L'hégémonie coopérative et le cyberespace: le défi de la coopération multilatérale[1]

Hugo Loiseau, Ph.D.
École de politique appliquée
Université de Sherbrooke
Hugo.Loiseau@USherbrooke.ca
&
Lina Lemay, B.A.
École de politique appliquée
Université de Sherbrooke
Lina.Lemay@USherbrooke.ca

Communication préparée pour
le Congrès annuel 2009 de
l'Association canadienne de science politique
à Carleton University
Ottawa, les 27, 28 et 29 mai 2009
(Version préliminaire, ne pas citer)

[1]Les auteurs désirent remercier le Fonds québécois de recherche sur la société et la culture (FQRSC) pour son généreux soutien financier.

Résumé

L'hégémonie coopérative et le cyberespace: le défi de la coopération multilatérale

Le présent document est fondé sur l'hypothèse que le développement du cyberespace, tout comme le processus d'intégration régionale, a pris une importance croissante dans nos sociétés. En tant que tel, ce document analyse le rôle des États-Unis et de l'Union européenne dans la formulation et la mise en œuvre d'une politique régionale de cybersécurité respectivement dans les Amériques et en Europe. L'objectif principal de cette étude vise à préciser les liens entre la nature des institutions régionales et les possibilités de développement d'une politique régionale en matière de cybersécurité. Le deuxième objectif consiste à participer aux des débats théoriques des relations internationales en ce qui concerne le rôle joué par les processus d'intégration régionale dans la sécurisation du cyberespace. Enfin, le troisième objectif est de comprendre le rôle d'un hégémon (ou l'absence de celui-ci) dans le développement et la mise en œuvre d'une politique régionale de la cybersécurité. Nous souhaitons, à travers l'étude de cas de cette communication, de vérifier les promesses de la théorie de l'hégémonie coopérative développée par Pedersen (Pedersen, 1998 et 2002; Mace et Loiseau, 2005).

Introduction

Les États et les sociétés occidentales deviennent de plus en plus dépendants des nouvelles technologies de l'information et plus particulièrement du réseau Internet (OCDE 2003). Ce constat se perçoit notamment à la lumière des vulnérabilités sociales et étatiques qu'il est possible d'énumérer : cybercriminalité, protection des infrastructures critiques et des données personnelles... (Libicki 2007) Les écrits scientifiques reflètent d'ailleurs cet état de fait. En dépit de la pertinence de ces écrits, une question demeure pourtant : quelles sont les conséquences de cette dépendance? D'un côté, les cyberoptimistes proposent une vision positive où les technologies favoriseraient l'épanouissement de l'humanité. De l'autre, les cyberpessimistes dénoncent la désagrégation du lien social et les dangers qu'engendreraient les nouvelles technologies (Hanson 2008). Le débat entre ces deux écoles de pensée a permis de dégager les nombreux enjeux que soulève le problème.

Toutefois, ces deux écoles de pensée n'ont pas ou ont très peu abordé la question sous l'angle des relations internationales et plus particulièrement celle de l'intégration régionale. Plus précisément, la nature même de la menace et du risque encouru, c'est-à-dire une origine provenant du cyberespace, espace qui ne connaît pas les frontières nationales, supposerait une approche multilatérale. En effet, en termes de sécurité, les menaces en provenance du cyberespace dépassent les cadres strictes de la sécurité nationale *stricto sensu*. De prime abord, on pourrait penser que cet état de fait favoriserait la coopération internationale et régionale en la matière. En toute logique, ces nouveaux enjeux transfrontaliers interpellent les États à agir de façon collective afin de réguler le cyberespace.

Bien entendu, un État, seul, ne peut affronter les menaces en provenance du cyberespace. De plus, à première vue, on peut supposer qu'un regroupement d'États, dans une institution régionale à caractère politique ou sécuritaire par exemple, seraient enclins à se doter d'une stratégie commune en matière de cybersécurité. La question se pose puisqu'il faut déterminer si les intérêts convergents des membres de ce regroupement dépassent la somme des intérêts nationaux spécifiques à chacun.

À cet égard, le concept d'hégémonie coopérative développé par Pedersen (1998 et 2002) et repris par Mace et Loiseau (2005) pour les Amériques semble une avenue intéressante pour l'analyse de la coopération multilatérale en matière de cybersécurité. Essentiellement, ce concept propose un schéma explicatif présentant les avantages majeurs des grandes puissances dans leur participation à un processus d'intégration régionale.

