ailleurs vont à la vitesse de la lumière, ce qui laisse peu ou pas de temps pour réagir » (Rapport de Commission annuel 2011 – Information et sécurité nationale, §31). En ce sens, cette caractéristique donne l'avantage à l'attaquant (Dunn Cavelty 2012, Geers 2010), ce qui a des conséquences juridiques mais surtout stratégiques parce que cela génère un sentiment d'incertitude et *in fine*, la décision politique comportera un risque, car tous les éléments de l'attaque ne peuvent être connus (Boyer).

Cependant, comme le montrent Amoore et de Goede : « Paradoxically, however, this recognition of incalculability does not lead to an abandonment of calculative techniques in favor of, for example, a political-philosophical recognition of the fragility of modern life » (2008, 10). En effet, nous verrons que l'OTAN, inspirée par les États-Unis, montre une volonté de maîtriser l'incertitude en essayant de gérer ces potentiels dangers, que nous appellerons risques. En nous appuyant sur des auteurs poststructuralistes, nous montrerons que la gestion du risque est une façon de gouverner (Aradau et van Munster 2011, Bigo 2005, Ericson 2008, Huysmans 2006).

Nous nous sommes demandés quelle était la stratégie mise en place par l'OTAN pour lutter contre les cyberattaques. Cette question nous a amené à analyser la façon dont l'OTAN, dans un contexte de mondialisation, perçoit les menaces et construit en conséquence sa doctrine en matière de cyber défense. Prenant part à une vaste réflexion sur le lien entre technologies et sécurité, notre recherche se veut être une contribution académique dans la discipline des relations internationales. La pertinence de ce sujet relève en premier lieu du contexte actuel et de l'importance grandissante du cyber dans les relations internationales. Nous pensons que le cyber permet de redistribuer les cartes en matière de stratégie, notamment militaire, mais également à l'échelle internationale. Il est possible de voir l'étude du cyber comme une façon de souligner la vulnérabilité de grandes puissances. A titre d'exemple, le cyber permet d'appréhender la Corée du Nord, État hermétique d'un point de vue technique, comme un acteur qui pourrait avoir l'ascendant sur des États très connectés. Le cyber permet donc dans une certaine mesure de nous interroger sur ce que nous comprenons des relations internationales. Il existe pour le moment très peu de publications dans cette discipline qui appréhendent le cyber comme un risque. Nous pensons qu'étudier le cyber en tant que risque permet de délaisser dans une certaine mesure l'aspect technique et micro de ce sujet

au profit d'une compréhension plus globale. En d'autres termes, notre recherche permet de se consacrer aux enjeux politiques qui ont investi le cyber. Pour ce faire, elle donne une place conséquente aux éléments doctrinaux et stratégiques en conduisant une étude discursive.

Cette thèse s'attache notamment à faire le lien entre la gestion du risque terroriste et la gestion du risque cyber. Le cas choisi est l'OTAN, car l'Alliance semble cristalliser les pratiques de sécurité occidentales : « The West imagines European security in terms of NATO. […] NATO thus provides an opportunity for studying the Western praxeology of security » (Rasmussen 2001, 295). S'intéresser au risque implique nécessairement de porter notre attention sur le rôle des décideurs politiques américains et la stratégie de précaution instaurée sous l'ère Bush. Le rôle des États-Unis est particulièrement important pour notre objet d'étude, parce que les États-Unis sont à l'origine de la révolution de l'information, tant sur le plan technique que sur le plan intellectuel (Dunn Cavelty 2009). Dans cette perspective, une attention particulière devra être portée aux efforts de l'administration Clinton dans la politisation et la militarisation du cyberespace. Par ailleurs, il sera important de se pencher sur les réactions des décideurs politiques américains aux attaques du 11 septembre 2001 et l'influence qu'elles ont eu sur les pratiques actuelles de l'OTAN. Dans cette thèse, nous soutenons l'idée que la doctrine de l'OTAN en matière de cyberdéfense est héritière de la gestion du risque terroriste telle qu'imaginée par l'administration Bush à la suite des attentats du 11 septembre 2001 ; elle se caractérise, entre autres, par une perception disproportionnée des risques liés au cyberespace, par la prolifération des risques et participe à l'aggravation du sentiment d'insécurité. Nous avons été témoins depuis ce jour-là d'un accroissement des mesures privilégiant la sécurité à la liberté, de la mise en place d'un état d'exception dans de nombreux pays occidentaux. La perception des risques a changé et certaines menaces issues du cyberespace comme le cyberterrorisme sont aujourd'hui perçues comme un risque à fort probabilité et à fort

impact par des firmes d'analyse de risque, des gouvernements, des organisations internationales et des think tanks. Comme le rappelle Dunn Cavelty : « The militarisation of cyber security is first and foremost based on the belief in a massive threat of a large-scale cyber attack » (Dunn Cavelty 2012, 114).

Aujourd'hui, notamment grâce aux révélations d'Edward Snowden, il n'est plus possible d'ignorer que nos recherches et informations sont potentiellement analysées dès que nous utilisons Internet. Ces abus ne vont aller que de façon croissante si nous ne prenons pas conscience qu'il nous faut maîtriser notre intégrité et notre vie privée en ligne. C'est dans cette perspective que cette thèse cherche à comprendre spécifiquement les effets de la gestion des risques cyber. La pertinence de cette recherche tient avant tout dans le fait qu'elle montre, en s'appuyant à la fois sur les travaux du sociologue Ulrich Beck et des poststructuralistes, que la gestion du risque ne nous donne pas plus le sentiment d'être en sécurité et, qu'au contraire, elle produit de l'insécurité. Nous argumentons notamment avec le cas du cyber terrorisme qu'il y a une exagération volontaire du risque. Cette recherche prend son inspiration dans l'affirmation de Frank Furedi : « Those who propose to avoid risks and gain safety will invariably find that what they acquire instead are obsessions » (Furedi 2002, 13).

Pour ce faire, le premier chapitre veut d'une part faire la lumière sur le nexus risque-sécurité qui est aujourd'hui au cœur des discours sécuritaires et des doctrines militaires, et d'autre part présenter les différentes perspectives théoriques qui ont participé à conceptualiser le risque. La première partie de ce chapitre sera l'occasion de revenir sur l'évolution du contexte post-guerre froide à un environnement stratégique marqué par des nouveaux risques. Nous introduirons ici

notre cas empirique, l'OTAN, afin de montrer ce changement de paradigme dans les discours sécuritaires occidentaux. Dans un second temps, nous voulons présenter une recension des différentes théories et écoles de pensée du risque, et notamment ce qui différencie les travaux issus des études critiques de sécurité et ceux produits par les tenants de la sociologie d'Ulrich Beck. Il s'agira de mettre en lumière les apports et les faiblesses de ces théories et d'établir le cadre théorique choisi pour cette recherche. Enfin, notre attention se portera sur les caractéristiques majeures du risque que sont l'incertitude et la virtualité, qui seront analysées à travers les notions de savoir et de temporalité.

Dans le second chapitre, les actes discursifs relatifs au risque terroriste post-11 septembre, en particulier ceux de l'OTAN et des Etats-Unis, seront analysés en détail. Nous chercherons à mettre en exergue la stratégie de préemption mise en place par l'Administration Bush, ainsi que ses effets pervers. Pour ce faire, nous utiliserons à la fois la littérature issue des études critiques de sécurité, qui met l'accent sur l'insécurité produite par les pratiques de sécurisation, ainsi que les travaux des tenants de la thèse de Beck portant sur les aspects psychologiques caractéristiques de la société du risque. Il sera notamment question de la perception des risques et du rôle de l'imagination dans la gestion de risque.

Le dernier chapitre cherchera à analyser la construction des risques liés au cyberespace par l'OTAN. Nous verrons d'abord comment l'Alliance a embrassé la gestion du risque en termes de stratégie militaire, notamment en ce qui concerne les « nouveaux défis de sécurité », en mettant en relief le rôle des Etats-Unis dans la sécurisation du cyber à travers la pratique de protection des infrastructures critiques. Ensuite, nous nous pencherons sur le cas du cyber-terrorisme qui nous permettra d'illustrer notre propos concernant la sécurisation du cyber par les Etats-Unis. Le risque cyberterroriste nous permettra de voir que la gestion de risque se caractérise notamment par la

distorsion de la perception des risques et l'amplification des sentiments de peur et d'anxiété. Enfin, en ralliant tous les éléments vus au cours de cette discussion, nous verrons comment la stratégie de cyberdéfense de l'OTAN partage d'une part des similarités avec la gestion du risque terroriste américaine, notamment par l'instauration d'une « forme de gouvernementalité par l'inquiétude, où pour rassurer les populations et les amener à obéir, on exacerbe leur peur par un discours du risque et de la suspicion au sein d'un horizon présenté comme celui de l'Apocalypse » (Bigo 2005, 7). D'autre part, nous mettrons en évidence une stratégie anachronique qui est héritière de la doctrine historique de dissuasion de l'OTAN.

CHAPITRE I – RISQUE ET CYBERSÉCURITÉ : PERSPECTIVES THÉORIQUES

Nous allons voir, dans ce premier chapitre, comment le risque a été théorisé dans différentes disciplines. Nous voulons expliquer qu'au lendemain de la fin de la guerre froide, dans un contexte de mondialisation et de multipolarisation du monde, les gouvernements occidentaux ont fait face à une montée de menaces asymétriques et se sont, de ce fait, orientés vers une gestion des risques, faute de pouvoir établir une stratégie de dissuasion : « First of all, protecting society against asymmetrical threats that arise partly form the information revolution has become *the* central security policy concern today" (Dunn Cavelty 2008, 152). Ensuite, notre attention se portera sur les caractéristiques majeures du risque que sont l'incertitude et la virtualité, qui seront analysées à travers les notions de savoir et de temporalité. Enfin, nous présenterons une recension des différentes théories et écoles de pensée du risque, et notamment ceux d'Ulrich Beck qui constituent la base théorique de notre réflexion sur la gestion des risques cybernétiques à l'OTAN.

A) Le risque au cœur des discours sécuritaires contemporains

Tout d'abord, nous l'avons vu en introduction, le risque n'est pas un concept nouveau. Il peut nous sembler que le risque comme concept sécuritaire soit contemporain, mais il n'en est rien. Cependant, c'est un concept qui est historiquement lié à la dimension économique et financière plutôt qu'à la sécurité des territoires nationaux. Puisque cette recherche s'inscrit dans la discipline des Relations Internationales, il convient de venir étudier plus en détail l'articulation entre le risque et la sécurité internationale. En conséquent, il nous faut identifier précisément le basculement dans ce nouveau paradigme. Nous avons constaté que le moment de bascule s'est opéré à la fin de la guerre froide. La décennie 1990 est en effet le point de départ de cette réflexion autour du concept

de risque pour les RI. Pour ce faire, nous nous intéressons à l'OTAN, pour qui, plus que toute autre organisation internationale sûrement, la chute de l'empire soviétique fût un moment crucial, car il en était de sa propre identité et de sa raison d'être.

1. *De la guerre froide à l'ère de la mondialisation*

Dans le contexte d'affrontement idéologique de deux blocs tels que c'était le cas pendant la guerre froide, la stratégie militaire employée était somme toute assez simple. A l'OTAN, bras armé et lieu de réflexion stratégique du bloc de l'Ouest, elle reposait avant tout sur le principe de dissuasion. Il s'agissait de montrer à l'adversaire que les gains de l'attaque étaient inférieurs aux coûts engendrés par les représailles. Cette stratégie défensive reposait sur l'arme nucléaire. En termes de stratégie et de tactique militaire, il était assez aisé d'anticiper et de calculer les risques, d'une part, parce que les acteurs étaient rationnels selon la définition de Weber (c'est-à-dire qu'ils répondaient à la logique coûts-bénéfices), et, d'autre part, parce que leurs capacités pouvaient dans une certaine mesure être calculées (Williams 2008, Rasmussen 2006). Cette logique que Beck appelle « means-ends », où l'acteur met en place les stratégies adéquate pour atteindre un objectif précis, était assez stable.

À la dislocation de l'Union Soviétique en 1991, la préoccupation des gouvernements n'était plus l'affrontement avec le bloc de l'Est. Comme l'écrit Myriam Dunn Cavelty: "After the Cold War, the US began to fear that its huge conventional military dominance would force any kind of adversary – states or sub-states groups – to use asymmetric means, such as dirty bombs, information operations, or terrorism" (Dunn Cavelty 2008, 26). L'identification de vulnérabilités a rappelé aux États-Unis que leur supériorité militaire, qui avait en partie permis de gagner le combat idéologique contre l'Union Soviétique, n'était désormais plus suffisant pour garantir leur

sécurité. Ainsi, les politiques de sécurité ont basculé vers le concept de risque, associé aux menaces asymétriques, mal définies et peu connues. En somme, nous mettons en évidence ici le basculement entre un environnement plutôt rationnel dans lequel on peut avoir des certitudes et un nouveau contexte, plus incertain, dans lequel émergent des acteurs aux motifs et capacités variés. En effet, au cours de la guerre froide, il y avait, d'une part, une certitude liée à la possibilité d'anticiper le comportement et la réaction de l'adversaire, et d'autre part, la possibilité de calculer le coût des dommages d'une attaque – par exemple, il était possible de calculer avec précision la portée d'un missile, le nombre de tanks postés à une frontière, etc. Cependant, il faut apporter ici une nuance. Il ne s'agit pas de dire que l'analyse de risque était fiable et que le système était stable en tout point. Nous cherchons simplement à mettre en avant le fait qu'à la sortie de la guerre froide, les acteurs ont dû s'habituer à un environnement stratégique qui s'éloigne de celui qu'ils avaient connu pendant près d'un demi-siècle. En effet, ils ont assisté à la montée d'acteurs non-étatiques, de menaces asymétriques telles que le terrorisme, et les armes de destruction massive sont devenues une priorité pour le gouvernement de George W. Bush. Selon Heng (2006) et Giddens (1994), ces nouvelles menaces sont qualitativement différentes à cause de la mondialisation et des technologies de communication, car elles peuvent affecter toute la population.

Pour garantir une nouvelle forme de sécurité, les gouvernements se sont donc tournés vers le concept de risque (Kristensen 2008). Le débat sur les stratégies à adopter pour lutter contre ces nouveaux risques est marqué par une logique de gestion qui se met progressivement en place, sous l'égide des États-Unis (Heng 2006, Petersen 2012, Dunn Cavelty 2009, Williams 2009, Rasmussen 2006, Lupton 2013). La conscience qu'on ne peut éliminer ces risques a engendré la transition de dissuasion à prévention et préparation (Dunn Cavelty 2008, Aradau et Van Munster 2008).

Cependant, une des caractéristiques majeures est le fait que les risques ne peuvent pas être éliminés; ils peuvent seulement être gérés, au mieux diminués.

Lors de la guerre froide, l'OTAN était considérée comme une communauté de sécurité, un groupement d'États partageant une identité commune, dont le but et la raison d'être était de garantir la sécurité (Adler 1997). Depuis 1949, la stratégie de l'OTAN, représentative de son identité principale à savoir la défense des valeurs démocratiques et des libertés fondamentales, a toujours été établie en fonction de la stratégie soviétique (Herd et Kriendler 2012). A la perte de sa raison d'être, l'OTAN est restée soudée en s'attachant à gérer les nouvelles menaces et les nouveaux risques qui s'imposaient à l'Occident : « NATO has imagined itself as the agent of change in the post-Cold War era. Its means of facilitating change has been through the broadening of the concept of security" (Rasmussen 2001, 307). Ce tournant vers le risque a clairement été énoncé par l'OTAN dès le mois de novembre 1991 à l'occasion de la publication du premier Concept Stratégique post-guerre froide. Dans ce document annonçant la nouvelle doctrine et la volonté d'élargir l'Alliance, l'OTAN rappelle que la menace unique et immobile à affronter a disparu et que, par conséquent, l'organisation se tourne vers la gestion des risques :

> Au lieu de résulter d'une menace prédominante, les risques qui subsistent pour la sécurité des Alliés se présentent désormais sous des formes complexes et proviennent de directions multiples, ce qui les rend difficiles à prévoir et à évaluer. L'OTAN doit être en mesure d'y faire face, si elle veut sauvegarder la stabilité en Europe et la sécurité de ses membres. Ces risques peuvent apparaître de plusieurs manières.
> (NATO, Concept Stratégique 1991, §9)

Il convient là encore d'apporter une nuance dans notre propos au sujet de cette rupture, qui n'est pas aussi nette qu'elle n'y paraît. En effet, si la guerre froide est symbolisée par l'opposition entre deux puissances, à savoir les États-Unis et l'URSS, la réalité était bien plus complexe et l'Histoire a d'ailleurs montré que le système n'était pas immobile, mais au contraire qu'il y a eu des périodes

de tensions extrêmes et à l'inverse des moments de détente dans les relations. Il ne s'agit donc pas de présenter un portrait binaire ici, mais de souligner quelques différences qui permettent de comprendre le changement observé en termes de doctrine et de stratégie. Nous verrons par ailleurs que la continuité entre la guerre-froide et la période post-guerre froide peut s'observer dans la construction identitaire qui sous-tend les doctrines encore aujourd'hui.

Certains auteurs identifient l'OTAN du XXIème siècle comme une communauté d'insécurité (Williams 2008, Coker 2002). Cela veut aussi dire qu'elle est passée d'une organisation définie par l'environnement stratégique à une alliance qui veut définir son environnement stratégique (Williams 2009, Rasmussen 2001, Williams 2008, Coker 2002) ; nous reviendrons plus en détail sur ce point dans le troisième chapitre.

1. Calculer l'incalculable et le tournant du 11 septembre 2001

Si la transition entre une sécurité forgée autour d'une menace unique, l'URSS, et une sécurité fondée sur la gestion des risques a été entamée dès 1991, c'est surtout 2001 qui marque ce changement complet de paradigme. En effet, les attentats terroristes contre le World Trade Center et le Pentagone ont accéléré l'avènement de la gestion de risque en tant que mode de gouvernement (Rasmussen 2006, Heng 2006). Désormais, tous les sujets sont en proie à devenir des risques et l'on observe d'ailleurs qu'ils sont traités de façon similaire : les stratégies en matière de protection environnementales se rapprochent par exemple des stratégies de lutte contre le crime (Rasmussen 2006, 93). C'est dans cette perspective que nous cherchons à montrer que la doctrine de cyberdéfense de l'OTAN partage beaucoup de similarités avec la doctrine anti-terroriste américaine.

Il est nécessaire de rappeler que le risque est lié à la prise de décision (Williams 2009, Lupton 2013). Pendant la guerre froide, ces décisions étaient liées à des calculs; on calculait les causes et les effets, les fins et les moyens (Williams 2009, Rasmussen 2006, Beck 2009). Aujourd'hui, puisque le risque est difficilement quantifiable, une grande place est laissée à la perception et à la subjectivité (Williams 2009). À l'OTAN, cela signifie concrètement que les 28 pays-membres ont chacun une vision particulière des risques, et notamment des risques cybernétiques. La résolution 387 sur la cybersécurité mentionne d'ailleurs à cet égard que ces différentes perceptions peuvent constituer un obstacle à la coopération et à la réalisation d'une cyberdéfense commune efficace : « ***Inquiète*** à l'idée que les capacités de cyberdéfense et la sensibilisation aux menaces cybernétiques varient considérablement d'un pays membre de l'OTAN à l'autre, affaiblissant ainsi la cybersécurité globale de l'Alliance » (Résolution 387 sur la cybersécurité, §3 emphase originale).

