UNIVERSITE GALATASARAY
Institut des Sciences Sociales
Relations Internationales

LES COMMUNAUTÉS ÉPISTÉMIQUES ET LA COORDINATION DE LA POLITIQUE INTERNATIONALE : LE CAS DE L'OCDE ET DU BIAC POUR LA SÉCURITÉ DES SYSTÈMES ET DES RÉSEAUX D'INFORMATION

Baran OSMANOĞLU

Directeur de recherche : Yrd.Doç.Dr.Selcan SERDAROĞLU

Memoire pour l'obtention du DEA 'Relations Internationales'

Février, 2004

Je tiens à adresser mes remerciements chaleureux à Melle Dr.Selcan SERDAROĞLU qui a beaucoup apporté à ce mémoire et à ma famille qui m'a supporté tout au long de mon travail.

TABLE DES MATIERES

ABREVIATIONS

ABM	: Le Traité de Missile Antiballistique
BIAC	: Business and Industry Advice Comity - le Comité Consultatif Economique
CFC	: Chlorofluorocarbones
CSCE	: Conférence sur la Sécurité et la Coopération en Europe
GATS	: General Agreement on Tariffs and Services
GATT	: General Agreement on Tariffs and Trade
OCDE	: Organisation pour la Coopération et le Développement Economique
OMC	: Organisation Mondiale du Commerce
ONU	: Organisation des Nations Unies
OPEP	: Organisation des Pays Exportateurs de Pétrole
OSCE	: Organisation de la Sécurité et la Coopération en Europe
SDN	: Société des Nations

TABLEAUX

INTRODUCTION

La croissance des problèmes de nature complexe et technique d'intérêt national, mais d'autant plus mondial donnent lieu à l'augmentation de l'incertitude de la part des acteurs étatiques vis-à-vis de l'environnement politique. En outre, les sujets de domaines politiques impliquant des différents acteurs, qui sont discutés, négociés et décidés ne cesse de croître dûment à la mondialisation, aux changements technologiques, économiques et politiques. De ce fait, la coordination de la politique internationale, qui d'après la formulation de Keohane où les actions des différents acteurs -qui ne sont pas dans une harmonie préexistante- sont apportées à une conformité l'un avec l'autre à travers un processus de négociation, devient de plus en plus compliqué pour les États.

Considérant que le système international contemporain fait intervenir des acteurs non souverains variés que sont l'ensemble des acteurs non-étatiques et que le paradigme stato-centré ne fournit pas une base adéquate pour l'étude de la politique mondiale en transformation, il devient important de savoir comment la coordination de la politique des États a évolué face aux problèmes complexes relevant un degré élevé d'incertitude dans le monde multicentré, composé des acteurs non souverains.

Dans ce cadre, les problèmes liés aux changements technologiques constituent une partie importante des problèmes de niveau mondial auxquels font face les autorités étatiques. Les progrès réalisés dans le domaine des technologies de traitement d'information et de télécommunication qui convergent sur Internet, décrit souvent comme la 'révolution de l'information', ont modifié les modes de gestion et d'organisation des institutions publiques et privées aussi bien que les capacités de communication des individus. Ainsi, Internet a aujourd'hui un impact important sur les domaines variés de la société et sur la diffusion de l'information. Cependant, ce medium a attiré l'intérêt des acteurs malveillants incités à accomplir des activités criminelles et illégales. L'architecture d'Internet avait été conçue pour la liaison d'un nombre limité d'ordinateurs, par conséquent cette restriction a impliqué des

contraintes techniques face à la dimension de son utilisation d'aujourd'hui. Ce déficit a favorisé les tentatives d'intrusions illégales aux réseaux et les fraudes informatiques, qui se manifestent notamment sous la forme de vols de données ou de propagations de virus informatique. Les dommages considérables causés par la « cybercriminalité » frappent aussi bien les pouvoirs publics que les entreprises et les individus.