Le problème de recherche

La recherche proposée s'inscrit dans le programme de recherche sur le régionalisme. Si le rôle et les conséquences du régionalisme sont parfois minimisés par les écoles réaliste et néoréaliste (Mearsheimer, 1994-1995), la multiplication des processus d'intégration régionale depuis la fin des années 1980 et leur existence dans chacune des régions du monde (Checkel, 2005) consacrent l'importance du sujet dans l'étude du système international actuel. Parce qu'elle s'intéresse aux impacts des normes internationales sur la politique intérieure des États (Cortell et Davis, 2000 et Thomas, 2001), aux effets de l'intersubjectivité existants dans les relations internationales sur l'identité des acteurs du système international (Klotz et Lynch, 1999) et aux résultantes qu'entraînent les processus de légalisation et d'institutionnalisation de l'espace international sur les acteurs (Goldstein, 2000 et Keohane, 2001), l'étude du régionalisme stimule la réflexion tant dans les milieux universitaires que dans les sphères gouvernementales ou dans les organisations internationales.

Bien entendu, la théorie de la stabilité hégémonique sert de toile de fond pour cette recherche. Cette théorie indique simplement qu'une puissance hégémonique est nécessaire à la mise en place et au maintien d'un régime ou d'une institution multilatérale dans un domaine spécifique de gouvernance internationale.

Tout comme l'intégration régionale qui enclenche un processus de formation d'un nouvel espace (Ténier, 2003) renouvelant l'analyse traditionnelle des structures internationales, l'apparition du cyberespace engendre un repositionnement quant à la définition classique des concepts de sécurité et de défense. Cependant, les gouvernements et les organisations internationales ont pris du retard en termes de législation et de contrôle face à ce développement, même si de grands secteurs de la société – économique, industriel, militaire – ont créé de puissants liens de

dépendance envers le cyberespace (Wautelet, 1998). Ce décalage des institutions à ce sujet se reflète également dans la littérature scientifique sur le cyberespace et la cybersécurité, rapidement obsolète face aux progrès rapides de l'industrie des hautes technologies (Dupuy, 2002).

Les écrits sur le cyberespace sont de diverse nature. Ils proposent en général plusieurs points de vue. En ce qui concerne la cybersécurité ou plus simplement dit la sécurisation du cyberespace par les États et les organisations internationales, les avis divergent. Pour Fleury, dans la sphère des communications, Internet aurait entraîné des transformations dans les relations et les échanges à tous les niveaux, mais aussi dans nos perceptions. De ce fait, malgré une certaine forme de libéralisme qui a cours sur la toile, Internet n'échapperait pas au pouvoir et à la réglementation. Dans ce contexte, l'auteur cherche à comprendre comment les autorités dominantes exercent leur pouvoir (2008 : 84-85).

Selon Fleury, une partie de la réponse résiderait dans le processus de transition vers une économie de l'information. Celle-ci serait désormais décentralisée et hors-marché. Ce statut aurait émergé de deux principaux changements, soient le développement progressif d'une économie de production de l'information et de la culture, puis du développement des techniques de communication efficaces et abordables. Cette nouvelle réalité aurait pour effet d'accroître les échanges et ainsi, les opportunités de « réseautage ». Ceci laisse émerger un nouveau type de citoyen, soit « transnational ». Or, le développement de cette économie étant limité (accessibilité, moyens techniques et financiers), l'exclusion demeure. Cette inégalité favoriserait ainsi le maintien de l'hégémon. (2008 : 85). D'après l'auteur, il importe de porter une attention particulière aux diverses institutions actuelles en matière de gouvernance d'Internet, car celles-ci auraient un rôle crucial dans le développement des normes et auraient une influence sur les utilisateurs. Or, il importe également d'élargir le regard vers « les forces sociales aux intérêts conflictuelles » ainsi qu'aux idées véhiculées par ces mêmes forces, en constant mouvement.

L'influence s'exercerait à partir de normes nationales et internationales. Cependant, il importe de préciser que la gouverne d'Internet repose aussi sur l'économie de marché. Ainsi, les acteurs qui souhaitent intégrer le marché de l'Internet ont souvent tendance à accepter les normes et les techniques en place. Lorsque les intérêts convergent, il y a coopération. Ceci réduit leurs coûts,

mais a aussi pour effet «collatéral» d'accroître le contrôle de l'hégémon; ce qui accroît son pouvoir.

Pour Hanson (2008), les technologies de l'information et des communications auraient modifié les relations internationales à un point tel qu'il serait possible de faire état d'une véritable révolution de l'information. Ainsi, même si les TICs permettent aux États de se développer et de mieux s'organiser, les nouvelles technologies augmentent parallèlement l'étendue des cibles possibles. Ainsi, l'État qui contrôle la gestion des TICs devient à son tour une cible privilégiée par les résistants ou les détracteurs. Subséquemment, les TICs sont devenues certes des outils de gestion, d'influence et de contrôle, mais aussi une source de menaces potentielles et des instruments de défense militaire. De ce fait, pour éviter les risques potentiels à cet effet, la défense fut contrainte de se réorganiser, voire de révolutionner les affaires militaires. Les TICs ont révolutionné les affaires militaires de trois façons, soient en offrant une nouvelle vision des menaces ou de la commande lors des opérations, en augmentant la vitesse, l'efficacité des commandes et les stratégies de combat et en rendant possible les armes intelligentes (« smart »). Ainsi, les TICs ont permis de réorienter les stratégies de combat ainsi que leur préparation, mais elles ont aussi ouverts la porte à de nouveaux dangers. De ce fait, ce qui apparaissait comme une révolution, qui s'inscrit dans le sens du progrès, pourrait alors sombrer dans la contre-révolution par les nouveaux dangers que les NTICs comportent.