En outre, il est désormais plus compliqué de quantifier avec certitude les menaces (Rasmussen 2006, Coker 2002, Heng 2006, Petersen 2012). En effet, il est difficile d'évaluer le risque et surtout de calculer les dommages qu'entrainerait la réalisation de ce risque (Williams 2008). Comme l'affirme explicitement le Concept Stratégique, les risques sont désormais « difficiles à prévoir et à évaluer » (NATO, Concept Stratégique 1991, §9). Selon Deborah Lupton, cela est notamment dû au fait que les risques ne sont pas facilement localisables et que leurs effets sont potentiellement de long terme (Lupton 2013). Ceci est d'autant plus vrai en ce qui concerne les risques cyber, car il est très difficile de connaître les capacités de ses adversaires. De plus, si le risque se matérialise, la durée d'une attaque dépend de sa propre capacité à identifier la faille dans le système et à la colmater.

B) Virtualité et incertitude : l'essence du risque

Cela nous amène à évoquer un point central dans notre discussion : avec le risque, le mythe de la contrôlabilité s'évapore (Beck 2009). Les risques sont toujours virtuels, ils ne sont que des hypothèses et des anticipations du futur (Lupton 2013, Van Loon 2002). De ce fait : « Nous sommes dans un temps des perceptions, de la virtualité plus que dans un temps de la commission des faits, de l'actualité. Et c'est cette transformation centrale du jeu sur le temps que permet en grande partie l'usage de l'informatique à travers une "virtualisation du réel" » (Bigo 1997, 424). Il y a donc une incertitude liée à cette réalisation (ou non) du risque.

1. Temporalité

En outre, la virtualité du risque réside avant tout dans la temporalité. Avant, les décideurs s'attardaient à analyser les erreurs passées pour construire de nouvelles stratégies ou bien c'était le niveau de menace présent qui les poussait les à agir (Dunn Cavelty 2009). Désormais, le présent est animé par la projection du futur : Beck parle de « colonisation du futur » (Beck 2009 : 4, Williams 2009, Dunn Cavlety 2009, Rasmussen 2001, Furedi 2002, Lupton 2013, Hagmann et Dunn Cavelty 2012, Amoore et de Goede 2008). Aujourd'hui, le risque est évalué par la formule suivante : risque = impact (degré de perte) x probabilité (de perte) (Luhmann 2005, Dunn Cavelty 2008). La gestion du risque, c'est l'ensemble des moyens mis en œuvre pour anticiper et éviter des catastrophes. Il s'agit donc d'une prise de décision au présent en réaction à un scénario futur que l'on cherche à éviter : « A risk is never a present danger : it only becomes a danger because of what it is expected to cause in the future » (Rasmussen 2006, 115). En ce sens, on assiste à l'avènement de l'âge de la spéculation et de la préemption (Heng 2006, Rasmussen 2001, Furedi

2002). En outre, la prise de décision se faisant à partir de beaucoup d'incertitude, le contrôle des actions n'est plus atteignable et par conséquent, le but non plus : assurer la sécurité (Rasmussen 2004).

2. Savoir

Lupton dit que le risque est devenu un concept hautement politique et qu'il faut, dans cette perspective, se demander qui produit le risque (Lupton 2013, 87). Il convient donc de s'intéresser au savoir. Tout d'abord, les décideurs agissent sur des scénarios, car le risque est une projection, un pari sur l'avenir, sur ce qui peut se passer. Comme dans toute projection, il y a une part, plus ou moins grande, d'éléments qui ne sont pas connus. Dans le cas d'une attaque cybernétique par exemple, on ne connaît pas à l'avance la brèche que les attaquants vont utiliser; on ne la découvre qu'au moment où l'attaque est lancée. Si pendant la guerre froide il était possible de calculer l'impact d'une attaque selon les capacités et l'intention de l'acteur, désormais les décideurs doivent agir avec moins d'informations (Petersen 2012), voire pas d'information, ce que Beck nomme *Nichtwissen* (Beck 1992, 2009, Mythen 2004). Ce non-savoir n'est pas éradicable selon Beck, mais pour autant: « This does not mean that risk annuls all forms of knowledge. Rather it amalgamates knowledge with non-knowing within the semantic horizon of probability » (Beck 2009, 5). Seulement, la division n'est pas binaire entre ce qui est su et ce qui ne l'est pas. Beaucoup d'auteurs ayant théorisé le risque (Williams 2009, Rasmussen 2006, Williams 2008, Aradau et Van Munster 2008) reprennent d'ailleurs la célèbre intervention de Donald Rumsfeld, alors Secrétaire de le Défense des Etats-Unis, lors d'une conférence de presse au quartier général de l'OTAN à Bruxelles le 6 juin 2002 :

> The message is that there are no "knowns." There are thing we know that we know. There are known unknowns. That is to say there are things that we now know we don't know. But there are also unknown unknowns. There are things we don't know we don't know. So when we do the best we can and we pull all this information together, and we then say well that's basically what we see as the situation, that is really only the known knowns and the known unknowns. And each year, we discover a few more of those unknown unknowns.[1]

Rumsfeld discerne ici les différents cas de figure en ce qui concerne le savoir face au risque. Ce qu'il appelle les « known knowns » représentent ce que nous sommes conscients de savoir. Viennent ensuite les « known unknowns », une notion intéressante qui consiste à admettre qu'il y a des trous dans notre connaissance. Par exemple, cela pourrait être avoir conscience qu'un antivirus ne détecte pas tous les problèmes sur un ordinateur sans toutefois connaître les virus qui n'ont pas été traités. Selon Aradau et Van Munster, ce type de risque peut tout de même être calculé et mis en probabilité (2008). Enfin, Rumsfeld évoque les « unknown unknowns », qui sont ne sont pas connus jusqu'à ce que le risque se matérialise puisqu'on n'a pas conscience de ce que l'on ignore. Ils représentent la bête noire des analystes de risques et des décideurs car ils sont tout simplement imprévisibles (Aradau et Van Munster 2008, 30). Certains auteurs reprennent l'analyse de Zizek (2004) qui met en exergue une configuration que Rumsfeld n'a pas abordée: « What Rumsfeld left out, however, are the "unknown knowns", the beliefs that one inadvertently adheres to when interpreting all the other "knowns" and "knowns" » (Williams 2009, 67; Grondin 2005).

Cependant, plus de savoir n'équivaut pas à moins d'incertitude ni à plus de sécurité. En effet, alors qu'avant, l'ignorance (le non-savoir) était source de danger, Beck dit que désormais le savoir créé une nouvelle conscience du risque (Beck 2009, Furedi 2002, Lupton 2013, Van Loon 2002, Dunn Cavelty et Mauer 2008, Mythen 2004). Par ailleurs, ces auteurs mettent également l'emphase

[1] http://www.nato.int/docu/speech/2002/s020606g.htm

sur le pouvoir de ce savoir diffusé par les experts qui occupent une place de choix auprès des décideurs, mais également auprès du public ; ce sont eux qui fixent le niveau de risque (Coker 2002, Mythen 2004, Furedi 2002, Lupton 2013). En ce qui concerne le cyber, l'immense majorité d'entre nous sont ignorants et il est donc facile d'accorder sa confiance à un expert qui s'exprime dans un journal ou dans une émission de télévision. Comme nous le verrons avec le cas du cyber-terrorisme, il est primordial de remettre en question les évaluations de ceux qui parlent avec une voix experte, d'autant plus que ce type de savoir est généralement utilisé pour masquer ce qui n'est pas su (les « known unknowns » en particulier) dans une perspective de réassurance et de feindre le contrôle : « They in fact employ a glorified form of guesstimates that is turned into objective security "truth" in the process » (Hagmann et Dunn Cavelty 2012, 81). Ce point nous paraît central dans notre démarche de démystification des risques cybernétiques.

En somme, pour les raisons évoquées, nous pouvons affirmer que nous avons une politique mondiale marquée par l'incertitude. Cependant, vivons-nous vraiment dans l'époque la plus dangereuse de l'histoire de l'humanité ? Bien au contraire, certains auteurs combattent cette idée et affirment que notre société est très sécure (Williams 2009, Furedi 2002, Lupton 2013). En revanche, elle est marquée plus que jamais par l'incertitude et donne le sentiment - l'impression, et cette différence est très importante - d'être en insécurité (Williams 2009, 20). En ce sens, le plus grand danger de la société est la société elle-même; cette idée s'inscrit dans la théorie de la réflexivité énoncée par Beck.

C) Théoriser le risque cybernétique à l'OTAN

1. Les perspectives théoriques qui ne réussissent pas à conceptualiser le risque

Beaucoup de chercheurs se sont intéressés à ce qu'était l'OTAN à l'ère post-guerre froide, chacun ayant tenté à sa façon d'expliquer ce qu'était devenue l'Alliance au lendemain de la perte de sa raison d'être initiale. En ce qui concerne les théoriciens associés aux approches réalistes en RI, ils avaient notamment prédit l'éclatement de l'OTAN à la suite de la disparition de l'URSS selon le concept central de *balance of power* qui explique qu'il faut nécessairement une force égale ou supérieure pour contrer une menace (Williams C. 2007, Williams 2009, Nau 2008). Or, en ce qui concerne les risques et menaces aujourd'hui, notamment dans le cas du cyber, leur caractéristique première est d'être asymétriques. Dans le cas du cyber par exemple, l'avantage est donné à l'attaquant, car il est probable qu'il trouve une brèche dans un système avant que celle-ci soit bouchée (Kempf 2015, Geers 2010). De plus, un individu peut se procurer des outils pour mener des cyber attaques contre des systèmes gouvernementaux ou de grandes entreprises. Par ailleurs, les théories institutionnalistes visent à expliquer comment, dans une dialectique entre résilience et transformation, l'OTAN a subsisté à travers une adaptation institutionnelle (Irondelle et Lachmann 2011). Bien qu'intéressante et profondément optimiste pour l'avenir, cette approche ne permet pas d'embrasser de façon approfondie et complexe les divergences internes et place l'OTAN comme réponse au problème de la sécurité transatlantique (Rasmussen 2006). Comme nous allons le voir, l'institutionnalisation du cyber et la multiplication des agences spécialisées de lutte contre les menaces et risques cybernétiques rend difficile la gouvernance à l'OTAN. En ce qui concerne l'approche constructiviste, elle nous semble à la fois utile et problématique ; en effet, en mettant au premier plan les normes, l'identité et les valeurs comme éléments moteurs des relations

internationales, les constructivistes ont par exemple permis de saisir les valeurs transatlantiques comme forces fédératrices à l'OTAN. Cet apport intéressant semble toutefois perdre sa pertinence au vu du délitement de ces valeurs au fil des dernières années. Toutefois, comme le fait remarquer Myriam Dunn Cavelty (2009), les constructivistes ont notamment su affirmer le besoin d'établir le lien entre risque et sécurité ; ce nexus est au cœur de notre recherche. Les approches qui viennent d'être mentionnées présentent un même défaut : l'environnement dans lequel l'OTAN évolue est tenu pour acquis et jamais il n'est question de la façon dont l'OTAN participe à « façonner la représentation dans l'optique de légitimer un statut clef dans la gestion des insécurités » (Pomarède 2011, 129). Or, nous soutenons l'idée que l'OTAN investit autant dans le cyber depuis une décennie afin d'obtenir une place dominante dans ce domaine dans un soucis de pertinence et de maîtrise de l'environnement stratégique. C'est pourquoi nous nous sommes intéressés à des travaux, plus novateurs et plus critiques, qui viennent combler cette lacune et donnent une place importante à cet aspect.

2. *Penser le risque cybernétique avec Ulrich Beck*

Cette recherche a trouvé son inspiration dans les travaux du sociologue allemand Ulrich Beck qui, depuis 25 ans, a théorisé de façon extensive le risque dans les sociétés modernes. Bien que le sociologue se soit avant tout intéressé aux risques environnementaux et écologiques lorsqu'il a théorisé le risque, nous allons montrer qu'à bien des égards, les travaux de Beck sont originaux et pertinents pour étudier les risques cybernétiques. Nous allons notamment nous intéresser à la théorie de la société globale du risque ainsi qu'à la théorie de la modernité réflexive. Comme l'écrit Rasmussen: « Ulrich Beck's theory of reflexive modernity and risk society offers a means to conceptualize and understand the transformation of Western security policies » (Rasmussen 2001,

285). Selon Beck, le risque amène à une transformation sociale marquée par la disparition des frontières (Beck 2009, Giddens 1994, Luhmann 2005). En effet, selon le sociologue, les sociétés sont devenues si interdépendantes par le fait de la mondialisation que les frontières nationales disparaissent et que les politiques décidées sont globales, ou du moins ont un aspect nécessairement international (Lupton 2013, Rasmussen 2001). De plus, pour Beck, cette interdépendance signifie également que les risques sont partagés. Rasmussen note la pertinence de cette thèse au regard des sujets des relations internationales tels que la pollution et le réchauffement climatique. A certains égards, nous pensons également que cet aspect s'applique au cyber. En effet, utiliser Internet, par exemple, implique que nous nous servions de serveurs situés dans différents pays, que nos informations voyagent dans des câbles sous-marins en eaux internationales, que nous achetons des produits sur des sites étrangers.

Pour Beck, les risques sont globaux (Williams 2008, 2009, Rasmussen 2006, Heng 2006, Beck 2009). De ce fait, ils sont répartis de façon équitable dans la société, ils transcendent la société, mais beaucoup d'auteurs rejettent cette notion (Mythen 2004, Lupton 2013, Furedi 2002, Giddens 1994). La limite qu'il faut noter est que Beck pousse cette théorie jusqu'à quasiment nier le pouvoir que peuvent avoir les États-Nations. Or, bien que les frontières dans le cyberespace ne correspondent pas à celles des États-Nations, il n'en reste pas moins que les législations sont essentiellement nationales et que, dans le cas d'une coopération multilatérale comme à l'OTAN, ce sont les États-Nations qui s'accordent. À ce propos, l'OTAN rappelle, dans ses documents officiels, qu'il est nécessaire que les réseaux au niveau national soient compatibles avec ceux de l'OTAN pour que les décisions prisent au niveau de l'organisation puissent être mises en œuvre au niveau national (Résolution 387 sur la cybersécurité 2011, §10).

Au niveau technique également, cette disparition des frontières est à nuancer. Comme l'explique Olivier Kempf (2015), dans chaque couche du cyber, il est possible d'identifier une présence nationale. Dans la couche physique, il est assez facile d'appréhender le fait qu'une base de données ou encore des câbles se trouvant par exemple sur le territoire canadien dépendent de la juridiction fédérale du Canada, bien que là encore, des contournements soient possibles. En ce qui concerne la couche logicielle, Kempf donne l'exemple de l'ICANN, la société qui attribue les noms de domaine (« .com », « .org », etc.), qui est basée en Californie. Cela n'est pas sans conséquences sur le plan géopolitique : « Par-là, le gouvernement américain disposerait indirectement d'une souveraineté étendue » (Kempf 2015, 36). Enfin, pour illustrer la souveraineté nationale pouvant s'appliquer sur la couche sémantique, nous pouvons prendre l'exemple de la gestion restrictive par les autorités chinoises de l'accès aux contenus par les utilisateurs chinois.

En outre, Beck induit plusieurs notions intéressantes : les effets boomerang (c'est-à-dire que nous sommes victimes des risques que nous produisons), le principe de précaution pris pour réduire les niveaux de risques, la perte du contrôle et, ce qui nous semble le plus intéressant, la réflexivité dans la construction de notre société (la construction du « Soi » en fonction de l' « Autre » n'existe pas). La notion de risque ne peut pas être conceptualisée, selon Beck, sans la modernisation. En effet, c'est la modernisation qui précède dans le raisonnement de Beck, car elle produit les risques, comme le rappelle sa définition du risque : « a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself » (Beck 1992, 21). Elle se concrétise selon Beck par le passage entre la volonté d'une société d'éradiquer les pénuries et les manques, à la volonté de réduire les risques (Scott 2000, Beck 2009). Pour le sociologue, en effet, la clé de voûte de cette nouvelle modernité, qu'il appelle « late modernity », celle dans laquelle

nous nous trouvons actuellement, est la gestion des risques. Toujours rapporté au volet environnemental, Beck démontre que les risques sont directement issus de la modernité, et qu'ils n'en sont pas qu'un effet secondaire néfaste ; Beck les appelle les risques manufacturés (1992, 2009). Selon certains auteurs, ces risques sont la conséquence du développement des sciences et de la dérégulation du marché (Mythen et Walkate 2016, Rasmussen 2006, Van Loon 2002). Cette notion est intéressante, car elle cherche à mettre en exergue les risques liés au développement des technologies, bien que cela semble prendre un tournant pessimiste chez Beck. Dans la même perspective, Rasmussen affirme que les risques sont perçus comme plus menaçants à cause de la mondialisation, car ils s'immiscent dans notre vie quotidienne et deviennent la logique selon laquelle nous construisons notre identité (Rasmussen 2006, 100).

A propos de la construction de l'identité, Beck a également théorisé ce que Williams résume ainsi: « If there is no other, then there can be no threat. The same is not true of risk. Risk can be perceived independent of an identifiable actor" (Williams 2009, 18). Cette notion prend tout son sens lorsque l'on aborde la question des risques cybernétiques. D'une part, comme nous l'avons vu, il existe une multitude d'acteurs aux compétences techniques, aux moyens et aux intentions très variés. Par conséquent, l'OTAN ne peut pas construire son identité en termes d'un « autre ». D'autre part, elle peut difficilement prendre appui sur les cyber attaques dont elle a été victime puisque la non-attribution rend très difficile l'identification de l'attaquant. La difficulté supplémentaire pour l'OTAN est de se mettre d'accord à l'unanimité sur les adversaires :

> Tandis que l'Estonie reste focalisée sur la Russie, les responsables américains désignent, dans leurs prises de position, une liste d'adversaires plus diversifiée. Ils rappellent en effet que des groupes terroristes comme al-Qaïda, le Hamas et le Hezbollah se sont dits prêts à mener des cyberattaques contre les États-Unis, même s'ils reconnaissent par ailleurs qu'aucun d'entre eux n'y est parvenu à ce jour. S'agissant des acteurs étatiques, tant la Russie que la Chine sont considérées comme des sources sérieuses de cyber-menaces à l'encontre des États-Unis. (Rapport de Commission annuel 2009 - L'OTAN et la cyberdéfense, §34).

Depuis, l'OTAN semble avoir fait le choix de se concentrer sur les États-nations au détriment des acteurs non-étatiques, suite aux cyber attaques vécues par l'Estonie et le virus Stuxnet, vraisemblablement développé par les États-Unis et Israël. L'OTAN agit donc sans avoir un « autre » précis et défini, mais se construit en fonction de ses propres inquiétudes et agissements : « Since the entire security scenario is constructed and a decision to act is based upon the virtual scenario, the essence of risk lies in self-creation. In this sense, the other becomes oneself » (Williams 2009, 35).

En outre, la gestion du risque est intrinsèquement liée à l'incertitude, un point que Beck et ses disciples mettent en exergue à de nombreuses reprises comme nous l'avons vu précédemment (Beck 2009, Rasmussen 2001, Rasmussen 2006, Heng 2006, Coker 2002) et qui nous semble central dans la gestion du risque cybernétique. Selon lui, nous sommes désormais dans une société qui est caractérisée par une perte de contrôle des conséquences de nos actions, ce qui est source d'incertitude : « Reflexivity is characterised by a loss of control. Ends are no longer believed to be controlled by the means allocated to achieve them » (Rasmussen 2001, 294). Cette incertitude latente est renforcée par ce que Beck nomme les « effets boomerang », qui sont en fait les effets secondaires néfastes créés en prenant des décisions pour réduire les niveaux de risque (Van Loon 2002, Beck 2009, Rasmussen 2001). En d'autres termes, prendre une décision revient à prendre de nouveau un risque ; on assiste donc à une prolifération des risques (Rasmussen 2006). Ceci est essentiellement dû au fait que les décideurs agissent en fonction de scénarios, ce qui revient à un choix entre des risques, plutôt qu'un choix entre la sécurité et l'insécurité (Rasmussen 2001, 294). Cette incertitude réside dans la différence entre le savoir imparfait et la prise de décision (Heng 2006). Au final, l'effet boomerang s'inscrit dans la réflexivité de Beck, car nous soyons confrontés

à nos propres actions. Selon Lupton, les stratégies mises en place pour contrôler les risques ont un effet paradoxal, car elles augmentent la peur (Lupton 2013, Williams 2009, Rasmussen 2006, Rasmussen 2001).