Toutefois, la caractéristique transnationale d'Internet et sa structure décentralisée se présentent comme des obstacles insurmontables dans la tentative d'instituer un mécanisme de contrôle dans les limites nationales des États. En effet, les États semblent être de moins en moins capables de réglementer individuellement les activités dans le cyberespace, les systèmes juridiques nationaux apparaissent largement inadéquats dans ce cadre. D'une part, ce problème surpasse les limites des territoires nationaux des États. D'autre part, la capacité du point de vue technique des États reste insuffisante dans ce domaine. En effet, les infrastructures des systèmes de télécommunications qui étaient maîtrisées par des opérateurs publics sont désormais détenues par les entreprises privées suite à la vague de privatisation surgie dans les années 1990. D'autant plus que les technologies d'information et de communication sont conçues et développées par les entreprises privées, ainsi ces derniers détiennent particulièrement l'expertise technique dans ce domaine.

Face au problème de la cybercriminalité, pouvant être classé dans les 'low politics' d'après la vision réaliste des Relations Internationales puisqu'il n'est pas issu du domaine militaire et de sécurité, qui surpasse les frontières nationales, il est nécessaire de savoir comment réagissent les États et quelle est l'approche adoptée par les décideurs qui ne sont pas suffisamment familiers aux aspects techniques du problème pour l'élaboration d'une solution viable.

Dans ce travail, c'est l'approche de réseaux d'experts, dénommés comme communautés épistémiques, introduit par Peter Haas, qui sera étudié comme une approche pour l'élucidation des problèmes complexes où est présent un degré élevé d'incertitude. Bien que les conditions systémiques actuelles imposent certaines contraintes sur les actions étatiques, l'analyse du rôle de ces réseaux d'experts, sera limitée en aide prêtée aux autorités étatiques sous forme de propositions de politiques

spécifiques dans l'articulation des problèmes complexes, l'identification de leurs intérêts et des points saillants pour la négociation.

La première partie de ce travail, cherche à monter comment varie la coordination de la politique des États dans les situations qui impliquent un degré élevé d'incertitude et qui surpassent la capacité d'action individuelle des États, en adoptant la méthode d'analyse de Rosenau considérant deux niveaux d'analyse dans les Relations Internationales : le niveau systémique et le niveau d'acteur.

Dans le premier chapitre, une analyse au niveau systémique cherche à montrer que l'approche adoptée par les États qui sont faces aux situations d'incertitudes où la complexité des problèmes surpassent leurs capacités est la coopération internationale. Dans ce cadre, est analysé l'évolution de la coopération. D'une part en présentant les différentes formes de coopération, d'autre part en montrant que la coopération interétatique n'est plus une approche suffisante pour répondre aux problèmes surgis dans le contexte de la mondialisation et dans un monde multicentré d'où des différents acteurs y sont impliqués.

Dans le deuxième chapitre, une analyse au niveau d'acteur cherche à montrer comment les réseaux d'experts, les communautés épistémiques, jouent un rôle important dans la coordination de la politique internationale pour l'articulation des problèmes de nature complexe et technique. En présentant les caractéristiques principales de ces réseaux et leurs principes d'intervention aux problèmes ainsi que leurs contributions à l'évolution politique, ce chapitre cherche à montrer comment ces acteurs sont capables d'influencer les résultats par l'intermédiaire du savoir.

Dans la deuxième partie de ce travail, une étude de cas comportant sur les travaux d'une Organisation Internationale, l'Organisation de Coopération et de Développement économique (OCDE) dans le domaine de la sécurité des systèmes est entamée afin de présenter comment les États agissent face au problème de la cybercriminalité, dans un contexte impliquant un problème de niveau transnationale nécessitant une coopération internationale et une intervention experte. Il est de même visé à montrer les interactions entre les différents acteurs en particulier les États et les membres du réseau d'experts au cours des processus de négociations.