C'est alors que sont apparues les contre-révolutions qui ouvrent la porte aux nouvelles guerres. Ces nouvelles formes de guerre auront moins recours aux stratégies traditionnelles, mais miseront davantage sur les NTICs et seront des forces irrégulières mises en réseaux. Ces contre-révolutions seront utilisées afin de diffuser des messages, d'élargir l'audience et de recruter. Or, ces contre-révolutions pourraient aussi être mises au service du pouvoir lui-même (Hanson 2008 : 123).

Malgré les diverses positions par rapport au devenir des États face à l'enjeu que leur pose les TICs, il n'en demeure pas moins que l'accroissement de la quantité et des sources d'information ainsi que la rapidité de leur traitement a pour effet d'amplifier la complexité de la gestion de l'information. Ceci a pour effet de rendre difficile l'obtention de consensus au niveau politique et

ce, à tous les niveaux. Enfin, l'arrivée des TICs rend la situation complexe et pose certainement un défi aux États en matière de souveraineté des États, d'identité et de cultures. L'ensemble de ces considérations augmenterait le besoin de coopération internationale en matière de gouvernance du cyberespace (Hanson 2008 : 184).

Libicki (2007) corrobore ces propos. Pour lui, Internet est un nouvel espace d'échange et de commerce, mais aussi un espace de dépendance, d'influence, voire de contrôle. Ce nouvel espace s'insère dans le système de l'information et comme tout système, il a ses limites qui soulèvent des risques potentiels. De ce fait, l'évolution et les transformations du cyberespace soulèvent des enjeux en matière de sécurité (attaques, guerre, etc.), mais aussi en matière de souveraineté (influence, contrôle) et de gouvernance (gestion du cyberespace).

De ce fait, Internet soulève un nouvel enjeu en matière de sécurité, car l'ennemi ne porte plus l'habit traditionnel. Cette nouvelle réalité requiert une *redéfinition de la sécurité*. À cet effet, il existerait deux types de conquêtes dans le cyberespace, soit la « hostile conquest » qui renvoie à l'approche fermée, au conflit, à la défense et au « hard power ». La seconde, la « friendly conquest », fait référence à la douce/subtile conquête. Elle repose sur le « soft power », mise sur l'approche ouverte et sur l'influence sur la culture. Cette approche accroît la dépendance à l'égard du système de l'information, ce qui augmente son contrôle. De ce fait, la problématique de la sécurité du cyberespace est certainement d'ordre technique par la nature du système, mais renvoie aussi à la gestion des politiques publiques (*policy*). L'auteur soutient qu'il serait favorable de miser sur une approche ouverte dans le cyberespace par rapport au fait de privilégier une approche fermée. Or, l'approche ouverte aurait le défaut d'accroître l'influence, mais aussi le contrôle (Libicki 2007 : 3-4).

La thèse de Libicki va essentiellement comme suit : il semble difficile de contrôler le monde par la « hostile conquest ». Cependant, la « friendly conquest » mériterait notre attention et une sérieuse analyse. Cette conquête amicale et subtile du cyberespace renvoie principalement à la dépendance des utilisateurs envers le système de l'information. Cette dépendance semble réelle et pourrait être profonde. Cette conquête soulève, à sa façon certains enjeux, tels le risque

d'accroître le nombre de victimes qui dépendent du système, tout en ouvrant la possibilité au risque que représente l'influence et le contrôle du système (Libicki 2007 : 125).

Or, l'approche qu'est la « friendly conquest » repose essentiellement sur un mécanisme de coalition. En fait, le cyberespace est un lieu propice à la création de coalitions et de ce fait, le nombre ne ferait que s'accroître. Cependant, Libicki soutient que ces coalitions seraient bien souvent asymétriques. De ce fait, le danger de la « friendly conquest » s'insère dans le cœur de ces coalitions par le fait que la coalition exerce une certaine influence sur les individus et que cette influence n'irait pas toujours dans le sens que les acteurs avaient choisi préalablement (Libicki 2007 : 166-168).

Par ailleurs, Libicki démontre l'étendue et l'influence de l'hégémon à travers le cyberespace. À cet effet, il propose deux cas qui illustrent ce constat, soient le *Géospatial Data* ainsi que le *National Identity Sytem*. En fait, ces bases de données sont catégorisées, ce qui nécessite une interprétation lors de leur analyse. Or, cette interprétation influencerait la pensée des utilisateurs et par le fait même, la culture. De ce fait, l'existence de ces bases de données augmenterait la dépendance des utilisateurs envers le système, mais en prime, cette utilisation aurait aussi pour effet d'accroître l'influence de l'hégémon sur les mêmes utilisateurs (Libicki 2007 : 192).