Dans ces circonstances, la possibilité de ne pas agir est envisageable et pourrait paraître comme étant la plus raisonnable. L'OTAN prend cet aspect très au sérieux. Dans plusieurs déclarations officielles, il est fait état des inquiétudes des Alliés à propos d'un retrait de certains États dans les débats concernant la cybersécurité. Il est vrai que les 28 pays ne sont pas tous dépendants au même niveau et l'OTAN craint que certains États peu connectés ne s'investissent pas, sur le plan politique mais aussi technique et financier, à améliorer la cyberdéfense. Ainsi, l'OTAN se dit : « ***[i]nquiète*** à l'idée que les capacités de cyberdéfense et la sensibilisation aux menaces cybernétiques varient considérablement d'un pays membre de l'OTAN à l'autre, affaiblissant ainsi la cybersécurité globale de l'Alliance » (Résolution 387 sur la cybersécurité, §3 emphase originale). De plus, il ne faut pas négliger que certains acteurs veuillent se mettre volontairement sur le banc de touche. Il existe cependant un risque à cela : le risque par omission. Antagoniste au risque par commission, le refus d'agir n'est pas bien accepté: « In the face of catastrophe, it is presumed better to do s*omething* than *nothing*, even if the consequences of doing something are not clear » (Coutin 2008, 218). D'autres auteurs mettent plutôt en relief ce que Beck nomme la « risk-trap », c'est-à-dire qu'il n'existe pas de bonnes solutions; dans les deux situations, le risque prolifère (Coker 2002, Rasmussen, Heng 2006).

Tous ces aspects nous amènent à formuler une idée centrale de Beck : la sécurité n'est pas atteignable. Pire, par le biais de la réflexivité, nous nous infligeons cette insécurité (Beck 2009, 8).

En fait, Beck cherche à démontrer que le risque est le contre-concept de la sécurité (Petersen 2012, 703). Beaucoup d'auteurs relèvent (Lupton 2013, Beck 1995, Giddens 1994, Dunn Cavelty 2008, Kristensen 2008) qu'il y existe une conscience très forte que les risques aujourd'hui ne peuvent être éradiqués de la façon dont on a réussi à éradiquer certains risques dans le passé, comme par exemples certaines maladies. En somme: « The concepts of controllability, certainty and security are integral to the first modernity collapse » (Williams 2008, 60).

3. Les écoles du risque qui viennent combler les lacunes de Beck

Bien que les travaux de Beck soient pertinents pour notre recherche, comme nous venons de le voir, il n'en reste pas moins qu'il existe des lacunes importantes dans les travaux du sociologue qu'il convient maintenant de mettre en exergue.

Tout d'abord, Beck néglige les aspects esthétique et culturel de la réflexivité (Mythen 2004). La conception du risque comme étant culturellement construit est au centre des travaux anthropologiques de Mary Douglas. Elle a notamment conceptualisé la théorie culturelle du risque avec Aaron Wildavsky. Leur approche structuraliste met en valeur l'existence de plusieurs façons de voir les risques et donc il existe différentes rationalités qui peuvent être en concurrence selon Mary Douglas et Aaron Wildavsky (Williams 2009, Heng 2006, Petersen 2012, Lupton 2013). Dans le cas de coopération multilatérale par exemple, cela veut dire que malgré des valeurs communes, les 2 côtés de l'Atlantique sont culturellement différents (Williams 2009). Dans les travaux récents sur le risque, cette posture est défendue aujourd'hui par des chercheurs comme Gabe Mythen, Deborah Lupton, et Michael C. Williams. La principale différence avec Beck réside dans l'idée qu'il y a une différence, une frontière nette entre Soi et l'Autre, notamment en ce que

le concept de risque permet de marginaliser l'Autre et donc de renforcer la légitimité du Soi (Lupton 2013, Kempf 2014). Sur ce point, nous pensons, pour les raisons évoquées plus haut, que le concept de réflexivité permet d'appréhender la cyberdéfense à l'OTAN de façon pertinente.

Ensuite, il nous paraît intéressant de s'intéresser aux travaux de la discipline de la psychologie sociale car ils présentent également des notions que Beck n'intègre pas à sa réflexion. En effet, les travaux du psychologue Paul Slovic ont permis de mettre une emphase nécessaire sur la perception du risque (Slovic 2002). En effet, ses travaux permettent notamment de comprendre comment la perception publique d'un risque influe sur l'analyse de risque faite par les experts et, par conséquence, sur la prise de décision (Slovic 2002). D'autres chercheurs comme Robert Jervis ont également pris part dans les recherches au sujet de la perception du risque. Ces auteurs ont notamment permis d'établir la différence entre menace et risque en mettant en avant l'idée que la menace est actuelle, réelle alors que le risque est potentiel et est donc intrinsèquement lié à la subjectivité individuelle (Williams 2009, Heng 2006). Nous nous intéresserons notamment aux questions de perception dans le deuxième chapitre sur le terrorisme et le cyber-terrorisme.

Un autre reproche que nous pourrions faire à Beck est de ne pas fournir une méthodologie convaincante et de ne pas intégrer à sa réflexion les conséquences de cette conscience du risque qu'il met en lumière. Nous pensons à cet effet que l'approche poststructuraliste offre des éléments incontournables à l'étude de notre sujet. Dans une perspective foucaldienne, les tenants des études critiques de sécurité, et plus particulièrement des études critiques du risque, ont conceptualisé le risque autour du discours de sécurisation et de la notion de dispositif. En prenant comme point de référence les attentats terroristes du 11 septembre 2001, les auteurs de ce courant cherchent à montrer que la gestion du risque produit des significations et qu'elle discipline (Mythen 2004, Grondin 2005, Dunn Cavelty 2008, Brunner 2008, Araday et van Munster 2008, Pertersen 2012,

Hansen 2012, Holland 2013). En d'autres termes, ces auteurs permettent d'approfondir ce que Beck écrit, ou plutôt n'écrit pas, à propos du savoir : « Discourses both delimit and make possible what can be said and done about phenomena such as risk » (Lupton 2013, 23). Nous voulons montrer que la gestion des risques est une méthode de gouvernement qui peut s'appliquer à plusieurs thèmes, aussi bien le terrorisme que le cyber, et qu'elle est génératrice d'insécurité (Pomarède 2011, Mythen 2004, Bigo 2005). De plus, elle permet des abus sécuritaires que nous voulons exposer dans cette recherche.

Ces différentes approches ne sont pas antinomiques et peuvent jusqu'à un certain point dialoguer entre elles. D'ailleurs, nos recherches montrent que quelle que soit la perspective adoptée, Beck est incontournable dans les discussions sur le risque. Petersen va même jusqu'à catégoriser tous ces auteurs (Beck, Luhmann, Foucault, Giddens) comme des « radical constructivists within sociology » (Petersen 2012, 697). En effet, d'après elle, le risque est appréhendé dans sa gestion, c'est-à-dire un moyen de calculer, de le rationaliser. Lupton relève également des points communs importants entre ces approches plus ou moins structuralistes. Selon elle, le premier point commun évident est le fait que tous considèrent le risque comme l'élément central autour duquel toute la société est organisée et qu'il est de ce fait devenu omniprésent dans l'existence humaine en Occident (Lupton 2013, 37). De plus, tous les auteurs reconnaissent que le risque est associé à la subjectivité humaine, notamment en ce qu'il est associé aux notions de choix et de responsabilité. Luhmann (2005) relève également un élément intéressant. Selon lui, le point commun entre tous est le consensus à propos du fait que le risque n'est pas uniquement psychologique, c'est un problème social. De plus, comme l'affirme Michael C. Williams: « 'Security', then, lies neither solely in the discourse or speech act, not solely in the knowledge

discourse, not directly in the organization. It functions in the context of all three. » En conséquence, nous choisissons d'adopter un cadre théorique hybride entre ces approches.

Avant d'évoquer notre méthodologie, nous souhaitons mettre l'emphase sur un point de divergence qui nous semble être important dans cette discussion. Beaucoup d'auteurs critiquent Beck pour ne pas être clair sur sa position constructiviste. En effet, Beck fait la distinction entre l'existence autonome du risque et sa perception. Il identifie notamment des risques externes, opposés aux risques manufacturés (Beck 2009), ce qui dans une certaine mesure n'est pas une idée incongrue en ce qui concerne les risques environnementaux (nous pensons notamment ici aux phénomènes tels que les typhons, les ouragans, etc.). Cependant, même en ce qui concerne les risques manufacturés, Beck n'admet pas clairement s'ils sont construits ou s'ils possèdent une existence intrinsèque (Mythen 2004), contrairement aux poststructuralistes qui considèrent que tout risque est construit (Hansen 2012). En ce qui concerne notre sujet, la perspective poststructuraliste nous semble la plus exacte. En effet, nous concevons chaque cyber attaque, chaque risque cybernétique, comme une construction. Selon Beck, moins les risques sont calculables, plus l'aspect culturel joue un poids dans la perception qu'on s'en fait. Par conséquent, on peut arriver à un flou entre risque et sa perception culturelle (Beck 2009). Pour cela, Beck est considéré comme étant réaliste et constructiviste à la fois (Mythen 2004, Heng 2006, Scott 2000).

4. Méthodologie

Cependant, deux difficultés se posent à nous au niveau méthodologique : d'une part, nous abordons un sujet très technique et complexe, il faudra donc s'attacher à le vulgariser (sans pour autant le simplifier). D'autre part, nous sommes conscients qu'une grande partie des documents

concernant la cyber défense de l'OTAN est classifiée. Une des solutions pour remédier à ce problème serait de conduire des entretiens auprès de personnes œuvrant à la cyber défense à l'OTAN. Cette recherche ne bénéficiant d'aucun soutien financier, et dans un souci de temps, nous avons fait le choix de ne pas mener d'entretiens. Par conséquent, nos sources primaires seront principalement des documents officiels de l'OTAN. Pour les analyser, nous utiliserons la méthodologie de Lene Hansen telle qu'elle l'a formulée dans son ouvrage *Security as Practice. Discourse Analysis and the Bosnian War* (2006). Nous pensons que cette méthodologie est pertinente, parce qu'elle se place dans une perspective poststructuraliste, c'est-à-dire que la construction d'idées et de pratiques s'opère par la construction de discours. Selon Hansen: « The analytical intent is not to measure the relative importance of ideas and materiality but to understand them as constructed through a discourse which gives materiality meaning by drawing upon a particular set of identity constructions » (Hansen 2012, 23). L'objectif de cette méthodologie est donc de déconstruire les discours sécuritaires afin de montrer que ce qui est présenté comme étant un risque sécuritaire objectif ne l'est en réalité pas. Cette perspective tente de palier aux faiblesses énoncées concernant l'application empirique des travaux de Beck mais également au flou laissé par Beck quant à sa posture constructiviste assez fragile (Mythen 2004). De plus, dans son ouvrage, Hansen applique cette méthodologie aux missions menées en Bosnie par l'OTAN pendant la guerre dans les Balkans. L'auteure propose ainsi une analyse qui s'intéresse à la façon dont l'organisation transatlantique construit de façon discursive son environnement stratégique, tout en s'interrogeant à la production d'une légitimation de ses actions et des conséquences sur son identité; c'est ce que la présente recherche essaye d'établir.

Le plan de recherche qu'Hansen propose se divise en 4 axes. Premièrement, il faut analyser la construction de l'identité de l'OTAN en identifiant quel(s) « Autre(s) » permettent de définir le

« Soi ». Suivant les travaux de Beck sur la réflexivité, nous soutenons que l'OTAN se construit en opposition à elle-même. Ensuite, il s'agit de choisir un cadre temporel. Pour cette recherche, nous nous intéresserons surtout à la période 2007-2017, car ce n'est que depuis une décennie que l'OTAN gère le risque cybernétique. Cependant, nous sortons de ce cadre temporel à plusieurs reprises; d'une part, nous utilisons des documents de stratégie des années 1990 afin d'expliquer l'évolution doctrinale de l'OTAN et, d'autre part, notre réflexion ne saurait être complète sans les stratégies de militarisation du cyberespace menées par les États-Unis, notamment la President's Commission on Critical Infrastructure Protection mise en place par l'administration Clinton en 1997. Troisièmement, il nous faut sélectionner des évènements à analyser. Nous en avons identifié deux majeurs : le 11 septembre 2001 et les cyber-attaques vécues par l'Estonie en 2007. Le chapitre 2 s'intéresse précisément aux effets du 11 septembre 2001 sur la construction de l'OTAN en tant que gestionnaire de risque. En ce qui concerne l'Estonie, nous jugeons qu'il s'agit du moment-clé qui a décidé l'OTAN à s'investir massivement dans la cause de la cybersécurité. Enfin, il faudra décrypter les références intertextuelles, c'est-à-dire identifier dans les discours des références faites à des concepts ultérieurs dans le but de renforcer la légitimité du texte présent (Hansen 2012, 57). C'est sûrement l'élément le plus original de la méthodologie que propose Lene Hansen, c'est pourquoi nous chercherons à le mettre en avant au cours de cette thèse. Nous verrons notamment comment les documents stratégiques de l'OTAN sur la cyberdéfense font référence à la stratégie de contre-terrorisme des États-Unis ainsi qu'à la doctrine historique de l'OTAN : la dissuasion. En ce qui concerne concrètement les sources, Hansen rappelle qu'une analyse des textes officiels de politique étrangère ne se suffit pas à elle-même et qu'il est important de replacer ces documents dans leurs contextes respectifs. Il faut selon elle les considérer: « as entities located within a larger

textual web; a web that both includes and goes beyond other policy texts, into journalism, academic writing, popular non-fiction, and, potentially, even fiction » (Hansen 2006, 55).

Conclusions

Ce premier chapitre a été l'occasion de présenter comment le nexus risque et sécurité est devenu le cœur des relations internationales de ces 25 dernières années. Nous avons tenté de mettre en lumière la montée de nouvelles menaces asymétriques et de nouveaux risques à la fin de la guerre froide et dans un contexte de mondialisation et de terrorisme mondial. Ces risques possèdent 2 caractéristiques que nous avons mis en avant à travers les notions de savoir et de temporalité: ils sont virtuels et incertains. Face à ces nouveaux risques, les décideurs ont compris qu'il n'allait pas être possible de garantir la sécurité et que chercher à éliminer les risques était vain. C'est en tout cas la conclusion que tirent les auteurs des différentes perspectives théoriques mobilisées pour cette recherche. Nous avons mis en exergue les travaux du sociologue Ulrich Beck qui a théorisé la « société mondiale du risque » et la réflexivité (Beck 2009). Beck a voulu montrer avant tout que la modernité a engendré la disparition des frontières nationales et la diffusion mondiale et homogène du risque. Il a notamment mis en avant le fait que les acteurs, dans notre cas l'OTAN, ne se définissent plus en fonction d'un autre (par exemple l'URSS), mais par rapport à eux-mêmes car le risque est une projection subjective d'une crainte présente. Cependant, nous avons jugé utile de venir combler les faiblesses, notamment méthodologiques, des travaux de Beck en mobilisation des contributions dans d'autres disciplines, notamment en psychologie et en science politique. En effet, nous pensons qu'il ne faut pas sous-estimer les questions de perception du risque, notamment en ce qui concerne les questions relatives au cyberespace. Nous allons voir dans la prochaine partie que les discours de sécurité reposent en grande partie sur la perception du risque, à la fois du côté

des analystes de risque et des décideurs, mais également du côté de public qui est plus enclin à accepter des mesures liberticides s'il a une perception élevée du risque (Slovic 2002). Par ailleurs, les auteurs poststructuralistes en relations internationales ont mis en exergue le concept de sécurisation afin de montrer que certains sujets sont devenus des enjeux de sécurité et que cela n'est pas sans conséquence. Nous donnons du crédit à ces travaux car un de nos objectifs est de montrer comment les autorités américaines et l'OTAN ont en partie militarisé les enjeux autour du cyber. Nous pensons à cet égard que la méthodologie de Lene Hansen, notamment grâce à l'importance qu'elle donne à l'intertextualité, va nous permettre de souligner les liens existants entre différentes sécurisations, particulièrement le terrorisme et le cyber. Nous cherchons à montrer que parler de risque, de gérer les risques, est une façon de légitimer le pouvoir octroyé et la mainmise sur le thème du cyber : « Politicians declaring something 'at risk' are more likely to get attention and get the nation focused on an issue » (Heng 2006, 22). Dans cette perspective, nous allons à présent nous intéresser aux effets qu'ont eu les attentats du 11 septembre 2001 sur l'OTAN. Nous cherchons à faire le lien entre gestion du risque terroriste et la gestion du risque cybernétique en analysant comment la préemption est devenue le cœur de la gestion des risques en Occident.

CHAPITRE II – LES EFFETS DU 11 SEPTEMBRE 2001 SUR L'OTAN : LA GESTION ALGORITHMIQUE DU RISQUE TERRORISTE

Nous procédons dans ce chapitre à une contextualisation de la doctrine de cyber défense de l'OTAN. Au sortir de la guerre froide, l'OTAN est à la recherche de nouvelles menaces, d'une nouvelle façon d'affronter sa réalité. Progressivement, il a été possible d'observer la transformation de l'OTAN en gestionnaire de risque. Pour ce faire, notre étude se penche en détail sur les concepts stratégiques de 1991 et 1999. Ensuite, nous verrons comment l'année 2001 a véritablement marqué un tournant dans la volonté de l'OTAN d'étendre sa sphère d'influence à l'Europe de l'Est. Dans un deuxième temps, il conviendra de se pencher sur l'acteur majeur de l'OTAN, à savoir les Etats-Unis, pour étudier en détail la mise en opération de la logique préemptive par l'Administration Bush dans le cadre de la guerre contre la Terreur. Nous verrons notamment les dérives engendrées par les pratiques sécuritaires de l'Administration Bush en nous intéressant à la surveillance et aux révélations d'Edward Snowden.

A) L'OTAN : une institution de sécurité collective

Un concept stratégique est révélateur de la façon dont l'OTAN perçoit son environnement et se perçoit elle-même. L'objectif d'un concept stratégique selon l'OTAN est d'identifier l'environnement stratégique et de décrire la nature et les objectifs des missions que se fixent les Alliés par rapport à cet environnement[2]. En somme, ces documents représentent des consensus sur

[2] OTAN 2016, http://www.nato.int/cps/fr/natohq/topics_56626.htm

la politique militaire à mener (Rasmussen 2001). C'est pourquoi nous pensons qu'il est incontournable de s'y pencher.

1. Un nouvel environnement stratégique

La chute de l'Union Soviétique a marqué la fin d'une ère dans les relations internationales. Elle a eu un impact singulier à l'OTAN, car il s'agit d'une alliance multiétatique qui a précisément vu le jour en 1949 : en 1955, l'URSS lui a opposé le Pacte de Varsovie. Dans le concept stratégique de 1991, l'OTAN déclare : « La menace monolithique, massive et potentiellement immédiate qui a été, au cours de ses quarante premières années d'existence, le souci primordial de l'Alliance, a maintenant disparu. Cependant, l'avenir reste entouré d'incertitudes et il subsiste des risques pour la sécurité de l'Alliance » (Concept Stratégique 1991, §6). La disparition de son ennemi unique a donc laissé l'OTAN dans une position inconfortable, car elle a perdu sa raison d'exister. De ce fait, le risque de désintégration était élevé et les théoriciens de l'école réaliste prédisaient d'ailleurs la fin de l'Alliance. Sans pour autant parler de fin de l'existence de l'OTAN, il faut reconnaître que s'il est facile de s'accorder à définir un ennemi unique et commun dans un contexte relativement stable, dans le contexte de mondialisation et de post-guerre froide est marqué par l'incertitude et la multiplication des menaces, cela a favorisé les désaccords à de nombreuses échelles (Coker 2002, Williams 2008). Le problème qui s'est révélé être le plus important fût l'identification des menaces et la façon dont elles devaient être appréhendées par les Alliés : « While the allies agree that risk is the concern of NATO now, they are unable to agree on the nature of risks, on what risks to manage and how to manage them. Managing insecurity is proving a much more difficult task than providing Cold War security ever was » (Williams 2009, 114).