De plus, les États-Unis sont un des seuls États qui a les ressources (financières et techniques) en vue de soutenir l'infrastructure du cyberespace et ce, tout en investissant dans les systèmes de sécurité. Or, le partage de l'information avec d'autres États crée des coalitions volontaires, mais parfois un certain état de dépendance et d'influence de ceux-ci envers les Américains. Ainsi, en matière de souveraineté, cette attitude serait anti-éthique du point de vue de la norme. Enfin, selon Libicki, il s'agit de coalitions qui prennent la forme d'interdépendance, mais aussi d'influence asymétrique et donc de dépendance. Cela accroît le contrôle et le pouvoir de l'hégémon (Libicki 2007 : 169-191).

Ce bref aperçu de la littérature sur le cyberespace et les relations internationales semble conclure que les mesures actuellement en place dans la gouvernance et de la sécurisation du cyberespace tendent à renforcer le pouvoir de l'hégémon. Toutefois, l'ensemble de cette littérature passe sous

silence le rôle des organisations internationales dans la sécurisation du cyberespace et se concentre pour la très grande majorité à des analyses de cas basées sur les actions des États à l'interne ou encore sur les conséquences possibles (politiques et économiques entre autres) des nouvelles technologies de l'information. De plus, cette littérature n'aborde pas la question sous l'angle de la stabilité hégémonique ou encore moins sous l'angle de l'intégration régionale, deux aspects facteurs de stabilité et de sécurisation internationale.

La méthode de recherche

Ce projet de recherche désire ainsi vérifier si les institutions régionales favorisent le développement et le fonctionnement de politiques communes de cybersécurité, et ce, à travers une analyse comparative de la gouvernance à ce sujet dans les régions des Amériques et de l'Europe.

Par conséquent, la recherche proposée s'articule autour de trois objectifs distincts. Le premier objectif vise à affiner le lien entre la nature des institutions régionales dans leurs nombreuses déclinaisons et les possibilités de développement de politiques communes en matière de cybersécurité. Selon Petiteville, le nombre d'États concernés, la vocation prioritairement politique ou commerciale du processus d'intégration, ainsi que le degré accepté d'institutionnalisation et de transfert de souveraineté des pays (Petiteville, 1997) constituent des facteurs décisifs quant à la nature de ces institutions et, de ce fait, dans l'efficacité de leur capacité d'action régionale pour ce qui est de l'élaboration d'une politique commune de cybersécurité. À travers cette étude de deux exemples de régionalisme, la présente recherche désire contribuer à la compréhension des mécanismes de création de politiques selon la nature du processus d'intégration régionale.

Le deuxième objectif consiste à participer aux débats théoriques en relations internationales quant au rôle joué par ces processus d'intégration régionale dans la sécurisation du cyberespace. L'apparition d'enjeux transfrontaliers d'importance, tels que la cybersécurité, provoque d'énormes conséquences pour ce qui est de la gestion de l'espace international, qui devient plus difficile puisque les États ne semblent plus être les uniques instigateurs de guerre et de violence dans le système international (Fortmann 2000; Libicki 2007). Or, il serait intéressant d'observer

si la résolution de problématiques transnationales par la voie d'institutions régionales se révèle avoir une portée concluante pour l'avenir des relations entre les États.

Finalement, le troisième objectif de la recherche s'efforce de comprendre le rôle d'un hégémon dans le développement et la mise en œuvre d'une politique commune de cybersécurité. L'étude de la présence de l'hégémon dans le cas interaméricain et de son absence dans le cas européen vérifiera la pertinence de la théorie de Pedersen (Pedersen, 1998 et 2002) à propos de la coopération hégémonique.

L'hypothèse à la base de cette recherche cherche à comprendre le rôle d'une puissance hégémonique dans la configuration d'une stratégie multilatérale de cybersécurité aux États-Unis et dans l'Union européenne. Dans le dernier cas, il s'agit en fait de vérifier le résultat de la coopération en la matière en l'absence d'une puissance hégémonique.

Trois méthodes de collecte de l'information et d'analyse des données ont été utilisées dans cette recherche. La première consiste en l'observation documentaire des textes (très nombreux) produits par l'Union européenne et les États-Unis en matière de cybersécurité. Bien entendu, une sélection des textes les plus pertinents a été effectuée. La deuxième méthode a consisté en une analyse de contenu par nombre d'occurrence des mots clefs (illustrés dans le tableau 1 ci-dessous). Enfin, la dernière méthode utilisée a servi à faire une lecture textuelle des textes les plus importants en matière de cybersécurité afin d'approfondir et de comprendre les résultats de l'analyse de contenu.