Il a donc fallu chercher de nouvelles menaces, se redéfinir dans un nouvel environnement stratégique. Dans le contexte de mondialisation, l'OTAN s'est intéressée à la montée des menaces asymétriques marquées par de nouveaux modes d'action et par la multiplication d'acteurs non-étatiques qui remettent en question la supériorité stratégique de l'OTAN (Abrial 2010). Des années 1990 à 2001, à l'instar des États-Unis, l'OTAN a priorisé des menaces telles que les armes de destruction massive, les changements de régime dans un objectif de stabilisation des relations internationales, de libéralisation économique et de démocratisation (Heng 2006, Williams 2009, Rasmussen 2001). Dans les concepts stratégiques de 1991 et 1999, l'emphase est mise sur la gestion du risque lié aux armes de destruction massive (Concept Stratégique 1999, §22-23-24). Ces menaces issues de la mondialisation sont également caractérisées par le fait que l'OTAN est désormais concernée par des risques qui sont géographiquement loin, ce qui a considérablement influencé sa culture stratégique (Abrial 2010). Certains pays-membres ont manifesté leur volonté que l'OTAN sorte de ses frontières et cela a généré des conflits en interne. En effet, il y a eu des désaccords à propos de la limite géographique à fixer : « After the 1999 Kosovo operation NATO had engaged in a debate on the meaning of "out-of-area" operations, but at the time it had failed to reach an agreement on how far the geographic area would extend » (Michta 2006, 108). L'OTAN fait référence à de nombreuses reprises à la gestion des crises, sans toutefois amener de précision quant à ces risques (Heng 2006, Williams 2009, Williams 2008, Herd, Kriendler et Wittman). Nous pouvons apprécier ce flou stratégique par exemple au paragraphe 3 du Concept Stratégique de 1999 : « Les dix dernières années ont toutefois vu également l'apparition de nouveaux risques complexes pour la paix et la stabilité euro-atlantiques, risques liés à des politiques d'oppression, à des conflits ethniques, au marasme économique, à l'effondrement de l'ordre politique, et à la prolifération des armes de destruction massive. » Selon Abrial, les objectifs

pour l'OTAN sont de maintenir des capacités flexibles et adaptables, et également une supériorité technologique (Abrial 2010). Nous notons ici le continuum de la gestion dissuasive, comme il l'est d'ailleurs affirmé en 1999 : « Exercer une fonction de dissuasion et de défense contre toute menace d'agression visant un pays quelconque de l'OTAN, conformément aux dispositions des articles 5 et 6 du Traité de Washington » (Concept Stratégique 1999, §10). Les nouveaux risques liés à la mondialisation viennent mettre en péril l'objectif de paix et de stabilité de l'OTAN, car ils sont difficiles à calculer et bien souvent, la stratégie dissuasive ne suffit plus : « Au lieu de résulter d'une menace prédominante, les risques qui subsistent pour la sécurité des Alliés se présentent désormais sous des formes complexes et proviennent de directions multiples, ce qui les rend difficiles à prévoir et à évaluer » (Concept Stratégique 1991 §9; Coker 2002). Huit ans plus tard, l'OTAN réitère : « La sécurité de l'Alliance reste exposée à des risques militaires et non militaires très divers, qui viennent de plusieurs directions et sont souvent difficiles à prévoir » (Concept Stratégique 1999, §20). On observe à travers ces déclarations que l'OTAN considère désormais les menaces de sécurité internationale comme un flot difficile à appréhender et donc à gérer (Rasmussen 2006, 109). Dès lors, l'OTAN se réinvente et intègre progressivement la gestion de risques comme nouveau mode de gouvernement.

2. L'élargissement de l'Alliance

La décennie 2000 a par ailleurs vu l'élargissement progressif de l'Alliance, résultant d'une volonté d'élargissement de l'OTAN entamé dans les années 1990, notamment avec le programme des Partenariats pour la paix, lancé en janvier 1994, et qui a constitué une porte d'entrée progressive pour des pays désireux de rejoindre l'OTAN. Cet élargissement visait à construire une « meilleure architecture de sécurité dans l'ensemble de la zone euro-atlantique » (OTAN, Étude

sur l'élargissement de l'OTAN, §1, 3 septembre 1995). Il n'y a eu aucun élargissement entre 1982 (Espagne) et 1999, lorsque la République Tchèque, la Hongrie et la Pologne ont intégré l'Alliance. C'est donc surtout à partir du début des années 2000 que le processus s'accélère réellement avec, dès 2003, la signature des protocoles d'accessions de sept nouveaux pays-membres (Bulgarie, Estonie, Lettonie, Lituanie, Roumanie, Slovaquie et Slovénie), qui adhèrent officiellement à l'OTAN le 29 mars 2004. L'Albanie et la Croatie ont rejoint l'Alliance en 2009, ce qui porte à 28 le nombre d'États-membres à l'heure actuelle, sachant que l'année dernière, les ministres ont signé le protocole d'adhésion du Monténégro, qui devrait donc devenir le 29ème membre. Ces vagues successives d'élargissement sont le résultat de la politique de « porte ouverte » ancrée dans le traité fondateur de l'OTAN. Mais il est également possible, au vu de la chronologie d'intégration, de dresser un parallèle avec la réorganisation militaire des Etats-Unis post-2001. En effet, comme l'explique David Grondin, les décideurs politiques américains ont articulé leur stratégie de guerre contre la terreur autour du basculement de la stratégie d'endiguement de la guerre froide à l'intégration mondiale : « US national security governmental managers have indeed responded to the security challenges of 11 September 2001 in re-discovering their homeland and in envisioning their homeland through global terms » (Grondin 2010, 89). Dès 1995 à l'OTAN, une étude menée sur les bénéfices offerts par l'élargissement de l'Alliance stipulait notamment que l'intégration de nouveaux membres favoriserait la stabilité et la sécurité collective « sans créer de zone de division » (OTAN 1995, §1), sous-entendu en repoussant la frontière entre le « noyau fonctionnel » et le « fossé non-intégré » (Grondin 2006, 49). En d'autres termes, l'OTAN s'inspire de la stratégie militaire impérialiste des Etats-Unis qui est de marquer la frontière entre les États libéraux qui ont embrassé la mondialisation et ceux qui y résistent, et qu'il faut nécessairement conquérir voire

combattre. En ce sens, cette logique géopolitique met en exergue comment l'OTAN est parvenue, par l'intégration de nouveaux membres, à étendre son influence en Europe de l'Est.

En outre, les concepts stratégiques sont perçus comme des « meta-narratives which have been constructed to re-invent a role for NATO after the implosion of the USSR and with the aim to reinforce a sense of NATO community in a period of critical security threats » (Ercolani 2012, 103). Il y a en effet une performativité dans les concepts stratégiques, c'est pourquoi il est important de les étudier. Cette approche de gestion de risque permet également à l'OTAN de participer de façon proactive à définir son environnement stratégique plutôt que de le subir comme pendant la guerre froide. En effet : « Following the end of the Cold War, NATO has turned institution-building into an offensive strategy of "rule-altering" politics. By making itself the institutional center of European security, NATO has sought to manage the transformation of the Cold War system » (Rasmussen 2001, 299). Dès 1991 d'ailleurs, on peut déjà déceler la volonté de l'OTAN d'imposer sa conception de la sécurité: « ce nouvel environnement offre en revanche à l'Alliance de nouvelles occasions d'inscrire sa stratégie dans le cadre d'une conception élargie de la sécurité » (Concept stratégique 1991, §15). Mais comme nous allons le voir, l'obsession de la sécurité a poussé l'OTAN à adopter une gouvernementalité par la gestion de risque.

B) 11 septembre 2001 et gestion du risque terroriste

1. 11 Septembre : le « choc de vulnérabilité » (William Perry)

Les attentats du 11 septembre 2001 ont mis un terme à l'idée que les Etats-Unis étaient une superpuissance impénétrable. En ce sens, le 11 septembre représente un réel « choc de

vulnérabilité » selon l'expression de William Perry, le Secrétaire de la Défense de l'Administration Clinton de 1994 à 1997 (cité dans Rasmussen 2006). Comme l'explique Holland : « US strategic culture has long been characterized by illusions of Homeland impenetrability (sheltered by two vast oceans), a zero-death military culture and a hypervaluisation of American life » (Holland 2013, 23). Les attentats contre le *World Trade Center* ont mis en exergue cette vulnérabilité et cela a provoqué une irrationnelle urgence d'agir. Les auteurs qui se sont intéressés au discours néoconservateur ont pu affirmer que les autorités américaines ont créé des récits patriotiques forts sur l'identité, établis en opposition aux terroristes (Holland 2013, Grondin 2005, Hansen et Nissenbaum 2009).

La responsabilité de ces attentats a beaucoup été porté sur le manque d'imagination des analystes des services de renseignement américains. En ce sens, les décideurs américains ont mis en parallèle Pearl Harbor et le 11 septembre dans la perspective d'un changement majeur de paradigme dans la gestion de la sécurité (Salter 2008, Holland 2013, de Larrinaga et Doucet 2010, Grondin 2010). L'intertextualité a permis aux décideurs américains de justifier des mesures exceptionnelles pour assurer la sécurité nationale. On voit dès lors la mise en place d'une logique de guerre froide, où l'ennemi ne serait plus l'URSS mais le terrorisme islamiste (si tant est qu'il soit possible de le circonscrire), face auquel se construit discursivement l'image des États-Unis (Grondin 2010, 2005).

Par ailleurs, les auteurs identifient la présence d'une illusion de sécurité qui s'inscrit en filigrane dans les discours officiels américains visant à instaurer la guerre de la terreur, notamment à travers les notions de risque et de scénarios-catastrophes (*worst-case scenarios*). Ce mode de gouvernement n'a pas vu le jour en 2001 puisque déjà dans le concept Stratégique de 1999, il est question de scénarios et de « gamme complète des situations possibles » (1999, §49) et plus loin,

l'OTAN fait part de la nécessité de se préparer au pire scénario à long terme (1999 §54). Cependant, la nouveauté réside dans le fait que les décideurs tendent à surestimer à la fois les menaces pesant sur le « territoire national » (*homeland*) et en même temps leur pouvoir d'agir, dans un objectif d'asseoir leur légitimité et le nouveau mode de gouvernementalité (Luhmann 2005, Aradau et Van Munster 2008, Dunn Cavelty 2009, Bonditti, Heng 2006). Ainsi, l'étude des discours permettent d'observer une stratégie qui vise à convaincre les citoyens américains que le gouvernement va se donner les moyens de garantir leur sécurité : « Risk in this sense is categorically not about reducing risk, achieving control, or even about ensuring safety or security – what matters instead is that the *appearance* of securability and manageability is sustained. […] To consider risk as the dominant technology of the war on terror, then, is to engage with the practices that are enacted *in the name of* managing risk and uncertainty » (Amoore et de Goede 2008, 9). Cette représentation du terrorisme mondial donnée par les États-Unis a permis aux décideurs américains d'exercer un contrôle sur les peurs des citoyens, ce que les auteurs des études critiques de sécurité ont nommé la gouvernementalité par l'inquiétude (Bigo 2005, Van Loon 2000 et 2002, Grondin 2005). L'atout majeur pour l'Administration Bush a été de pouvoir de ce fait maintenir son agenda (Grondin 2005).

2. *Homeland Security ou le retour de la superpuissance américaine*

Le 11 septembre a permis de réaliser que certains risques liés à la mondialisation ne sont plus les fruits de stratégies préméditées. Par conséquent, ils ne sont plus calculables, ce qui rend les stratégies de réaction caduques et promeut les stratégies de prévention (Heng 2006, 25). La gestion du risque terroriste se décline de deux manières : l'anti-terrorisme, dont le but est de réduire la probabilité d'une attaque, et le contre-terrorisme, qui réside dans les actions proactives prises pour

prévenir une attaque terroriste (Heng 2006). Le premier terrain où il fallait agir était le terrain discursif et de ce point de vue, les auteurs s'accordent à dire que George W. Bush a réussi à définir sa politique contre-terroriste (Holland 2013, Heng 2006). En effet, il a réussi à présenter et faire accepter aux citoyens américains du bien-fondé d'une gestion de risque préemptive, de la rupture avec tout ce que les États-Unis avaient connu auparavant. D'ailleurs, Holland a observé à juste titre que dans les discours de George W. Bush, le marqueur « outlaw » est très fréquemment utilisé ainsi que le champ lexical du choc et de la rupture (Holland 2013). Cette rupture s'effectue avant tout au niveau militaire comme le prouve l'étude des doctrines post-11 septembre. Grondin nous permet de comprendre la réorganisation de l'appareil gouvernemental militaire américain en analysant les deux documents doctrinaux majeurs : la stratégie de sécurité nationale (SSN) et la stratégique militaire nationale (SMN). L'auteur montre dans une approche intertextuelle « [l'] incapacité [des États-Unis] à comprendre les particularités d'un nouveau contexte stratégique sans recourir à des pratiques établies » en mettant en exergue le poids de l'héritage de la *Loi sur la Sécurité nationale* de 1947 (Grondin 2006, 36). A travers la création du département de la Sécurité intérieure, les États-Unis visent à recouvrer leur place de superpuissance acquise après la Seconde guerre mondiale.

La doctrine sur la préemption a été officialisée par George W. Bush lui-même lors d'un discours à l'académie militaire de West Point le 1er juin 2002 (Grondin 2016). La stratégie de sécurité nationale de 2002 marque le moment charnière entre deux paradigmes sécuritaires : le premier étant marqué par une logique de dissuasion, le second par une logique de préemption (Grondin 2005). La SSN s'inspire en grande partie du *Defense Planning Guidance*, rédigé sous l'Administration de George H. Bush en 1992 par deux néoconservateurs qui ont eu une influence

considérable auprès de George W. Bush : Paul Wolfowitz et Lewis Libby. Ce document prônant une logique préventive était marqué par une volonté très forte de retour à l'unilatéralisme et à l'affirmation de la primauté des États-Unis (Grondin 2005). De prime abord, il semble y avoir une différence entre prévention et préemption. La prévention militaire consiste à agir dans le but de conserver la supériorité stratégique, contrairement à la préemption qui répondait de façon plutôt tactique à une menace estimée comme étant imminente (Grondin 2005, 2008). Mais les auteurs s'accordent à dire que dans la stratégie de sécurité nationale, les frontières entre les deux notions ne sont pas claires car elles reposent sur une même logique de proactivité : « The logic of the distinction between pre-emption and prevention breaks down when the distinction is transplanted from theory or law into strategic practice » (Rasmussen 2006, 94). En d'autres termes, prévention et préemption reposent sur l'idée que les risques ne peuvent pas être évités, seulement contrôlés. (Rasmussen 2006, Grondin 2016).

En 2003, George W. Bush annonce une intervention préemptive en Irak. Tout comme la mission de l'OTAN au Kosovo menée en 1999 était la première action préemptive de l'Alliance, l'Irak a été le moment décisif pour les États-Unis pour mettre en opération leur nouvelle doctrine. Mais le cas de l'Irak illustre le fait que prendre des mesures préemptives pour éviter un risque peut créer un risque encore plus important, ce que Beck appelle les effets boomerang : « They risk falling in a "pre-emptive trap" by acting on every scenario, thus ending by being caught in so many unintended consequences of their actions that they may have very few political resources left to manage these, or indeed any future risks. In both cases the mismanagement of pre-emptive strategies makes it difficult to manage risks » (Rasmussen 2006, 39). A terme, nous faisons le constat qu'en voulant anticiper et maitriser le futur, les sociétés ne participent qu'à produire

davantage d'insécurité. En ce sens, le risque est performatif: « As risks are claimed to exist, but their date and place of materialization are held impossible to predict, a sense of comprehensive and ever-present insecurity is created. Insecurity comes to be regarded as substantial if not all-encompassing, always present and always possible » (Hagmann et Dunn Cavelty 2012, 89).

Si Beck soutient l'idée que les sociétés du risque se réinventent plus démocratiques, nous pensons, à l'instar d'Aradau et de van Munster, qu'elles permettent des excès autoritaires (Aradau et van Munster 2007). Par ailleurs, la précaution est un mode de gouvernementalité qui permet surtout de favoriser des agendas cachés : « It should not be forgotten that risk management in the war on terror is not only a technique of governance, but also a profitable industry » (Amoore et de Goede 2005). D'une part, un agenda politique, car nous savons que l'Administration Bush, lorsqu'elle a été élue, ne possédait pas encore les moyens de mener à terme ses ambitions (Grondin 2005). D'autre part, il ne faut pas négliger les nombreux lobbys et partis d'intérêt qui ont soutenu cette politique. Nous pouvons tout à fait établir ici un parallèle avec le cyber. En effet, il ne faut pas sous-estimer le poids de toute l'industrie de la cybersécurité qui promeut ses services auprès des gouvernements, ainsi que les grandes entreprises du secteur elles-mêmes qui détiennent de fait une position de force en participant grandement à l'expansion et à la stabilité du cyberespace (nous pensons, entre autres, à Google, Microsoft, IBM, Apple).

Cependant, pour Bigo, « la dimension proactive en effet n'est en rien une simple prévention car elle suppose une action de surveillance visant éventuellement à influer sur un sujet individuel » (Bigo 1997, 423). En effet, la surveillance est au cœur de la gestion de risque en tant que mode de gouvernement, car ce dernier repose sur la scénarisation du futur et le calcul des risques par des probabilités (Grondin 2013). Dans le spectre du 11 septembre et de l'objectif zéro mort de la gestion par précaution, on a vu l'instauration d'une surveillance à très grande échelle :

« Precautionary risk management implies the surveillance of all the population, of all flights for example, independent of existing intelligence. Hence more and more technologies of surveillance are indiscriminately targeted at the whole population: stop and search policies in the UK, biometric identifiers or the introduction of identity cards » (Aradau et van Munster 2007, 104). Ce que nous indiquent Aradau et Van Munster a été confirmé par les révélations d'Edward Snowden à propos des programmes illégaux de surveillance massive développés par les États-Unis. Snowden était un ingénieur informatique américain qui a travaillé comme employé puis contractuel pour différentes agences de renseignement, dont la CIA et la NSA. Suite aux divulgations, il a dû s'exiler en Russie où il réside présentement. Snowden a notamment révélé l'existence du programme PRISM dont le but est d'épier l'ensemble des télécommunications mondiales par l'accès illégal aux flux de données des serveurs américains des géants des télécommunications tels que Google et Verizon, ainsi qu'à leurs réseaux de communication transitant par le territoire américain. Cette surveillance mondiale se fait à partir d'algorithmes; cette logique sécuritaire est qualifiée par David Grondin d'« assemblage de surveillance algorithmique » ou plus simplement de « gouvernance algorithmique » (Grondin 2016, 180-181) : en collectant toutes les traces que nous laissons dans le cyberespace et en croisant différentes bases de données, les analystes comptent sur les algorithmes pour quantifier le risque là où l'Homme échoue.