Les résultats de l'analyse sont présentés en deux parties. La première illustre les résultats préliminaires de la recherche en ce qui concerne les Amériques et le rôle du gouvernement étasunien, la puissance hégémonique dans la région, dans la promotion de la coopération multilatérale en matière de cybersécurité. La deuxième partie présente les résultats préliminaires de la recherche en ce qui concerne l'Union européenne et la création d'une coopération ou d'une collaboration à propos du même enjeu, mais en l'absence de puissance hégémonique porteuse d'une volonté de coopération multilatérale.

Les Amériques et le rôle des États-Unis

La première série de variable était destinée à trouver l'importance relative des principaux mots clefs relatifs à la cybersécurité dans les documents officiels du gouvernement américain. Pour ce faire, nous avons dénombrés 15 termes dans la documentation pertinente[1]. Le même processus a été utilisé pour la deuxième série de variables relatives à la coopération dans les Amériques. Dans la perspective d'un scénario de coopération hégémonique, plus le gouvernement américain se préoccupe de cybersécurité et plus il comptera sur la coopération continentale pour réaliser ses objectifs. En d'autres termes, le gouvernement américain poursuit une stratégie de coopération hégémonique dans la région à propos de la cybersécurité dans lequel il favorise un niveau relativement élevé d'institutionnalisation régionale et une ouverture à des solutions multilatérales.

Les deux tableaux suivants (Tableaux 1 et 2) exposent les résultats générés par l'analyse de contenu. Les termes sont classés par fréquence d'apparition, à commencer par les termes les plus souvent mentionnés dans le document. Le traitement de l'analyse de contenu a été effectué en anglais puisqu'il s'agit de la langue officielle utilisée dans ces documents.

Tableau 1 Fréquence des termes relatifs à la cybersécurité dans les documents officiels des États-Unis

Termes	Nombre de document	Fréquence
1. Cybersecurity	23	2038
2. Critical Infrastructure	38	871
3. Cyberspace	24	671
4. Cyberterrorism	14	134
5. Information Warfare	15	64
6. Networks Security	18	47
7. Computer Attack	10	36

[1] La liste des documents analysée serait trop longue à mettre dans cette communication. Elle peut être obtenue sur demande.

8. Cyberwar	6	18
9. Cyberthreat	2	2
10. Information War	0	0
11. Cybernetic Attack	0	0
12. Cybernetic War	0	0
13. Networks Conflict	0	0
14. Networks War	0	0
15. Cyberconflict	0	0

Table 2 Fréquence des termes relatifs à la coopération dans les Amériques dans les documents officiels des États-Unis

Termes	**Nombre de document**	**Fréquence**
1. Cooperation	32	178
2. Regional	14	126
3. Multilateral	8	18
4. Hemisphere	3	4
5. Organization of American States (OAS)	3	4
6. Regional security	2	2
7. Hemispheric	1	2
8. South America	1	1
9. Inter-american	1	1
10. Hemispheric Cooperation	0	0

11. Summit of the Americas (SOA)	0	0
12. Multilateralism	0	0
13. Hemispheric security	0	0
14. Inter-American Defense Board (IADB)	0	0
15. Inter-American Security	0	0
Total	67	359

L'analyse de contenu a montré qu'il existe une forte impulsion mise de l'avant par le gouvernement américain pour sécuriser le cyberespace. Pourtant, en contradiction avec notre hypothèse, les résultats de l'analyse de contenu n'ont pas affiché une volonté claire de promouvoir une institutionnalisation régionale pour contrer la menace et favoriser la cybersécurité. La relative insignifiance du nombre d'occurrence des termes concernant la coopération dans le continent appuie cette conclusion.

Aussi, notre analyse visait à déterminer l'impact potentiel des documents officiels étasuniens sur l'Organisation des États américains à propos du développement et de la mise en œuvre d'une politique régionale commune en matière de cybersécurité. Nous avons trouvé des recommandations sur la coopération dans l'hémisphère sous des formes diverses en ce qui concerne la cybersécurité dans la *National Strategy to Secure Cyberspace* et dans *The Federal Plan for Cyber Security*.

Nous avons observé que l'importance relative de la coopération internationale dans les documents officiels du gouvernement américain est très faible et que les États-Unis ont choisi d'orienter leur action pour améliorer davantage la cybersécurité à l'échelle nationale. Nous pouvons conclure

que le développement d'un mécanisme de coopération hémisphérique n'est pas une priorité dans la stratégie des États-Unis pour sécuriser et pour améliorer la gouvernance dans le cyberespace.