Pour Coutin, les analystes ne cherchent pas à acquérir plus de savoir, mais ils cherchent à obtenir les meilleures prémonitions, « a stab in the dark » (Coutin 2008, 213). Ce n'est pas sans rappeler le film *Minority Report* produit par Steven Spielberg (2002) qui met en exergue ce rapport nouveau à la temporalité : la gouvernance par le futur. Dans la fiction de Spielberg, ce sont les actions futures d'un individu (un « pré-criminel ») qui sont calculées par des êtres mutants ayant

des capacités de précognition, ce qui permet à l'agent Anderton d'agir de façon proactive (en arrêtant l'individu) dans le but d'éviter le crime (Coutin 2008, Grondin 2016). Cette fiction est l'occasion de montrer que le concept de tolérance zéro au risque pousse à une projection vers le futur, vers le virtuel. Dans le domaine militaire, on retrouve cette virtualité dans des technologies comme les drones qui tendent à se rapprocher du « zero casualty » (voir Grondin 2013 et Holmqvist 2013). De la même façon, on retrouve cet objectif dans la lutte contre-terroriste qui justifie les actions préemptives (Amoore et de Goede 2008, 11). De plus, *Minority Report* met en relief le lien entre préemption et suspicion normalisée (Ericson 2008). De ce fait, on a assisté à l'avènement du gouvernement par l'exceptionnalisme justifié par la doctrine Bush et la projection de scénarios-catastrophes (Aradau et van Munster 2008, 25; Grondin 2013).

Conclusions

En somme, dans ce chapitre, nous avons voulu montrer que l'OTAN est devenue une gestionnaire de risques en cherchant à maîtriser son environnement stratégique ainsi que des menaces asymétriques. Ainsi, nous avons montré que l'Alliance a largement été influencée par les considérations sécuritaires américaines. En outre, les attentats du 11 septembre 2001 ont permis l'avènement d'une nouvelle gouvernementalité qui a porté le concept de sécurité nationale comme fer de lance de la politique impérialiste militaire mondiale des États-Unis (De Larrinaga et Doucet 2010). Ce mode de gouvernement par la sécurité nationale s'est opéré par une transition entre l'élimination des menaces à la préparation et au management des risques et des incertitudes (Heng 2006, Coutin 2008, Ericson 2008, Aradau et Van Munster 2008, Grondin 2010, Mythen et Walkate 2016). Pour traiter ce thème, il nous apparaît que l'approche foucaldienne de gouvernementalité a été la plus pertinente. En effet : « Despite the similarity to Beck's uninsurable risks, a Foucaldian approach does not portray risks as calculable/incalculable, but rather focuses on "how" presumably

incalculable catastrophic risks like terrorism are governed » (Aradau et Van Munster 2007, 101). En d'autres termes, les travaux de Beck constituent une base intéressante pour penser le rapport entre le savoir et le risque, mais la notion de dispositif et les travaux sur le principe de précaution nous ont permis d'approfondir notre réflexion. En effet, le dispositif du risque nécessite une tentative de calculer le futur dans la perspective de le contrôler et de réduire ses effets néfastes (Aradau et Van Munster 2007, 97-98). Mais, comme nous l'avons montré, cela donne lieu à plus d'insécurité et à une réduction des libertés dans le cyberespace, qui de fait devient un espace à la fois libérateur et disciplinant (Grondin 2016). Nous souhaitons désormais illustrer notre propos sur la gouvernementalité par l'inquiétude en nous intéressant au cyber-terrorisme, un risque qui permet de se pencher sur les effets psychologiques et la question des imaginaires.

CHAPITRE III – LA GESTION DU RISQUE CYBER À L'OTAN : PRÉCAUTION ET DISSUASION

Le cyberespace est devenu un sujet majeur des réflexions stratégiques. Si nous avons consacré notre deuxième chapitre au 11 septembre et à ses effets sur l'OTAN, il ne s'agit pas de penser que rien n'a été fait pour tenter de sécuriser le cyberespace. Ainsi, comme le rappelle Petersson : « Cyber warfare and cyber threats are not a new phenomenon, but during the last decade they have been discussed in a new way, although this debate was not necessarily connected to 9/11. Rather, it was due to a more general, and growing, concern that strategic cyber attacks have been directed against government information systems from other states and organizations » (Petersson 2013, 144). Nous voulons à présent montrer comment la doctrine a été formée et quels évènements ont marqué cette stratégie en Occident. Nous verrons comment le cas des cyber attaques vécues par l'Estonie en 2007 et le virus Stuxnet ont participé à cette perception du risque cyber. Il y a, par exemple l'adoption en 2014 du cyber dans la défense collective. Il a été annoncé au sommet de Galles que le cyberespace se trouve désormais sous la protection de l'Article 5 du traité fondateur de l'OTAN selon lequel « toute attaque armée contre l'un ou plusieurs de ses membres sera considérée comme une attaque dirigée contre toutes les parties ». Cet article n'a été déclenché qu'une seule fois à la demande des États-Unis en septembre 2001. On observe dès lors que le cas estonien et le virus Stuxnet ont participé à façonner la perception du risque à l'OTAN qui s'est depuis attachée à orienter sa stratégie vers une défense des cyber attaques pouvant avoir des conséquences semblables à des attaques plus conventionnelles (Rapport de Commission annuel 2011 – Information et sécurité nationale §65). En ce sens, nous partageons l'avis de Dunn Cavelty : « The Estonian example is one of the cases most often referred to in government circles to prove

that there is a need for action and the age of 'cyber war' has begun » (Dunn Cavelty 2012, 111). À ce titre, nous voulons montrer comment le cyber a été sécurisé par l'OTAN. L'objectif ici n'est pas de montrer comment l'OTAN gère les cyber menaces sur un plan technique, mais de voir que la doctrine de cyberdéfense s'inspire, d'une part, de la stratégie de précaution, notamment utilisée comme mode de gouvernement dans la lutte contre le terrorisme aux Etats-Unis. Afin d'illustrer notre propos, nous nous pencherons sur le risque de cyber-terrorisme, un risque qui permet de s'intéresser aux effets psychologiques et la question des imaginaires dans la gestion de risque. D'autre part, il s'agira de mettre en exergue tout le poids de la doctrine historique de dissuasion nucléaire.

A) La sécurisation du cyber par l'OTAN et l'antécédence de la stratégie américaine

Le contexte dans lequel l'OTAN s'est intéressée au cyber est à comprendre dans la perspective de la sécurisation du cyberespace née aux États-Unis, d'abord sous l'administration Clinton autour du concept d'infrastructures critiques, dont l'OTAN s'est servie pour construire sa propre doctrine de cyberdéfense. Puis sous Bush, on a vu l'incorporation du cyber dans la stratégie globale de lutte contre le terrorisme. Nous allons mettre en exergue l'adoption de la gestion américaine du risque cyber à l'OTAN. Nous verrons d'ailleurs dans le sous-chapitre subséquent la construction du risque cyber-terroriste et ses effets sur la gestion de risque.

1. Une prise de conscience progressive

La toute première fois que l'OTAN s'est officiellement intéressée à l'enjeu de la cyberdéfense remonte à 2002, lorsque le Conseil de l'Atlantique Nord, l'organe majeur de décision politique de l'OTAN, a approuvé, pendant le sommet de Prague, l'implantation d'un programme de

cyberdéfense (Hunker 2013, Everard 2008, Healey et Jordan 2014, Burton 2015). Le contexte dans lequel le cyber est arrivé sur la table des discussions politiques et militaires est sans surprise le 11 septembre 2001, mais il est important de rappeler que l'OTAN a été marquée par sa première cyber-attaque vécue lors de sa mission dans les Balkans en 1999. En effet, l'OTAN a subi ses premières attaques en déni de service distribué (DDoS) pendant qu'elle conduisait des attaques militaires contre la Serbie. Ces cyber-attaques ont causé l'interruption des services de courrier électronique et ont rendu impossible l'accès au site de diplomatie publique de l'OTAN qui servait à justifier ses opérations pendant la guerre du Kosovo (Everard 2008). C'est dans ces conditions que l'OTAN a décidé de mettre sur pied un organe de réaction aux incidents informatiques, le NCIRC (pour NATO Computer Incident Response Capability).

C'est en 2007 que l'OTAN prend réellement conscience qu'elle n'a pas de réelle capacité de cyberdéfense et surtout pas de doctrine adaptée (Hughes 2009). Les cyber-attaques subies par l'Estonie en réaction au démantèlement d'une statue de l'époque soviétique ont été le catalyseur de la stratégie de cyberdéfense de l'Alliance (Everard 2008, Petersson 2013). Dans un rapport publié en 2009, l'OTAN explique ce type d'attaque de la façon suivante :

> Pour préparer une attaque DDoS, l'agresseur commence par infecter au moyen d'un logiciel malveillant une série d'ordinateurs non protégés disséminés de par le monde, qui seront utilisés par la suite pour cibler la victime qu'il a choisie. Au moment de l'attaque à proprement parler, il envoie à chacun de ces ordinateurs « zombies » un minuscule paquet de données difficiles à repérer auquel il ordonne d'inonder la victime de dizaines de milliers de visites, brouillant et neutralisant ainsi les serveurs gérant la fourniture de services web. Parfois aussi, le logiciel d'attaque présent sur les machines compromises est doté d'un temporisateur déclenchant une attaque coordonnée sur la victime (Rapport de Commission annuel 2009 - L'OTAN et la cyberdéfense, §6).

Concrètement, les Estoniens ont été privés pendant plusieurs semaines d'accéder aux sites des deux plus grandes banques du pays, ainsi qu'à certains sites gouvernementaux. De plus, la possibilité de s'informer sur la situation a été entravée par le fait que de nombreux sites

médiatiques n'étaient pas fonctionnels (Hansen et Nissenbaum 2009). Ce même rapport met l'emphase sur le fait que l'Estonie a été l'élément déclencheur de la nécessité de protéger non pas seulement les réseaux propres de l'OTAN, mais également ceux de ses membres, un point qui deviendra central dans sa stratégie de cyberdéfense. Cependant, ces attaques n'ont eu que des conséquences économiques mineures et il s'agissait d'attaques assez communes, techniquement parlant (Dunn Cavelty 2012, Kempf 2014).

Malgré cela, les conséquences psychologiques de ces cyber-attaques ont poussé les Alliés à agir politiquement et militairement au cyberespace. 2007 marque donc le moment où le cyber est passé de sujet technique à sujet politique (Dunn Cavelty 2012) ; en ce sens, l'Estonie représente le début de la sécurisation du cyber par l'OTAN : « The ability of Estonian securitizing actors to have the attacks accepted as ''the first war in cyberspace'' and to have them prominently covered by the world press makes for at least a partially successful case of cybersecuritization » (Hansen et Nissenbaum 2009, 1169). Hansen et Nissenbaum notent que les Estoniens n'ont pas réussi à convaincre les Alliés de déclencher l'Article 5 de défense collective. On note toutefois l'extension du spectre de gouvernance de l'OTAN vis-à-vis du cyberespace dès le sommet de Bucarest en 2008 (Hughes 2009). Le lien a tout de suite été établi entre la cyberdéfense et les infrastructures critiques. Il convient donc ici de se pencher sur l'histoire parallèle de l'OTAN et des États-Unis. En effet, le cyber a été lié au discours de sécurité nationale par l'Administration Clinton dès 1997 à travers le concept d'infrastructures critiques. Dans une perspective foucaldienne, nous allons montrer que la protection d'infrastructures critiques répond à un problème de sécurité (Collier et Lakoff 2008, 17).

2. *La « protection des infrastructures critiques » : la sécurisation du cyber par les Administrations Clinton et Bush*

Le débat sur la cybersécurité a commencé aux États-Unis dans les années 1970 en parallèle du développement des nouvelles technologies de l'information. Une décennie plus tard, il a été estimé que le marché et le secteur privé ne pouvaient pas à eux seuls lutter efficacement contre les menaces, devenues de moins en moins faciles à anticiper et à analyser. C'est du moins ce qu'affirme un rapport publié en 1984 intitulé *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks* qui construit le lien entre certaines infrastructures et le concept de sécurité nationale (Collier et Lakoff 2008).

Nous allons à présent discuter de la protection des infrastructures critiques (CIP en anglais) comme concept pour penser la sécurité et comme pratique de la sécurité. S'il paraît que le nexus sécurité nationale et infrastructures critiques a pris de l'ampleur après le 11 septembre, il faut bien comprendre qu'il n'est pas né en 2001 en lien avec le terrorisme islamiste (Dunn Cavelty and Kristensen 2008). En réalité, c'est l'Administration Clinton qui a mis au point une stratégie de cybersécurité en formant une commission en 1996 (President's Commission on Critical Infrastructure Protection, ci-après désignée sous l'acronyme PCCIP) ayant pour but d'identifier les infrastructures vitales des États-Unis. L'année suivante, la PCCIP a publié un rapport identifiant huit grandes infrastructures : les télécommunications, la banque et le domaine financier, l'électricité, la distribution et le stockage de pétrole et de gaz, l'approvisionnement en eau, les transports, les services d'urgence et enfin les services gouvernementaux (Denning 2003, 26). Leur point commun, c'est le fait qu'elles soient critiques, vitales, c'est-à-dire que la prospérité économique, la puissance militaire et le pouvoir politique américain reposent sur ces

infrastructures et que leur dysfonctionnement engendrerait de grave conséquence pour la société (Cavelty et Kristensen 2008, Collier et Lakoff 2008).

Ces infrastructures sont pour la plupart gérées par le système SCADA (en français, système d'acquisition et de contrôle de données) reposant sur la gestion à distance des systèmes de protection. Ainsi, le système SCADA utilise le cyberespace pour opérer. Selon Dunn Cavelty et Brunner: « the overall capability of malicious actors to do harm is seen to be enhanced by inexpensive, ever more sophisticated, rapidly proliferating, and easy-to-use tools in cyberspace » (Dunn Cavelty et Brunner 2008, 7). Cependant, SCADA repose sur une complexe interdépendance de systèmes très sophistiqués qui sont beaucoup plus résilients que ce qu'il nous est laissé entendre. D'une part, les infrastructures critiques reposent sur des centaines de systèmes différents, plus ou moins connectés à Internet, nécessitant plus ou moins l'intervention humaine, ayant chacun leurs propres caractéristiques et vulnérabilités (Lewis 2002, Geers 2010). Des exercices et des cyber-attaques sont menés pour tester leur résistance et leur défense. En conséquence, il faut une très grande maîtrise technique pour pouvoir réaliser une attaque.

Comme nous allons le voir dans la prochaine sous-partie de ce chapitre, l'Administration Bush s'est saisie du thème de la cybersécurité afin de renforcer l'image d'un terrorisme apocalyptique et donc donner plus de légitimité à sa stratégie de contre-terrorisme. Mais nous voulons ici étudier la stratégie nationale pour sécuriser le cyberespace (NSSC) de 2003 afin de mettre en exergue la stabilité et la continuité du cadre défini par le PCCIP (Dunn Cavelty 2008a). Ainsi, en 2002, Bush annonce que les agences fédérales de cybersécurité vont être intégrées au département de sécurité nationale, faisant prospérer de fait le nexus cyberespace-sécurité nationale : « This *National Strategy to Secure Cyberspace* is part of an overall effort to protect the Nation. It is an implementing component of the *National Strategy for Homeland Security* and is

complemented by the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* » (National Strategy to Secure Cyberspace, 1). Dans ce document, l'Administration Bush reprend exactement les huit mêmes infrastructures critiques, auxquelles elle ajoute l'agriculture et les monuments nationaux (NSSC, 6). Cette stratégie établit dès l'introduction le lien entre cyberespace et infrastructures critiques : « Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security » (National Strategy to Secure Cyberspace, vii). Il est pertinent de notre la continuité dans le ton alarmiste employé et la volonté de sécurisation du cyberespace: « A similar tone is struck a year later in the so-far most authoritative and comprehensive statement of US cyber security policy » (Hansen et Nissenbaum 2009, 1161).

Par ailleurs, la stratégie américaine de cybersécurité s'opère autour de la protection des infrastructures et des grandes entreprises privées, car ce sont elles qui détiennent le savoir technique et qui sont responsables en grande partie de la stabilité du cyberespace. En effet, on estime qu'entre 85% et 95% des infrastructures sont détenues par le secteur privé (Dunn Cavelty 2012,123). C'est pourquoi on observe la volonté d'une collaboration croissante entre le public et le privé. Cela est exprimé dans la stratégie américaine comme suit: « Public-private engagement is a key component of our Strategy to secure cyberspace » (National Strategy to Secure Cyberspace, ix). À l'OTAN on peut l'observer notamment par l'engagement officiel de l'Assemblée Parlementaire de « promouvoir des partenariats plus étroits entre les pouvoirs publics, le secteur privé et les organisations de la société civile en vue d'assurer la sécurité des réseaux gouvernementaux et d'améliorer l'échange de savoir-faire en cas de violation du système de sécurité » (Résolution 387 sur la cybersécurité 2011, §9.c). Cela s'est concrètement traduit par la

mise en place d'un « cyberpartenariat OTAN – Industrie » (Healey et Jordan 2014). Toutefois, il semble que le secteur privé est mieux à même d'assurer la défense et de garantir la stabilité du cyberespace, notamment en termes de crédibilité et de capacités techniques : « There is a rejection here of government liability for private networks that is framed in the belief that the government has neither the authority nor the capability to deal with cyber security » (Carr 2016, 56). Dunn Cavelty notamment met en exergue le fait que ces partenariats marginalisent les acteurs privés dans le débat, car la militarisation du cyberespace concentre l'essentiel des efforts et des ressources. Le fait de mettre le concept de sécurité nationale au cœur du thème de la cybersécurité ne permet pas de trouver des solutions efficaces. La volonté de sécurisation du cyberespace se fait au détriment de solutions économiques et est, de ce fait, vouée à l'échec. En effet, ces partenariats donnent l'impression que les enjeux sont les mêmes pour les acteurs privés et les acteurs gouvernementaux, ou tout du moins que la finalité de la cybersécurité est la même. Dans la NSSC, on lit : « The federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector » (2003, ii). Or, il n'en est rien puisque les entreprises privées recherchent en premier lieu le gain financier et qui leur fait une bonne réputation (Carr 2016). Elles ont donc beaucoup à perdre d'une mauvaise cybersécurité. En conséquence, il est légitime de penser qu'elles fournissent des efforts supérieurs pour protéger leurs infrastructures et leurs réseaux, ou du moins prétendent le faire. En outre, ces partenariats privé-public participent au sentiment d'insécurité lié à la faisabilité des mesures de protection (Dunn Cavelty 2012, 104).

3. Le principe de précaution au cœur de la protection des infrastructures critiques

Nous l'avons vu, le cyber s'opérationnalise désormais à travers les infrastructures critiques, le

terrorisme, l'espionnage et la guerre : « cyber-crime was interlinked with foreign intrusion and espionage to elevate it to a national security issue. Then, the resulting threat "package" was linked to critical infrastructures and terrorism. In this way, the old idea of vital system security was firmly hoisted onto the security political agenda in a new form » (Dunn Cavelty 2008b, 55). La conséquence de cet assemblage de menaces et de risques a eu pour conséquence à l'OTAN la formation d'une gestion similaire à la gestion du risque terroriste et de protection des infrastructures critiques. C'est notamment dans le concept stratégique de 2010 que l'on peut observer le lien de filiation qui existe entre la gestion du risque cyber à l'OTAN et la sécurisation établie par les États-Unis au niveau des infrastructures critiques et du terrorisme (Hunker 2013). Le concept stratégique 2010 explique en effet que la gestion du risque cyber se décompose en 5 étapes : protection, prévention, détection, réponse, rétablissement (Healey et Jordan 2014). Dans le texte, on peut identifier la stratégie défensive :

> Nous continuerons de développer notre capacité à prévenir et à détecter les cyberattaques, à nous en défendre et à nous en relever, y compris en recourant à la planification OTAN pour renforcer et coordonner les capacités nationales de cyberdéfense, en plaçant tous les organismes de l'OTAN sous une protection centralisée et en intégrant mieux les fonctions de veille, d'alerte et de réponse de l'OTAN avec celles des pays membres » (Concept Stratégique 2010, §19).

Ce processus est exactement le même que celui décrit dans la NSSC de 2003. Ainsi, on peut lire : « The first priority focuses on improving our response to cyber incidents and reducing the potential damage from such events. The second, third, and fourth priorities aim to reduce threats from, and our vulnerabilities to, cyber attacks. The fifth priority is to prevent cyber attacks that could impact national security assets and to improve the international management of and response to such attacks » (National Strategy to Secure Cyberspace, x). De plus, il est intéressant de noter que l'OTAN s'appuie sur une gestion des risques préventive, de précaution que l'on peut notamment rapprocher à la gestion du risque terroriste que nous avons détaillé au chapitre précédent : « Risk

management has emphasized the rationality of prevention. » (Aradau et Van Munster 2011, 33). C'est notamment le rôle des « emergency planners » de scénariser le futur. Cette activité s'est institutionnalisée à l'OTAN comme aux Etats-Unis, avec la création d'une CERT américaine (Computer Emergency Response Team) et de son équivalent à l'OTAN, la NATO Computer Incident Response Capability (NCIRC) qui a été mise sur pied en 2008.

Le discours de cybersécurité concernant les infrastructures critiques a connu un essor particulier suite la révélation du virus Stuxnet en 2010, une cyber-arme conjointement conçue par les Etats-Unis et Israël pour attaquer le système SCADA de centrifugeuses d'enrichissement d'uranium en Iran dans le but de mettre à mal le développement du programme nucléaire iranien. La révélation de ce virus a eu plusieurs effets, surtout au niveau de la perception des risques et des scénarios à envisager par les « emergency planners ». Beaucoup d'experts ont eu peur d'une prolifération rapide de ce type de programme, mais Dunn Cavelty explique que ces craintes sont infondées dans la mesure où d'une part, même si le code a été récupéré, il faut avoir une très grande maitrise technique pour le modifier, et d'autre part, la fuite aura déjà été bouchée (« patched ») donc le code qui a été écrit pour cette faille précise ne fonctionnera pas deux fois (Dunn Cavelty 2012, Geers 2010, Hunker 2013).

Par ailleurs, Stuxnet a permis de recentrer le débat à propos des acteurs adversaires à prioriser sur les États-Nations. Sous l'ère Clinton, les figures du hacker et du cyber-terroriste étaient prépondérantes, car ces acteurs étaient considérés les plus qualifiés et les plus motivés pour attaquer les infrastructures critiques. Lorsque George W. Bush est arrivé au pouvoir, l'accent a été mis sur les pays étant souspçonnés de pouvoir mener des cyber-attaques de grande ampleur. Bien qu'après le 11 septembre le spectre du cyber-terrorisme ait été fort, les États-Nations sont restés les adversaires dans le cyberespace (Bendrath 2003). De son côté, l'OTAN privilégie également

les scénarios dans lesquels les adversaires sont des États-nations. L'Alliance dénonce d'ailleurs les actions menées par la Russie, notamment dans le cas de l'Estonie et des cyber-agressions vécues par la Géorgie en 2008, et la Chine (Rapport de Commission annuel 2009 - L'OTAN et la cyberdéfense, §8 et §13).

Comme nous allons le voir, le cyber-terrorisme reste un scénario possible et imaginé par l'OTAN. Bien que nous pensions que ce risque n'a que très peu de probabilités de réalisation, il est intéressant de s'y pencher afin de comprendre comment le cyber est sécurisé dans le discours. Dans cette perspective, nous voulons mettre l'emphase sur le rôle de l'imaginaire.

B) La gestion du risque cyber et la place de l'imaginaire : le cas du cyber-terrorisme

Après nous être intéressé à la sécurisation du cyberespace par l'OTAN en étudiant la doctrine des Etats-Unis, nous voulons désormais étudier le risque cyber-terroriste. Selon Hansen et Nissenbaum, le 11 septembre a renforcé l'attention portée aux problèmes de sécurité informatique (2009). En effet, l'administration Bush a quelque peu délaissé les travaux de son prédécesseur en matière de cybersécurité à son arrivée à la Maison Blanche avant de s'emparer du sujet dans le cadre de la lutte anti-terroriste (Dunn Cavelty 2008b). Le cyber a été intégré dans la redéfinition de la sécurité nationale telle que choisie par l'administration Bush. En ce sens, nous pouvons affirmer que le cyber a été sécurisée, au sens de Buzan *et al.* (1998), c'est-à-dire la problématisation sécuritaire d'un enjeu social (mais surtout technique, dans le cas du cyber). Notre démarche ici est de déconstruire le mythe du cyberterrorisme qui, bien qu'ayant été créé avant 2001, a pris toute son ampleur à la suite du 11 septembre. En effet, il est vu comme le point culminant de deux logiques (terroriste et cyber), ce qui le rend à la fois très absurde et très

effrayant. Le cyberterrorisme est une notion vague dont la définition est contestée : Doit-on privilégier l'intention de l'acte ? Ou bien les effets ? (Burton 2015). La définition adoptée par le Bureau de Sécurité de l'OTAN met davantage l'emphase sur les effets recherchés, à savoir des destructions suffisantes pour instaurer la terreur : « cyber attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal » (Everard 2008, 119). Par ailleurs, doit-il y avoir perte de vie pour qualifier une attaque de cyber-terrorisme ? Le scénario est envisagé par les États-Unis qui, dans la Stratégie nationale pour sécuriser le cyberespace (ci-après nommée SNSC), déclare : « Cyber attacks on United States information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life » (National Strategy to Secure Cyberspace 2002, ix). Le flou définitionnel que nous voulons mettre en évidence n'est pas anecdotique, car il participe grandement à faire pénétrer dans les imaginaires un phénomène qui ne s'est jamais produit jusqu'à aujourd'hui.

1. La place de l'imaginaire dans la gestion de risque

Les auteurs qui ont pensé le concept de risque s'accordent à dire que l'imagination joue un rôle central dans la gestion de risque (Coker 2002, Mythen 2004, Heng 2006, Furedi 2002). A cet égard, il convient d'intégrer à notre réflexion des travaux issus de la psychologie. Ces études sur le lien entre risque et cognition nous apprennent notamment que la perception du risque est intimement liée à l'intuition et aux émotions, et notamment la peur et l'anxiété. Tout d'abord, il convient de distinguer ces deux émotions. Il existe un consensus général, héritier de la logique freudienne, autour de cette distinction. La peur serait la réaction de la perception d'une menace immédiate et spécifique, alors que l'anxiété serait un sentiment plus général reposant sur l'anticipation du

danger, faisant par conséquent appel à l'imagination (Heng 2006, Ercolani 2012, Coker 2002). Selon Mythen, les deux font partie de la condition moderne (Mythen 2004, 96). Cependant, l'anxiété est davantage présente que la peur car, selon Beck, le risque est virtuel et réflexif. En ce sens, il ne prend vie que dans les imaginaires, contrairement à la menace qui est définie et provoque la peur (Williams 2009). Certains auteurs ont observé l'instauration d'une anxiété ambiante (« free-floating anxiety » Furedi 2002, Heng 2006), caractéristique de la société du risque, notamment à la suite des attentats du 11 septembre : « With mass-casualty terrorism, people are more anxious because they don't know what to be afraid of, with so many possible doomsday scenarios » (Heng 2006, 94).

La peur du terrorisme a été présente le 11 septembre et les jours suivants en réaction aux évènements. Mais l'anxiété a été construite et entretenue. Par exemple, Rasmussen (2006) dit que le risque d'attaque nucléaire sur Manhattan n'était pas plus élevé le 12 septembre 2001, mais la perception de ce risque était plus élevée car les attentats du 11 ont atteint les imaginaires. Dans le discours, c'est surtout par l'intertextualité qu'elle prend vie. Le risque, et surtout le risque cyber, est virtuel et il est difficile de le définir, de capter les imaginaires. A titre d'exemple, en invoquant Pearl Harbor ou le 11 septembre, le public peut se représenter visuellement les dégâts d'une attaque. Il n'est donc pas rare de lire ou d'entendre des expressions telles que « digital Pearl Harbor » (Lewis 2003, Desforges 2014, Hansen et Nissenbaum 2009). À première vue, la similitude entre le 7 décembre 1941 et le risque cyberterroriste n'est pas très convaincante. En revanche, la démarche argumentative et psychologique derrière cette comparaison a des effets non négligeables. En effet, elle permet aux décideurs politiques de sécuriser un domaine technique : « Securitizations always mobilize the specter of the future to some extent, but most nevertheless articulate the past as a legitimating reference that underscores the gravity of the situation. […]

Cyber securitizations on the other hand have no similar history of founding incidents to base themselves on but try to conjure historical analogies such as "electronic Pearl Harbors" » (Bendrath 2003, 50). Selon Conway, ces analogies permettent de créer le lien (imaginaire) entre les réseaux virtuels et les infrastructures critiques sous attaque terroriste, ce qui n'a que peu voire pas de réalité empirique (Conway 2008, 124). A ce jour, ni l'État islamique ni aucun groupe terroriste n'est parvenu à mener une cyber-attaque qui provoquerait la terreur ainsi que des dégâts matériels et/ou physiques (Dunn Cavelty 2008, Denning 2000). L'OTAN reconnaît que cela ne signifie pas pour autant que ces acteurs ne cherchent pas à développer leurs compétences de piratage informatique, bien au contraire (Everard 2008, 120). Cependant, les seules attaques conduites par des groupes terroristes furent des dénis de service ou des défacements, qui sont respectivement les versions cyber de protestations et de graffitis selon James Lewis du think tank *Center for Strategic and International Studies*. (Lewis 2002, 8). Il faut ici mettre l'emphase sur le fait que ce type de cyberattaques peut être menée pour différents motifs selon les acteurs qui en sont à l'origine. Cette idée est relayée par Green (2001) qui reste sceptique face au concept de cyberterrorisme car une cyberattaque ne permet pas à l'heure actuelle de causer de pertes humaines. En effet, selon Dunn Cavelty, la réalité des cyber attaques quotidienne relève davantage de la cybercriminalité (virus, vers informatiques, etc.); les attaques paralysantes restent des « chimères » (Dunn Cavelty 2009, 180). Le risque le plus probable dans les années à venir, selon les experts et selon l'OTAN, est la combinaison simultanée d'une attaque cybernétique et d'une attaque cinétique (Weimann 2009, Denning 2003, Everard 2008). C'est également un des risques pris en compte à l'OTAN, surtout depuis 2008 lorsqu'il a été possible d'observer dans le conflit opposant la Russie à la Géorgie que des cyberattaques pouvaient devenir un élément essentiel de la guerre conventionnelle (NATO 2017, « La Cyberdéfense »).

2. *La banalisation de l'anxiété par les gouvernements et les médias*

En étant décrit comme apocalyptique, ce risque est imaginé comme étant plus dangereux. Plus un risque est perçu ainsi, plus la demande de protection et l'attente de sécurité sera grande, au prix du sacrifice de sa propre liberté En effet, la projection d'un spectre de grand péril ne fait qu'augmenter le sentiment d'insécurité. Par voie de conséquence, les institutions de sécurité se rendent indispensables. En psychologie, la notion de risque mortel (« dread risk ») est utilisée pour décrire ce phénomène (Slovic 2002). Ce type de risque est donc complètement déconnecté de sa probabilité de réalisation (Furedi 2002, 6). Nous pensons que la plupart des risques cybernétiques se classent dans cette catégorie, notamment le cyberterrorisme qui le symbolise :

> Cyber risks, especially in their more extreme form, fit the risk profile of so-called "dread risks", which are perceived as catastrophic, fatal, unknown, and basically uncontrollable. There is a propensity to be disproportionally afraid of these risks despite their low probability, which translates into pressure for regulatory action of all sorts and the willingness to bear high costs of uncertain benefit (Dunn Cavelty 2012, 116).

Étudier le cyber-terrorisme permet de souligner la pertinence des travaux de Foucault à l'heure de l'âge de l'information. Ce discours apocalyptique représente la pierre angulaire d'un nouveau mode de gouvernement : «By promoting an imaginary of catastrophe as worst case scenario and by shifting the burden of proof, the *dispositif* of precautionary risk simultaneously grounds decisions in concrete representations of catastrophe and deprives them of accountability by pointing to the radical contingency and unknowability of these catastrophic visions » (Aradau et Van Munster 2008, 35). En d'autres termes, les notions d'urgence et d'incertitude liées aux risques cybernétiques permettent aux gouvernants d'agir sans résistance. Cela a permis à l'Administration Bush de mener à bien son agenda politique (Kempf 2014b). Sur le plan national, elle a pu octroyer des budgets exorbitants à la Défense : « The events of September 11 and the war on terrorism are

leading to new initiatives, funding, and legislation aimed at combating all forms of terrorism, including cyber-terrorism. These include establishment of a Department of Homeland Defense, which will bring together programs currently housed in other agencies » (Denning 2003, 44). Sur le plan international, le spectre de la catastrophe lui a permis d'imposer sa vision à ses alliés. A titre d'exemple, dès le 18 décembre 2001, le Secrétaire de la défense de l'époque Rumsfeld a essayé de convaincre les membres de l'OTAN d'intégrer à l'agenda politique le risque cyberterroriste (Bendrath 2003, 62).

On observe par ailleurs une banalisation de l'anxiété et une sorte de résignation des citoyens, une sorte d'acceptation de cet environnement (Grondin 2006). En outre, le caractère apocalyptique se trouve renforcé par l'addition de plusieurs risques, ce qui est le cas du cyberterrorisme, en tant que projection du risque terroriste et projection du risque cyber (Van Loon 2002) :

> In this threat representation, the fear of random and violent victimization in the case of terrorism and the distrust or outright fear of computer technology, which both capitalize on the fear of the unknown, are combined. The big problem with the use of the term "cyber-terrorism" in this discourse is that the term has become totally bereft of meaning by its frequent evocation in the media for attacks of any kind with the help of computers, which is exacerbated by similar use of the term by government officials (Dunn Cavelty 2009, 182).

La disproportion entre la probabilité de réalisation du risque cyberterroriste et l'anxiété ressentie en anticipation de ce risque nous amène à craindre des démesures (Dunn Cavelty 2008a).

Dans cette perspective, les auteurs s'intéressent au rôle que les médias ont dans le façonnement des perceptions. Les médias contribuent à créer une distorsion entre ce qu'il pourrait arriver rationnellement et ce qui est craint. D'une part, le rôle des images participe grandement à basculer dans un registre émotif plutôt que cérébral : « Once statistical and probabilistic knowledge faces the limit of the unexpected and the unknown, aesthetics become a technology that can give

free rein to the human sensorium for the governance of catastrophic events » (Aradau et van Munster 2011, 92). Elles empêchent en quelques sortes les raisonnements plus rationnels (Mythen 2004). A titre d'exemple, Furedi confronte les faits et les peurs : « Despite the fact that more Americans drowned in their bathtubs than were killed by terrorists, travelling to Europe seemed like a dangerous entreprise » (Furedi 2002, 51). D'autre part, bien que les médias ne soient pas à l'origine de la perception du risque, ils n'en restent pas moins des acteurs-clés dans la diffusion de l'anxiété et de la violence (Dunn Cavelty 2009, Furedi 2002, Holland 2013, Grondin 2006). Les médias contribuent à creuser l'assise de l'anxiété notamment en jouant la carte de la surestimation des menaces : la perception de ces dernière est fortement exagérée par les médias qui s'attardent sur des attaques sophistiquées très rares alors que la majorité des cyberattaques sont assez simples à réaliser et à contrer. Selon Dunn Cavelty, « in 2010, only about 3 per cent of all incidents were considered so sophisticated that they were impossible to stop » (Dunn Cavelty 2012, 117). De plus, ils se font l'écho, sans prendre de recul, d'estimations d'analystes qui sont très subjectives et dépendent beaucoup du degré de sécurité ou d'insécurité ressenti par la personne qui établit cette évaluation (Coker 2002, Slovic 2002).

3. Un risque qui s'ancre dans une méconnaissance du cyber

Enfin, nous souhaitons mettre l'emphase sur le fait que si la diffusion de ce type de discours est aussi bonne, c'est en partie dû à une mauvaise connaissance du cyberespace, de ses acteurs et de ses possibilités. Comme le soulève Mythen : « While risk consciousness may be in the ascendant, the composition and quality of public understandings of risk remains disputable » (Mythen 2004, 142). De la même façon que le terrorisme est mal compris, le cyber reste un domaine méconnu, ce qui donne lieu notamment aux réactions psychologiques que nous venons d'analyser (Slovic et

Weber 2002, 13). Ce manque de connaissances peut également expliquer l'usage de l'intertextualité que nous avons vu préalablement, c'est-à-dire l'usage d'analogies et la mobilisation d'autres référents pour expliquer un phénomène. Comme l'explique Christophe Wasinski à propos du discours de sécurité : « Plus encore, on pourra penser que le succès même de la mise sur agenda repose sur la capacité des acteurs politiques à faire usage de la justification technique » (Wasinski 2009, 16). Dès lors, il est possible de voir l'existence d'un fossé entre les justifications techniques données et le manque de connaissances du public. Ce manque de connaissances permet aux gouvernants de diffuser des discours anxiogènes. Bendrath explique que le 14 septembre 2001, l'organe gouvernemental américain en charge de la protection des infrastructures critiques, le National Infrastructure Protection Center, a publié une note destinée au grand public faisant état de la volonté d'acteurs politisés de mener des cyberattaques via des virus et des vers informatiques. En jouant sur l'ambiguïté sémantique, ce document de communication a participé à la promotion de l'anxiété et de la peur du cyberterrorisme : « For example, the old virus "life_stages.txt.shs" had been renamed "wtc.txt.vbs," alluding to the World Trade Center. This, of course, posed no real danger, especially not comparable to terrorism. But still, to people who are not IT security experts, the context in which this warning was issued made it look like a warning of cyber-terrorism » (Bendrath 2003, 60). Plus généralement, les discours à propos du risque cyber s'appuie sur la peur de l'inconnu que génère les technologies de l'information (Coker 2002). De plus, le cyber est un sujet complexe et abstrait, ce qui promeut un sentiment de méfiance à son égard (Dunn Cavelty 2008b, 52).

La peur du cyberterrorisme est surtout liée aux scenarios d'attaques sur les infrastructures critiques (notamment le système SCADA), mais elles sont beaucoup plus résilientes que ce que les médias et les décideurs veulent nous laisser penser :

> What Weimann calls "cyberterrorism angst" is greatly caused by fear related to vital systems such as power grids, water and drain infrastructures, most of them being regulated by the Supervisory Control and Data Acquisition (SCADA) system. The main concern about the SCADA system is its supposedly vulnerability, too often relayed by the media although no terrorist groups have ever tried to hack it (Green 2002)

Par ailleurs, il semble y avoir une confusion du grand public à propos des conséquences d'une cyberattaque. Il est nécessaire d'appréhender la nature variée des conséquences, notamment en termes de pertes économiques et financières, lesquelles sont généralement happées par le discours sur la sécurité nationale (Lewis 2002). En ce sens, la peur du cyberterrorisme, et plus généralement des cyberattaques, repose sur le fait que le cyber est transversal : il concerne l'économique, le social, le politique, mais également la vie privée et le quotidien. Selon Conway, le discours autrefois centré sur le hacker comme terroriste a basculé vers une perception de l'acteur terroriste en tant que hacker. Or, cela entrave la discussion autour du risque cyberterroriste (Dunn Cavelty 2008a), notamment parce que cela vient flouer les frontières entre les catégories d'actions définies au préalable. Par exemple, l'OTAN considère qu'une cyber-attaque relève soit de la cybercriminalité, soit du cyber-terrorisme ou bien est un acte de cyberguerre (L'OTAN et la cyberdéfense, §1). Dans la perspective du terroriste en tant que hacker, on peut donc se demander si un groupe terroriste qui pirate des cartes bancaires dans le cyberespace dans le but de se financer commet un acte de cybercriminalité ou de cyberterrorisme. L'OTAN reconnaît qu'il est bien souvent difficile de déterminer si une cyberattaque est d'origine criminelle ou terroriste (Everard 2008, 118). Il est donc important que les décideurs explicitent leurs conceptions de chaque attaque et de chaque acteur, notamment dans le cadre de coopération multilatérale.