L'Europe et l'absence de puissance hégémonique

L'analyse de contenu des documents officiels émanant de l'Union européenne a été effectuée différemment de celle concernant les États-Unis et les Amériques. En effet, dans le cas européen nous voulions vérifier les relations entre l'Union et les différents pays membres de cette Union aurait été inapproprié puisque le cadre juridique est totalement différent de celui qui prévaut dans les Amériques pour l'OÉA par exemple. En somme, les deux régions du monde et les deux principales organisations multilatérales qui gouvernent ces deux régions ne sont pas nécessairement comparables. La délégation des parts de souveraineté nationale et les processus décisionnels sont très différents par exemple. Toutefois, toutes deux sont irrémédiablement des organisations internationales qui exécutent la volonté de leurs États membres. Des États membres à la puissance différente et aux capacités différentes. Ainsi, vérifier l'influence d'un hégémon dans le cas des Amériques s'avère instructif quant aux possibilités que ce dernier peut mettre de l'avant en comparaison à une organisation internationale multilatérale sans hégémon ou sans une puissance réellement dominante par rapport aux autres.

Il n'est donc pas surprenant que l'analyse de contenu des documents officiels de l'Union européenne dévoile des résultats différents de ceux présentés ci-dessus pour les États-Unis. Le Tableau 3 qui suit présente les résultats exhaustifs de l'analyse de contenu des documents officiels de l'Union européenne en matière de cybersécurité[2]. Contrairement à l'analyse de contenu précédente, les documents officiels de l'Union européenne qui ont été analysés sont en français et en anglais, ce qui explique la présence des termes français et anglais dans le Tableau 3.

[2] La liste des documents analysée serait trop longue à mettre dans cette communication. Elle peut être obtenue sur demande.

Tableau 3 Fréquence des termes dans les documents officiels de l'Union européenne		
Termes	**Fréquence**	**Nombre de document**
1. safer internet	1331	34
2. sécurité de(s) réseau(x)/network(s) security	488	82
3. cybercriminalité/cybercrime(s)	331	75
4. critical infrastructure	302	35
5. criminalité informatique	124	19
6. critical information(s)	120	27
7. cybersécurité/cybersecurity	95	41
8. cyberespace/cyberspace	74	21
9. pourriel(s)	73	5
10. cyber-attaque(s)/cyber-attack(s)	64	22
11. computer-related crime	48	9
12. IT-security	23	7
13. cyberterrorisme/cyberterrorism	19	11
14. ICT-security	16	3
15. attaque(s) informatique(s)	6	5
16. information warfare	3	2
17. criminalité dans le cyberespace	2	2

18. cyber-threat(s)	2	2
19. cyberdétective	1	1
20. cyber-délit(s)	1	1
21. cyberwar	1	1
22. computer attack	1	1
23. I-war	0	0
24. e-war	0	0
25. safer network	0	0
26. govocert	0	0
27. gov-certs	0	0
28. g-certs	0	0
29. ePractice	0	0
30. espilogiciel(s)	0	0
31. espi-logiciel(s)	0	0
32. safe network	0	0
33. cybernetic war	0	0
34. guerre cybernetique	0	0
35. cybernetic attack	0	0
36. attaque cybernétique	0	0
37. cyberfraud	0	0
38. cyber-fraude	0	0

39. network(s) conflict	0	0
40. cyberconflict(s)	0	0
41. cyber-conflict	0	0
42. cyber-conflit	0	0
43. cyberconflit	0	0
Total	3125	406

À la lumière des résultats de l'analyse de contenu, il est possible d'affirmer que les États membres de l'Union européenne sont conscients des risques et des menaces associés au cyberespace. En effet, les résultats reflètent trois choses principales dans les objectifs et les intentions des membres de l'Union européenne. Premièrement, il semble bien que l'objectif principal est de sécuriser le réseau internet. Ainsi, la fréquence très élevée des termes «safer internet» en position 1, «sécurité de(s) réseau(x)/network(s) security» en position 2 et du terme «cybersécurité/cybersecurity» en position 7 le démontrent clairement. Cette volonté de sécuriser le cyberespace est tout à fait compréhensible puisqu'il s'agit du principe sur lequel repose l'ensemble de tout processus de sécurité. Dans le cyberespace, la sécurisation du réseau passe inévitablement par la protection des infrastructures critiques (critical infrastructure) en position 4 et des informations critiques (critical information(s)) en position 6. D'ailleurs, le European Programme for Critical Infrastructure Protection (EPCIP) définit les infrastructures critiques de façon très large et ayant un facteur de risque très élevé en cas de vulnérabilité:

> Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services.[3]

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF, (consulté le 21 avril 2009)

Deuxièmement, la sécurisation mentionnée précédemment passe par la lutte contre les cybercrimes et concerne le deuxième aspect de la sécurisation du cyberespace c'est-à-dire la protection des informations critiques. Ainsi les termes « cybercriminalité/cybercrime(s)» en position 2, «criminalité informatique» en position 5 et, dans une moindre mesure, les termes «pourriel(s) en position 9 et « computer-related crime» en position 11 affichent sans équivoque la volonté des membres de l'Union européenne d'agir dans ce domaine. D'ailleurs, l'UE a mis sur pied le CEPD (Contrôleur européen de la protection des données) qui agit «en tant qu'autorité de contrôle indépendante chargée de surveiller le traitement des données à caractère personnel par les institutions et organes communautaires[4]». Le CEPD s'active dans la proposition et la formulation de politiques en contribuant à la préparation des positions communes et des avis conjoints pour les États membres de l'Union européenne. Il est de plus consulté lors de la formulation des nouvelles législations de l'UE. De plus, afin de compléter le travail effectué par le CEPD, les membres de l'UE ont mis en place le CTOSE (le cyberdétective de l'Union européenne). «Le projet CTOSE (Cyber Tools On-Line Search for Evidence: Outils de recherche de preuves électroniques) de l'UE permet d'identifier, de garantir, d'intégrer et de présenter des preuves électroniques concernant des cyber-délits[5]».

Enfin, le dernier constat qu'il est possible de faire est l'absence totale des termes concernant les cyberconflits en tant que tels. Les termes «cyber-attaque(s)/cyber-attack(s)» en position 10 et «attaque(s) informatique(s)» en position 15, dans ce contexte, ne concernent pas les cyberconflits mais font plutôt référence à des attaques informatiques de nature criminelle sans nécessairement avoir d'objectif politique ou militaire. Le terme «information warfare» semble constituer ici une anomalie puisqu'il apparaît seulement trois fois dans deux documents sur les 406 documents analysés. D'ailleurs, cette constatation se confirme par l'absence des termes «cybernetic war», «cyberconflict(s)» et tous les autres termes relatifs ou synonymes à ceux-ci.

L'analyse de contenu est certes intéressante, mais elle ne dévoile pas toute la densité institutionnelle qui a été progressivement bâtie par les États membres de l'Union européenne. En fait, l'Union européenne a généré une multitude d'agences ou d'institutions en son sein ou en

[4] http://www.edps.europa.eu/EDPSWEB/edps/pid/1?lang=fr (consulté le 21 avril 2009)
[5]http://europa.eu/rapid/pressReleasesAction.do?reference=IP/03/1443&format=HTML&aged=0&language=FR&guiLanguage=en (consulté le 21 avril 2009)

partenariat avec le secteur privé. Cette toile institutionnelle est tantôt dense tantôt souple et relâchée. On retrouve ainsi l'ENISA (European Network and Information Security Agency) qui «vise en tout premier lieu à renforcer la capacité de la Communauté européenne, des États membres et du secteur des entreprises, en matière de prévention, de réaction et de gestion des problèmes liés à la sécurité des réseaux et de l'information[6]». L'ENISA a mis en œuvre l'EISAS (European Information Sharing and Alert System). Ce système «has been asked by the European Commission to deliver a feasibility study on a Europe-wide sharing system for NIS related information to end-users/citizens and SMEs, to raise IT security awareness and close gaps in the coverage with such information.[7]».

Enfin, toujours parmi les principales institutions, il y a le EPCIP (European Programme for Critical Infrastructure Protection) dont il a été question ci-dessus. En 2004, le Conseil européen a demandé à la Commisson européenne de préparer une stratégie générale pour améliorer la protection des infrastructures critiques. Un ensemble de travaux (séminaires, communications, Livre vert) a été effectué de 2004 à 2006 à ce sujet. La protection des infrastructures critiques est davantage ici entendue comme la protection contre les attaques terroristes visant les réseaux informatiques que par rapport aux activités criminelles (d'origine terroriste ou non).[8]

Conclusion

Cette communication avait pour objectif d'exposer les résultats préliminaires de l'analyse de contenu effectuée sur deux corpus de documents officiels. Le premier était composé des 67 documents officiels produits par le gouvernement des États-Unis à propos de la cybersécurité et des termes qui y sont termes associés. Le deuxième corpus était composé des 406 documents officiels produit par l'Union européenne à propos des mêmes thèmes.

[6] http://www.enisa.europa.eu/ (consulté le 21 avril 2009)
[7] http://www.enisa.europa.eu/pages/faq_technical.html#t01 (consulté le 21 avril 2009)
[8] http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm (consulté le 21 avril 2009)

L'objectif central était d'apporter des éléments de réponse à la problématique plus générale de l'hégémonie coopérative et des résultats potentiels qu'elle peut produire en termes de formulation et de développement de politiques communes.

Essentiellement, l'analyse des résultats générés par l'analyse de contenu des deux corpus permet de conclure que les États-Unis n'ont pas mis de l'avant une stratégie d'hégémonie coopérative en matière de sécurisation du cyberespace dans ses relations avec les pays des Amériques. En fait, l'aspect multilatéral semble très négligé dans l'approche en termes de sécurité qui est entreprise face au cyberespace. Cela contredit d'autres résultats de recherche à propos d'autres domaines de coopération entre les États-Unis et les autres pays des Amériques (Mace et Loiseau, 2005). Il semble que l'enjeu soit trop sensible et au cœur même de la sécurité nationale des États-Unis pour qu'une approche multilatérale de la question soit envisagée pour l'instant.