En somme, nous avons voulu montrer que le risque de cyberterrorisme est une création discursive née de la peur du terrorisme au lendemain du 11 septembre et d'une anxiété latente liée

au cyberespace, laquelle se nourrit d'une méconnaissance publique du sujet. Nous avons voulu dépeindre le contexte dans lequel la menace cybernétique a été fortement sécurisée :

> The diffuse nature of the threat, coupled with a heightened sense of vulnerability, has brought about a growing militarization of cyber security. This has resulted in too much attention on the low probability of a large scale cyber attack, a focus on the wrong policy solutions, and a detrimental atmosphere of insecurity and tension in the international system. Though cyber operations will be a significant component of future conflicts, the role of the military in cyber will be limited and needs to be carefully defined (Dunn Cavelty 2012, 203).

Si ce mode de gouvernance est aussi efficace, c'est avant tout parce qu'il rapproche, met en parallèle et, à plus forte raison, entrelace deux logiques distinctes : le terrorisme et le cyber. En les associant, leurs effets paraissent démultipliés. Ainsi, nous avons pu mettre l'emphase sur la projection d'un risque apocalyptique dans les discours en tant qu'outil de gouvernance de l'Administration Bush, qui a été repris par l'OTAN. L'Alliance peut notamment justifier l'appropriation de la gestion de risque terroriste dans la construction et la gestion de risques cyber en établissant un lien entre ces risques. En effet, surtout au niveau programmatique, la question de l'incalculabilité est mise en avant. Les risques cyber sont construits comme étant susceptibles de toucher n'importe quelle infrastructure à n'importe quel moment, rendant la prévention difficile, des critères que l'on retrouve dans les stratégies anti-terroristes.

Nous allons à présent nous intéresser aux éléments de la doctrine de cyberdéfense de l'OTAN qui laisse voir une gestion dissuasive des risques cyber.

C) Mais la doctrine est également héritière de la dissuasion nucléaire

En 2010, un groupe d'experts, le « groupe Albright », a été chargé de faire des recommandations en vue de l'élaboration d'un nouveau concept stratégique. Dans son rapport, le groupe a notamment mis l'emphase sur la nécessité de protection des systèmes de communications et de commandement, mais également la mise en place d'une cyberdéfense venant soutenir la stratégie de dissuasion (Rapport de Commission annuel 2011 - Information et sécurité nationale, §44). Ce rapport, ainsi que d'autres travaux, nous renseignent sur le paradigme dissuasif qui semble sous-tendre la doctrine de cyberdéfense. A cet égard, nous voulons faire montre de la logique gouvernementale adoptée par l'OTAN en multipliant les organes et les agences de cyberdéfense. Nous nous appuierons ici sur le travail d'Olivier Kempf qui a tenté de dresser un portrait exhaustif de la dissuasion dans le cyberespace.

1. De la cyberdissuasion

Tout d'abord, il convient de noter que la sécurisation du cyber par l'OTAN a connu un nouveau retentissement l'année passée. En effet, il a été décidé au sommet de Varsovie que le cyber serait officiellement reconnu comme domaine opérationnel au même titre que les domaines aérien, terrestre et maritime. Il n'y a rien d'anecdotique à cette décision qui renforce la militarisation et l'appropriation du cyberespace dans les réflexions et les actions militaires menées à l'OTAN. Ce changement est d'autant plus significatif dans sa portée, car le cyberespace devient simultanément plus autonome et transcendant des autres domaines; en d'autres termes, il devient omniprésent (Kempf, Boyer). Comme le fait remarquer Dunn Cavelty, cette reconnaissance du cyberespace comme domaine opérationnel est le résultat d'analogies permanentes entre des concepts militaires familiers comme les « armes », la « défense » et leurs équivalents cybernétiques, caractérisés par

le préfixe « cyber », par exemple « cyberarmes », « cyberdéfense », etc. (Dunn Cavelty 2012, 119). Elle met en garde contre ce type de pratiques qui déconnectent les décideurs et les risques qu'ils tentent de gérer : « Again, this assumption clashes with the reality of the threat and the possibilities for countermeasures » (Dunn Cavelty 2012, 119). C'est dans cette perspective que nous voulons montrer comment l'OTAN a essayé de calquer sa stratégie historique de dissuasion à sa réflexion stratégique concernant le cyber.

La dissuasion est la doctrine historique de l'OTAN. De 1945 au début de la décennie 1990, l'Alliance transatlantique opère la sécurité autour de cette stratégie que Kempf, reprenant la définition du glossaire interarmées de terminologie opérationnelle, définit comme étant : « le fait de persuader un agresseur potentiel que les conséquences d'une action coercitive ou d'un conflit armé l'emporteraient sur les gains escomptés. Cela nécessite le maintien d'une puissance militaire et d'une stratégie crédible reposant sur une volonté politique nette d'agir » (Kempf 2015, 163). La dissuasion repose donc en grande partie sur la capacité de persuader son adversaire. Cependant, le calque entre la dissuasion classique et la dissuasion dans le cyberespace n'est pas idéal. La notion de réponse est teintée de l'action de riposte utilisée en dissuasion. Selon Kempf, la riposte dans le cyberespace est compliquée parce qu'elle nécessite un processus en plusieurs étapes : il s'agit d'abord de savoir que l'on est attaqué ce qui n'est pas toujours aisé, notamment dans le cas du cyberespionnage ; ensuite, il s'agit de faire le constat des dégâts, puis d'identifier l'agresseur. Mais comme nous l'avons mentionné au début de cette étude, il est très difficile d'attribuer une cyberattaque, c'est-à-dire de la relier à son agresseur. Il faut que tous ces critères soient réunis pour pouvoir élaborer et exécuter une réponse adéquate. En ce qui concerne la rhétorique, Kempf juge que « l'opacité du milieu cyber, la règle de l'inattribution, l'improbabilité d'une arme absolue rendent peu pertinente la notion de cyberdissuasion » (2015, 167). Il faut également noter que si

l'attaquant réussi à être identifié au terme de l'investigation, alors son adversaire en apprend beaucoup sur ses capacités techniques en matière de développement de cyberarmes.

Kempf conclut son chapitre en rappelant la non-pertinence du modèle de dissuasion nucléaire pour penser à la cyberdissuasion. L'OTAN ne peut ignorer les recommandations des rapporteurs qui partagent cet avis. Il a notamment été rapporté devant l'Assemblée Parlementaire de l'OTAN que : « La dissuasion, élément essentiel de la conception classique de la défense, ne fonctionne pas dans l'espace cybernétique. De plus, la plupart des cyberattaques sont réalisées par des groupes civils de hackers et il est donc pratiquement impossible de prouver l'implication d'un gouvernement » (Rapport de Commission annuel 2011 - Information et sécurité nationale, §32). Malgré l'impossible dissuasion dans le cyberespace, les documents officiels explicitent la volonté de l'OTAN d'arriver à dissuader. Outre le rapport Albright mentionné ci-dessus, on peut notamment déceler des indices de dissuasion dans certains éléments de communication de l'OTAN à propos de la stratégie de cyberdéfense. Ainsi, dans un communiqué, l'Agence OTAN d'information et de communications (NCIA) explique que le but de l'Alliance est d'acquérir une supériorité militaire dans le cyberespace grâce à plusieurs initiatives : « NATO's 360-degree functional approach ensures it maintains an edge in military technology over its adversaries through agile acquisition, early engagement and closer partnership with industry, enhanced interoperability, and by projecting resilience beyond NATO borders » (NCIA).

2. *Une logique gouvernementale : multiplication des agences*

Cependant, nous pensons que c'est dans une logique gouvernementale, qui se manifeste par la multiplication d'agences, que l'Alliance a choisi d'inscrire sa doctrine de cyberdéfense. On peut à première vue penser que ces créations institutionnelles ne relèvent pas de la dissuasion mais

représentent simplement les efforts multilatéraux de cyberdéfense (Burton 2015). Cependant, en s'intéressant aux documents doctrinaux et stratégiques officiels, il apparaît que les agences en charge de la cyberdéfense se développent à un rythme soutenu dans un objectif de dissuasion.

La politique de cyberdéfense de l'OTAN est supervisée au niveau politique par le Conseil de l'Atlantique Nord, qui est le principal organe de décision pour ce qui est de la gestion des crises liées à la cyberdéfense. Nous l'avons vu, c'est en 2002 avec la création de la NATO Computer Incident Response Capability (NCIRC), que l'OTAN a commencé à sécuriser le cyberespace. En charge de la surveillance et de la protection des réseaux de l'OTAN, son rôle central tient dans la coordination des activités de cyberdéfense de l'OTAN avec les États-membres. C'est surtout à partir de 2008 que l'on voit le développement massif des agences, à commencer par l'établissement du Bureau de gestion de la cyberdéfense (CDMB) en charge de la coordination des activités de cyberdéfense au sein de l'OTAN, notamment entre les agences civiles et militaires. L'objectif a été de centraliser les capacités opérationnelles de cyberdéfense. Pour ce faire, le CDMB repose sur une veille en temps réel permettant de détecter les menaces et de partager ces informations aux Alliés (Hughes 2009). Pourtant, l'émergence d'autres organes semblent compromettre cet effort de centralisation. Ainsi, sans rentrer dans les détails au risque de donner un effet catalogue, on peut observer que les responsabilités sont disséminées entre plusieurs agences, qu'elles soient préexistantes ou spécialement créées pour la cyberdéfense, pour un mandat consultatif ou opérationnel.

Nous interprétons cette volonté de monopoliser tous les aspects du cyberespace comme faisant partie d'une stratégie de dissuasion. De plus, en parallèle de ces agences opérationnelles, un important dispositif de formation, de recherche et d'entraînement a été développé. C'est notamment là que la doctrine et la stratégie de long-terme est pensée (Hughes 2009). Établi à

Tallinn en 2003, le CCD CoE (Cooperative Cyber Defence Centre of Excellence) est un centre de réflexion, notamment au niveau juridique, et d'exercice qui a été accrédité par l'OTAN en 2008. S'il n'a pas de vocation opérationnelle pour le moment, il est important, car il participe à l'élaboration de la stratégie à long-terme et conduit notamment des recherches sur la cyberguerre, ce qui laisse entrevoir la direction dans laquelle l'OTAN dit vouloir se diriger (Hunker 2013). Le Collège de la Défense de l'OTAN à Rome joue également un rôle important dans cette réflexion stratégique. Des centres d'entraînement et de formation en Italie, en Allemagne et au Portugal permettent à l'OTAN de développer les capacités de cyberdéfense de l'Alliance.

En somme, on se trouve dans la situation de gestion de risque où tout est fait pour donner l'impression d'une maitrise des vulnérabilités et d'une sécurité assurée. Cependant, il n'existe pas de bonne stratégie défensive militaire dans le cyberespace. Ainsi, en essayant d'adapter les modèles classiques de stratégie défensive au cyberespace, Kempf conclut qu'« il n'y a pas de stratégie absolue » (Kempf 2015, 152). En adaptant le modèle de défense préventive (ou périmétrique), qui consiste à défendre le front dans le but de sécuriser le reste du territoire, Kempf affirme qu'un dispositif de sécurité dans le cyberespace peut toujours être pénétré, et que le reste du système s'en trouve fragilisé. L'éventualité d'une « étanchéité absolue » n'est pas souhaitable car, d'une part, isoler un système est très contraignant et a pour conséquence de réduire les flux, et d'autre part, l'infiltration est toujours possible (c'est le cas du virus Stuxnet par exemple) (Kempf, 150-151). Pour ce qui est de la défense élastique, qui s'étend sur plusieurs couches dans l'optique « d'épuiser le choc de l'adversaire et conserver des possibilités de contre-attaques » (Kempf, 150), ce modèle n'a aucune pertinence dans le cyberespace, puisque l'ennemi ne perd pas ses forces, notamment logistiques, s'il gagne du terrain. Enfin, la défense en profondeur, qui suppose d'analyser les procédés offensifs de l'ennemi pour adapter sa propre défense, nécessite

une gestion de toutes les couches. Or, comme l'écrit Kempf, « tout système stratégique qui n'incorpore par la possibilité de son contournement et qui ne ménage pas les moyens de réagir à la surprise est erroné. [...] Dans le cyberespace, cela signifie que le système défensif retenu doit de plus intégrer cette fonction d'adaptation, qui est souvent omise : elle représente un surcoût apparent alors qu'elle est l'élément de sécurisation du système » (Kempf : 153). C'est pourquoi, selon Kempf, la résilience du système global est la clé pour rétablir une faille. Cependant, si la cyber-résilience semble idéale de prime abord, il ne faudrait pas qu'elle devienne une fin, un but à atteindre à tout prix. En effet, attacher beaucoup d'importance à la résilience, technique et politique, produit des conséquences. La plus néfaste d'entre elles est la dépolitisation, car elle entraîne une déresponsabilisation de la part des acteurs. Elle force les acteurs à atteindre l'objectif aux dépens d'une réflexion sur les actions menées. À l'OTAN, et notamment dans le cadre des partenariats entre l'Alliance et certains acteurs du secteur privé, nous sommes en droit de nous interroger au sujet de cette cyber-résilience qui semble être au cœur des projets communs. Il s'agira d'être vigilant sur le développement de ces collaborations, dont les participants se trouvent de moins en moins imputables et cherchent à se dédouaner de certaines responsabilités.

Conclusions

Nous avons voulu montrer dans ce chapitre que la construction de la doctrine de cyberdéfense de l'OTAN a, d'une part, été initiée suite à la stratégie de protection des infrastructures critiques élaborée à la fin des années 1990 aux États-Unis, et d'autre part, elle semble reprendre des éléments de sa doctrine historique de dissuasion.

Pour ce faire, nous avons identifié les deux éléments qui, selon Dunn Cavelty, participent à la sécurisation du cyberespace : d'une part, nous avons mis en exergue un *discours centré sur*

les infrastructures critiques comme objet référent, et d'autre part, nous avons vu une représentation de l'insécurité et des vulnérabilités de ces dernières à travers *le cas du cyberterrorisme* (Dunn Cavelty 2012, 105). Ainsi, *nous soutenons l'idée que le cyber a pu être sécurisé, parce qu'il a été relié au discours des infrastructures critiques et à la pratique de sécurité en résultant* (CIP). Dans ce cadre, nous avons montré que la stratégie de cyberdéfense de l'OTAN est héritière de cette sécurisation américaine. Comme l'ont identifié Aradau et van Munster : « Cyber security *is* successfully securitized as evidenced by such institutional developments as the establishment of the Commission on Critical Infrastructure Protection by President Clinton in 1996, the prominent location of cyber security within the Department of Homeland Security, President Bush's formulation of *The National Strategy to Secure Cyberspace* in 2003, and the creation of a NATO-backed cyber defense center in Estonia in 2008 » (Hansen et Nissenbaum 2009, 1157). Mais nous relevons déjà un problème, car ces infrastructures appartiennent en majorité à des acteurs du secteur privé. Or, protéger des infrastructures privées « as a military mandate is impossible, and conceiving of cyberspace as an occupation zone is an illusion. Militaries cannot defend the cyberspace of their country – it is not a space where troops and tanks can be deployed, because the logic of national boundaries does not apply » (Dunn Cavelty 2012, 121).

En outre, à travers les cas du virus Stuxnet, des cyber-attaques subies par l'Estonie en 2007 et du risque cyberterroriste, nous avons également voulu mettre en exergue le rôle de l'imagination et des émotions dans la gestion des risques et dans la sécurisation : « This fear has political consequences. First, on the national level, governments are currently releasing or updating cyber strategies and are setting up new organizational units for cyber defence. Second, internationally, increased attention is being devoted to the strategic-military aspects of the problem. » (Dunn Cavelty 2012, 114). Le risque étant virtuel et nécessitant une projection cognitive dans le futur,

nous avons voulu montrer comment l'imagination permet également aux décideurs, à travers différentes activités discursives, de sécuriser le cyber. En forçant la cybersécurité comme sujet politique majeur, différents groupes réussissent à imposer leurs agendas respectifs. Les consultants en cybersécurité et les compagnies de ce domaine sont pratiquement assurés de bénéficier financièrement du fait que le cyber soit intégré au cœur des enjeux de sécurité nationale (Bendrath 2003, Dunn Cavelty 2008). Plus généralement, tous les experts (académiques, experts ingénieurs, consultants), que Bigo nomme les « professionnels de l'insécurité », arrivent à convaincre le grand public de la nécessité de l'intervention des États dans la pratique de la cybersécurité, notamment en créant et en entretenant une anxiété à propos des risques cyber. Nous pensons que cela masque en réalité une grande incertitude qui règne au sein de cette communauté d'experts qui s'appuient sur des estimations et des probabilités qui sont présentées, dans les discours, comme des vérités : « Also, the type of knowledge that is empowered by risk registers is typically not actuarial or statistical in nature, but a type of expert-generated knowledge that is actively used to mask non-knowledge, and that is complicit in "feigning control over the uncontrollable" (Beck, 2002: 41) » (Hagmann et Dunn Cavelty 2012, 81).

Par ailleurs, ce chapitre révèle aussi la nécessité de repenser totalement les stratégies défensives dans le cyberespace, et non de tenter d'adapter les stratégies classiques qui ne sont valables que dans les sphères stratégiques de la terre, de la mer et de l'air. Dans cette perspective, nous avons tenté de montrer que les acteurs les mieux à même d'assurer la défense et de garantir la stabilité du cyberespace sont les acteurs privés et, à ce titre, la sécurisation massive du cyberespace par certains acteurs étatiques et multiétatiques peut représenter un frein à l'accomplissement de ces missions. À ce titre, nous pensons qu'une stratégie de cyber-résilience serait peut-être plus appropriée qu'une stratégie de cyberdéfense (Carr 2016, 62).

CONCLUSION GÉNÉRALE

Une des caractéristiques majeures du cyberespace, qui rend ce sujet si complexe à appréhender, est sa virtualité. Pour mener à bien cette recherche, nous avons solliciter les travaux du sociologue Ulrich Beck, grâce auxquels nous avons pu mettre l'emphase nécessaire sur la virtualité et l'incertitude à travers le concept de risque. L'idée de Beck que nous trouvons la plus pertinente et que nous avons cherchée à mettre en relief dans cette étude réside dans le fait que la société du risque et la gestion des risques amènent à plus d'incertitude et à une prolifération des risques. En effet, la gestion du risque repose sur la nécessité de prendre un risque pour en prévenir un. En somme, Beck permet de souligner, comme le font également les poststructuralistes du courant des études critiques du risques, la production d'insécurité : « Risk Society alerts us to the centrality of insecurity, risks and their management, the optimum means to pre-empt any adverse outcomes, and the tendency to imagine problems that may occur in the future » (Heng 2006, 33). De plus, Beck nous a notamment permis d'étudier la doctrine de cyberdéfense de l'OTAN par le spectre de la réflexivité ce qui nous permet d'affirmer que l'OTAN se construit désormais non plus en fonction de l'URSS, mais par rapport à elle-même, à ses propres angoisses et perceptions. Le risque est donc par essence virtuel et amène à donner une grande place au futur dans les réflexions politiques et militaires. Comme l'écrit Beck: « Risk means the *anticipation* of the catastrophe. Risk concern the possibility of future occurences and developments; they make present a state of the world that does not (yet) exist » (Beck 2009). Pour autant, nous avons été conscients des faiblesses des travaux de Beck qui s'appliquent davantage à des thématiques liées au changement climatique/thématiques environnementales par exemple. C'est pourquoi nous avons également sollicité les conceptualisations des poststructuralistes qui ont beaucoup réfléchit aux impacts du 11 septembre 2001. L'hybridité du cadre théorique se voulait être un mariage entre les tenants de

la gestion globale des risques (Beck et ses héritiers : Rasmussen, Coker, Heng, Williams) et ceux des études critiques de sécurité (Amoore et de Goede, Bigo, Ardau et van Munster, Grondin). Cette recherche a voulu comprendre comment les décideurs politiques se sont adapté à cette incertitude et quelles pratiques de gouvernement ont été développées pour gérer les risques cybernétiques.