En Europe, la situation est très différente. En effet, d'une part, l'absence de puissance hégémonique et de stratégie d'hégémonie coopérative sous-jacente au processus de coopération régional ne semble pas freiner la coopération en matière de cybersécurité. D'autre part, la densité des relations antérieures de coopération, les processus et les institutions déjà en place semblent démontrer que les membres de l'Union européenne n'ont pas hésité à transformer cet enjeu de sécurité en un thème débattu et traité de façon ouverte et multilatérale par eux-mêmes. En termes de coûts et de ressources, le gain potentiel (la sécurisation du cyberespace et des infrastructures critiques) pour l'ensemble des membres semblait plus important que des gains équivalents pour chacun des membres pris individuellement.

Bien entendu, ces résultats demeurent préliminaires et demandent un approfondissement des pistes lancées et des constats faits dans cette communication. Les prochaines étapes seront de vérifier le rôle transatlantique qu'ont pu jouer d'autres institutions internationales (l'OTAN par exemple) dans la sécurisation du cyberespace.

Bibliographie

CHECKEL, Jeffrey T. «International Institutions and Socialization in Europe: Introduction and Framework», *International Organization*, vol. 59, n. 4, Fall 2005, pp. 801-826.

CONKLIN, Art et WHITE, Gregory B. *e-Gouvernment and Cyber-Security : The Role of Cyber Security Exercises*, Hawaii, USA, Communication présentée au International Conference on System Sciences, 2006.

CORTELL, Andrew P. et DAVIS, James W. Jr. «Understanding the Domestic Impact of International Norms : A Research Agenda», *International Studies Review*, Vol. 2, Issue 1, printemps 2000, pp. 65-87.

DUPUY, Gabriel. *Internet, Géographie d'un réseau*, Paris, Éllipses, 2002. FLEURY, Guillaume. 2008. « Internet comme vecteur de pouvoir », *Études internationales*, vol. 39, no1, pp. 83-104.

FORTMANN, Michel. «À l'Ouest rien de nouveau ? Les théories sur l'avenir de la guerre au seuil du XXI^{e} siècle», *Études internationales*, XXXI, no 1, mars 2000, pp. 57-90.

GALLAHER, Micheal P. *et al*. 2008. *Cyber Security Economic Strategies and Public Policy Alternatives*, Cheltenham, Edward Elgar, 266 p.

GANSLER, Jacques S. «Protecting Cyberspace», dans BINNENDIJK, Hans (dir.). *Transforming America's Military*, Washington DC, National Defense University Press, 2002, pp. 331-344.

GOLDSTEIN, Judith *et al*. «Introduction : Legalization and World Politics», *International Organization*, Vol. 54, no 3, été 2000, pp. 385-399.

HANSON, Elizabeth C. 2008. *The information revolution and world politics*, Lanham, Rowman and Littlefield Publishers, 269 p.

KEOHANE, Robert O. «Governance in a Partially Globalized World», *American Political Science Review*, Vol. 95, no 1, 2001, pp. 1-13.

KLOTZ, Audie et LYNCH, Cecelia. «Le constructivisme dans la théorie des relations internationales», *Critique internationale*, no 2, hiver 1999, pp. 51-62.

LIBICKI, Martin C. 2007. *Conquest in cyberspace. National security and information warfare*, New York, Cambridge University press, 324 p.

MACE, Gordon et LOISEAU, Hugo. «Cooperative Hegemony and Summitry in the Americas», *Latin American Politics and Society*, Volume 47, Number 4, Winter 2005, pp. 107-134.

MEARSHEIMER, John J. «The False Promise of International Institutions», *International Security*, Vol. 19, no 3, hiver 1994-1995, pp. 5-49.

Organisation de Coopération et de Développement Économiques (OCDE). 2003. *Les risques émergents au XXIe siècle, Vers un programme d'action*, Paris, 325 p.

PEDERSEN, Thomas. *Germany, France and the Integration of Europe: A Realist Interpretation*, London, Cassell/Pinter, 1998.

PEDERSEN, Thomas. « Cooperative Hegemony : Power, Ideas, and Institutions in Regional Integration », *Review of International Studies*, 2002, 28 : 677-696.

PETITEVILLE, Franck. «Les processus d'intégration régionale: vecteur de structuration du système international?», *Études internationales,* vol. 28, no 3, 1997, pp. 511-533.

TÉNIER, Jacques. *Intégrations régionales et mondialisation, Complémentarité ou contradiction*, Paris, La documentation française, 2003.

THOMAS, Ward. *The Ethics of Destruction, Norms and Force in International Relations*, Ithaca, Cornell University Press, 2001.

WAUTELET, Michel. *Les cyberconflits, Internet, autoroutes de l'information et cyberespace : quelles menaces ?*, Bruxelles, Éditions GRIP, 1998.