Dans un premier temps, nous avons trouvé que les États-Unis, à la suite des attentats du 11 septembre 2001, ont développé une gestion du risque terroriste préemptive s'appuyant sur une « gouvernance algorithmique », c'est-à-dire que « ce sont les algorithmes qui créent les conditions de possibilités de la préemption et dont la finalité est de calculer l'improbable, de rendre opérationnel ce qui tient du domaine de l'aléatoire et de gouverner l'incertain » (Grondin 2016, 181?). Ce concept nous permet de souligner que la gestion du risque terroriste donne lieu à une augmentation du soupçon, de la surveillance et surtout de l'insécurité. Ces politiques anti-terroristes se sont appuyées sur le risque d'attentat pour mettre en place un état d'exception et l'instauration d'une « culture de l'apocalypse » (Van Loon 2002) reposant en premier lieu sur une anxiété générale et une peur du terrorisme. Nous avons voulu montrer que la véritable gestion des risques s'opère dans les imaginaires. Nous avons également trouvé que depuis la fin des années 1990, les États-Unis ont développé une gestion sécuritaire par la protection des infrastructures critiques. Nous avons pu mettre en avant la contribution des États-Unis, tant sur le plan technique que sur le plan idéel, notamment avec les efforts de l'administration Clinton. Nous pouvons affirmer qu'il existe une réelle influence des États-Unis au sein de l'OTAN au niveau idéologique et stratégique car nous avons également trouvé que dans une certaine mesure, l'OTAN a repris cette façon de sécuriser le cyberespace. Dunn Cavelty explique à ce sujet que : « Most countries simply follow the threat perception and reasoning of the US, even though the strategic context and disparity in power positions warrant a different threat assessment » (2012, 115).

Les risques cyber étant techniques et mal connus du grand public, la perception de ces risques est aggravée. Nous avons vu à travers le cas du cyberterrorisme que ce risque est volontairement surestimé et nous avons cherché à montrer que la peur du cyberterrorisme est infondée. Elle est dangereuse car dans l'imaginaire, elle combine la peur d'une cyberattaque sur les infrastructures critiques et d'une attaque terroriste. En réalité, la faisabilité technique d'un tellement type d'attaque est très compliqué et hautement improbable et donc l'anxiété créée par les discours sur les risques contemporains est infondée : « What the events of 11 September 2001 show is that our culture encourages us to fear the wrong things. It is not Frankenstein food, stem-cell research, mobile phones or new technologies that threaten the world. These achievements of science and ingenuity represent the constructive side of humanity. What happened on 11 September represents the destructive side of human passions. In many ways this was an old-fashioned act of terror, executed with low-tech facilities by a small number of zealots driven by unrestrained hatred. However, our obsessions with so-called theoretical risks actually distracts society from dealing with those old-fashioned dangers that have always threatened our lives » (Furedi 2002, xvii). Nous avons voulu montrer à travers le cas du cyberterrorisme comment les décideurs américains sont arrivés à construire et véhiculer le spectre d'un risque apocalyptique dont la probabilité de réalisation est extrêmement faible (Furedi 2002, Mythen 2004, Salter 2008, Coker 2002). En ce sens, le 11 septembre a renforcé la perception du risque et du « besoin » de sécuriser davantage les infrastructures critiques.

Enfin, nous avons défendu l'idée que si la doctrine de cyberdéfense de l'OTAN est très largement inspirée des efforts américains pour sécuriser le cyberespace : il est possible de voir des traces d'une gestion dissuasive des risques cyber. Nous avons pu voir que le risque est devenu le concept central des stratégies de sécurité de l'Occident après la guerre froide, notamment en

montrant que les menaces sont devenues plus floues, plus difficiles à définir, moins localisables. Cela est d'autant plus vrai dans le cas du cyber à cause du principe de non-attribution qui caractérise le cyberespace. Cette recherche a notamment mis l'emphase sur la multiplication exponentielle des agences otaniennes en charge, de près ou de loin, à la cyberdéfense. De plus, nous avons vu que l'OTAN ne cherche pas seulement à gagner une place prépondérante en matière de capacités techniques et humaines de défense, mais également en termes de recherche pour penser la stratégie à long-terme, sur les aspects techniques mais aussi légaux. A titre d'exemple, un groupe d'experts du centre d'excellence de cyberdéfense coopérative de l'OTAN a publié le « National Cyber Security Framework Manual » qui tente de poser les bases d'un encadrement juridique pour le cyberespace.

Somme toute, en s'intéressant à la construction de la doctrine de cyberdéfense de l'OTAN, nous sommes parvenus à mettre en relief la déconnexion qui existe entre le discours politico-militaire et la faisabilité technique de cyberattaques ainsi que la gravité de leurs conséquences. Cependant, nous reconnaissons la faiblesse empirique de cette recherche. Nous sommes conscients qu'une grande partie des documents concernant la cyberdéfense de l'OTAN est classifiée. Une des solutions pour remédier à ce problème aurait été de conduire des entretiens auprès de personnes œuvrant à la cyber défense à l'OTAN. Une autre piste de recherche pourrait être de mener une étude comparative poussée sur les différentes conceptions nationales de la cybersécurité des Etats-membres dans le but de mieux comprendre la coopération multilatérale à l'OTAN. En outre, des voix s'élèvent pour remettre en question le bien-fondé de la gestion de ces risques par l'OTAN. Certains auteurs comme Kempf (2014) avancent l'idée que la nature des menaces cybernétiques ne permet pas aux institutions bureaucratiques de lutter de façon efficace et que des alliances de circonstance, plus informelles et moins rigides, seraient plus à même d'être efficace dans la

coopération. En ce qui concerne le cyberespace, l'OTAN n'a peut-être pas sa place dans sa régulation et cela fait naître des doutes quant à la pertinence de l'organisation dans le futur. En définitive, nous soutenons l'idée que : « "Cyber security" can, in short, be seen as "computer security" plus "securitization" » (Hansen et Nissenbaum 2009, 1160). Cette recherche trouve que la volonté de l'OTAN d'anticiper les risques pour s'en protéger amène à plus d'insécurité; nous soutenons ce faisant que nous vivons dans une époque où les menaces sont faibles, mais les vulnérabilités grandes, car la construction des risques s'opère de façon réflexive.

BIBLIOGRAPHIE

Abrial, Stéphane. (2010). Le contexte stratégique de l'OTAN à l'horizon 2030. *Revue internationale et stratégique*, *4*, 67-73.

Amoore, Louise et de Goede, Marieke. (2005). Governance, risk and dataveillance in the war on terror. *Crime, law and social change*, *43*(2), 149-173.

Amoore, Louise et de Goede, Marieke. (2008). Introduction : Governing by risk in the war on terror. Dans Louise Amoore et Marieke de Goede (dir.), *Risk and the War on Terror* (p. 5-20). Londres and New York: Routledge.

Aradau, Claudia et van Munster, Rens. (2008). Taming the Future : the dispositif of risk in the war on terror. Dans Louise Amoore et Marieke de Goede (dir.), *Risk and the War on Terror* (p. 23-40). Londres et New York: Routledge.

Beck, Ulrich. (2000). Risk Society Revisited: Theory, Politics and Research Programmes. Dans Barbara Adam, Ulrich Beck et Joost Van Loon (dir.), *The risk society and beyond: critical issues for social theory* (p. 211-229). Londres : Sage.

Beck, Ulrich. (2002). The terrorist threat: world risk society revisited. *Theory, culture & society*, *19*(4), 39-55. Londres : Sage.

Beck, Ulrich. (2009). *World Risk Society*. Cambridge : Polity.

Benchérif, Adib. (2015). L'Analyse du Risque Géopolitique: du Plausible au Probable, *Glocalism, 3*, 1-16.

Bendrath, Ralf. (2003). The American cyber-angst and the real world–any link. Dans Robert Latham (dir.), *Bombs and bandwidth: the emerging relationship between information technology and security* (p. 49-73). New York : The New Press.

Bigo, Didier. (1997). La recherche proactive et la gestion du risque. *Déviance et société*, *21*(4), 423-429.

Bigo, Didier. (2005). La mondialisation de l'(in)sécurité?, *Cultures & Conflits*, *58*(2), 53-101.

Bigo, Didier. (2011). Pierre Bourdieu and international relations: Power of practices, practices of power. *International Political Sociology*, *5*(3), 225-258.

Brunner, Elgin M. (2008). The Gendered Narratives of Homeland Security. Anarchy at the Front Door Makes Home a Haven. Dans Myriam Dunn Cavelty et Kristian Soby Kristensen (dir.), *Securing 'the Homeland'. Critical infrastructure, risk and (in)security* (p. 153-175). Londres et New York: Routledge.

Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, *Defence Studies, 15*(4), 297-319.

Carr, Madeline. (2016). Public-private partnerships in national cyber-security strategies, *International Affairs*, *92*(1), 43-62.

Collier, Stephen J. et Lakoff, Andrew. (2008). The vulnerability of vital systems: How 'critical infrastructure' became a security problem. Dans Myriam Dunn Cavelty et Kristian Søby Kristensen (dir.), *Securing 'the Homeland'. Critical infrastructure, risk and (in)security* (p. 40-62). Londres et New York: Routledge.

Conway, Maura. (2008). Media, fear and the hyperreal: the construction of cyberterrorism as the ultimate threat to critical infrastructures. Dans Myriam Dunn Cavelty et Kristian Søby Kristensen (dir.), *Securing 'the Homeland'. Critical infrastructure, risk and (in)security.* Londres et New York: Routledge.

Coutin, Susan B. (2008). Subverting Discourses of Risk in the War on Terror. Dans Louise Amoore et Marieke de Goede (dir.), *Risk and the War on Terror* (p. 218-232). Londres et New York: Routledge.

Coker, Christopher. (2002) Globalisation and Insecurity in the Twenty-first Century: NATO and the Management of Risk. *The Adelphi Papers*, *42*(345), 1-103.

Coker, Christopher. (2013). *War in an Age of Risk*. Cambridge: Polity Press.

Deibert, Ronald J. et Rohozinski, Rafal. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15-32.

Denning, Dorothy E. (2003). Cyber-security as an Emergent Infrastructure. Dans Robert Latham (dir.), *Bombs and bandwidth: the emerging relationship between information technology and security* (p. 25-48). New York : The New Press.

Doucet, Marc G. et de Larrinaga, Miguel. (2010). Introduction: the Global Governmentalization of Security and the Securitization of Global Governance. Dans Marc G. Doucet et Miguel de Larrinaga (dir.), *Security and Global Governmentality: Globalization, Governance and the State* (p. 1-20). Londres : Routledge

Dunn Cavelty, Myriam. (2007). Is Anything Ever New? Exploring the Specificities of Security and Governance in the Information Age. Dans Myriam Dunn Cavelty, Victor Mauer et Sai Felicia Krishna-Hensel (dir.), *Power and Security in the Information Age. Investigating the Role of the State in Cyberspace* (p. 19-44). Farham: Ashgate.

Dunn Cavelty, Myriam. (2008). Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*, *4*(1), 19-36.

Dunn Cavelty, Myriam. (2008b). Like a phoenix from the ashes. The reinvention of critical infrastructure protection as distributed security. Dans Myriam Dunn Cavelty et Kristian Søby Kristensen (dir.), *Securing 'the Homeland'. Critical infrastructure, risk and (in)security.* Londres et New York: Routledge.

Dunn Cavelty, Myriam. (2012). The militarisation of cyber security as a source of global tension. Dans Daniel Möckli (dir.), *Strategic Trends 2012*, Center for Security Studies, ETH Zurich, 103-124.

Dunn Cavelty, Myriam. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, *20*(3), 701-715.

Dunn Cavelty, Myriam et Brunner, Elgin M. (2007). Introduction: Information, Power, and Security–An Outline of Debates and Implications. In Myriam Dunn Cavelty, Victor Mauer et Sai Felicia Krishna-Hensel (dir.), *Power and Security in the Information Age. Investigating the Role of the State in Cyberspace,* (p. 1-18). Farham: Ashgate.

Dunn Cavelty, Myriam, & Mauer Victor. (2007). The Role of the State in Securing the Information Age–Challenges and Prospects. In *Power and Security in the Information Age. Investigating the Role of the State in Cyberspace,* Dunn Cavelty, Myriam, Mauer Victor, & Krishna-Hensel Sai Felicia (Eds.), Ashgate, 151-162

Dunn Cavelty, Myriam et Søby Kristensen, Kristian. (2008). Introduction: securing the homeland: critical infrastructure, risk, and (in)security. Dans Myriam Dunn Cavelty et Kristian Søby Kristensen (dir.), *Securing 'the Homeland'. Critical infrastructure, risk and (in)security.* Londres et New York: Routledge

Dunn Cavelty, Myriam, Kaufmann, M. et Søby Kristensen, Kristian. (2015). Resilience and (in) security: Practices, subjects, temporalities. *Security Dialogue*, *46*(1), 3-14.

Ercolani, Giovanni (2012). NATO, Discourse, Community and Energy Security. *Central European Journal of International and Security Studies*, *6*(1), 103-131.

Ericson, Richard V. (2008). The State of Preemption: managing terrorism through counter law, Dans Louise Amoore et Marieke de Goede (dir.), *Risk and the War on Terror* (p. 57-76). Londres et New York: Routledge.

Furedi, Frank. (2002). *Culture of Fear. Risk-taking and the Morality of Low Expectation.* Revised Edition. Londres : Continuum.

Geers, Kenneth. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, 298-303.

Giddens, Anthony. (1994). *Les conséquences de la modernité*. Paris : L'Harmattan.

Grondin, David. (2005). Une lecture critique du discours néoconservateur du nouvel impérialisme: La lutte globale contre le terrorisme comme Pax Americana. *Études internationales*, *36*(4), 469-500.

Grondin, David. (2006). La cartographie "impériale"/néolibérale états-unienne dans la guerre idéologique contre la terreur : décodification de la production et de la planification stratégiques des États-Unis d'Amérique. *Études internationales*, *37*(1), 35-56.

Grondin, David. (2010). The new frontiers of the national security state. Dans Marc G. Doucet et Miguel de Larrinaga (dir.), *Security and Global Governmentality: Globalization, Governance and the State* (p. 79-95). Londres : Routledge.

Grondin, David. (2013). The Study of Drones as Objects of Security: Targeted Killing as Military Strategy. Dans Mark B. Salter et Can E. Mutlu (dir.), *Research Methods in Critical Security Studies*. Londres : Routedge.

Grondin, David. (2016). Mobilité, vie algorithmique et société de surveillance dans Person of Interest : la traque du national security state cyberspatial. Dans Isabelle Lacroix et Karine Prémont (dir.), *D'Asimov à Star Wars : représentations des rapports de force dans la science-fiction*. Québec : Presses de l'Université du Québec.

Hagmann, Jonas et Dunn Cavelty, Myriam. (2012). National risk registers: Security scientism and the propagation of permanent insecurity. *Security Dialogue*, *43*(1), 79-96.

Hansen, Lene. (2013). *Security as practice: discourse analysis and the Bosnian war*. Londres : Routledge.

Hansen, Lene et Nissenbaum, Helen. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175.

Healey, Jason et Jordan, Klara Tothova. (2014). NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. Washington DC: Atlantic Council of the United States.

Heng, Yee-Kuang. (2006). *War as risk management: strategy and conflict in an age of globalised risks*. Londres: Routledge.

Herd, Graeme P. et Kriendler, J. (dir.). (2013). *Understanding NATO in the 21st century: Alliance strategies, security and global governance*. Londres: Routledge.

Holland, Jack. (2013). *Selling the war on terror: Foreign policy discourses after 9/11*. Routledge.

Hughes, Rex B. (2009). NATO and Cyber Defence: Mission Accomplished?, *Atlantisch Perspectief*, (1)4.

Irondelle, Bastien, & Lachmann, Niels. (2011). L'OTAN est-elle encore l'OTAN?. *Critique internationale*, *4*, 67-81.

Kempf, Olivier. (2014). *Alliances et mésalliances dans le Cyberespace*. Paris : Economica.

Kempf, Olivier. (2014b). Le cyberterrorisme: un discours plus qu'une réalité. *Hérodote*, (1), 82-97.

Kempf, Olivier. (2010). *L'OTAN au XXIème siècle.* Perpignan : Artège.

Kristensen, Kristian Søby. (2008). The absolute protection of our citizens: Critical infrastructure protection and the practice of security. Dans Myriam Dunn Cavelty et Kristian Soby Kristensen

(dir.), *Securing 'the Homeland'. Critical infrastructure, risk and (in)security,* (p. 63-83*)*. London and New York: Routledge.

Luhmann, Niklas (2005). *Risk: A Sociological Theory*. Piscataway: Transaction Publishers.

Lupton, Deborah. (2013). *Risk*. Second Edition. Londres: Routledge.

Mythen, Gabe. (2004). *Ulrich Beck: A Critical Introduction to the Risk Society*. Chicago: Pluto Press.

Mythen, Gabe, & Walklate, Sandra. (2016). Not knowing, emancipatory catastrophism and metamorphosis: Embracing the spirit of Ulrich Beck. *Security Dialogue*, *47*(5), 403-419.

Nau, Henry R. (2008). Iraq and previous transatlantic crises: Divided by threat, not institutions or values. Dans Jeffery J. Anderson, John G. Ikenberry et Thomas Risse (dir.), *The End of the West?: Crisis and change in the Atlantic order*, (p. 82-111). Cornell University Press.

Petersen, Karen L. (2012). Risk analysis–A field within security studies?. *European Journal of International Relations*, *18*(4), 693-717.

Petersson, Magnus. (2013). Just an Internal Exercise? NATO and the 'New'Security Challenges. Dans Ellen Hallams, Luca Ratti et Benjamin Zyla (dir.), *NATO Beyond 9/11: The Transformation of the Atlantic Alliance*, (p. 140-154). Londres et New York: Palgrave MacMillan.

Pomarède, Julien. (2014). L'(in)sécurisation par les technologies militaires et la mise en sens de la violence. *Cultures & Conflits*, *93*, 125-145.

Rasmussen, Mikkel V. (2001). Reflexive security: NATO and international risk society. *Millennium*, *30*(2), 285-309.

Rasmussen, Mikkel V. (2006). The risk society at war. *Terror, Technology and Strategy in the Twenty-First*. Cambridge: Cambridge University Press.

Salter, Mark B. (2008). Conclusion: Risk and Immigration in the War on Terror. Dans Louise Amoore et Marieke de Goede (dir.), *Risk and the War on Terror* (p. 233-246). London and New York: Routledge.

Scott, Alan. (2000). Risk society or angst society? Two views of risk, consciousness and community. Dans Barbara Adam, Ulrich Beck et Joost Van Loon (dir.), *The risk society and beyond: critical issues for social theory* (p. 33-46). London: Sage.

Shackelford, Scott J. (2010). Estonia Three Years Later: A progress Report on Combatting Cyber Attacks, *Journal of Internet Law*.

Shea, Jamie. (2015). NATO: the challenges ahead. *Global Affairs*, *1*(2), 121-128.

Van Loon, Joost. (2000). Virtual risks in an age of cybernetic reproduction. Dans Barbara Adam, Ulrich Beck et Joost Van Loon (dir.), *The risk society and beyond: critical issues for social theory* (p. 165-182). London: Sage.

Van Loon, Joost. (2002). *Risk and technological culture: Towards a sociology of virulence*. Londres: Routledge.

Williams, Michael J. (2008). *NATO, security and risk management: from Kosovo to Kandahar*. Londres: Routledge.

Williams, Michael J. (2008). (In) Security studies, reflexive modernization and the risk society. *Cooperation and Conflict*, *43*(1), 57-79.

Williams, Michael C. (2007). *Culture and security: symbolic power and the politics of international security*. Londres et New York: Routledge.