PREMIERE PARTIE

Coordination de la politique internationale :

La coopération et l'intervention des communautés épistémiques

A. La coopération internationale

Les débats sur la recherche de l'ordre dans le système international anarchique se convergent sur la notion de coopération. Face à la situation de l'incertitude provenant du manque d'information au niveau des actions des autres, les États coopèrent c'est-à-dire « ajustent leurs comportements aux préférences réelles ou anticipées d'autrui, à travers un processus de coordination »[1] par l'intermédiaire des institutions internationales qu'ils conçoivent. Comme l'affirme Keohane, la capacité des États de communiquer et de coopérer dépend des institutions établis par ceux-ci et les modes de coopération sont concevables que dans le contexte des institutions qui permettent de définir la signification des actions des acteurs. Cependant, en moins d'un siècle l'image de la société internationale est passée du modèle statocentré composé d'acteurs étatiques suivant les mêmes buts de puissance et d'intérêt vers le modèle multicentré. Cette transformation a conduit donc une révision de la notion de coopération internationale, ses acteurs, ses moyens et ses fins.

1. La coopération et la loi internationale

Les premières formes de coopération entre les États étaient fondées sur le droit de cœxistence, jusqu'à la première guerre mondiale. Les exigences de ce droit, dont la base était constituée par les notions de souveraineté et d'égalité, émergeaient plutôt comme prohibition de conduites tels qu' intervention dans les affaires intérieures des autres États, la violation des traités, la restriction des activités des diplomates. Dans un tel système, l'ordre international était mené à être établi par le strict respect des compétences de chaque État, sans la présence d'organisation permanente particulière. Depuis le milieu du XIX^{e} siècle, des règles, souvent contestées et changées, étaient émises par les États dans le but d'assurer leur subsistance sur la scène internationale.

---

[1] Telle est la définition de la coopération proposée par R. Keohane, **After Hegemony. Cooperation and Discord in the World Political Economy**, Princeton, Princeton University Press, 1984 p.51

Cette revendication du droit de cœxistence reposait donc sur la gestion de la séparation imperturbable des États en compétition[2].

L'approche de droit international a été l'objet de longs débats sur la suggestion qu'un système légal ne peut être établi et renforcé qu'à l'intérieure de la structure centralisée fournie par l'État. Bien que ceci soit contesté, il n'existe pas non plus une certitude pour déterminer la manière dont les lois sont formulées et maintenues dans la structure anarchique et décentralisée du système international.

Néanmoins, cette problématique reliée au statut des règles dans un système anarchique a été largement sousestimée après la période suite à fin de la première guerre mondiale, lorsque des études institutionnalisées des relations internationales ont été établies. Durant cette période, une volonté exigeant le besoin de coopération entre les États a émergé avec la conception 'idéaliste' des relations internationales. L'idée principale de cette vision reposait sur la nécessité de la prévention de toute guerre probable, prenant en compte les effets dévastateurs de la Grande Guerre. La création d'une organisation internationale vouée au maintien de la paix - la Société des Nations (SDN)- avait été l'idée ardemment défendue en particulier par Woodrow Wilson considéré comme l'un des représentants de l'idéalisme classique. Cette vision a donc encouragé la fondation des Nations Unies en 1945 et l'accroissement du développement de programmes couvrant tous les domaines de l'activité humaine.

D'après l'approche 'idéaliste', la société internationale est constituée d'États indépendants qui rivalisent pour la défense de ses intérêts propres. Cependant, les relations internationales peuvent être civilisées et pacifiées par l'institutionnalisation avec le développement du droit international et des organisations internationales qui contribuent au règlement des conflits et au renforcement de la coopération entre États. Il est de même accentué que le développement de la communication et des échanges constituent les principales assurances pour l'atteinte à cet objectif.[3]

---

[2] M.-C. Smouts, **Les Nouvelles Relations Internationales**, Paris, Presses de Sciences Po, 1999, p.136
[3] I. Clark, **Globalization and International Relations Theory**, New York, Oxford Univ. Press, 1999, p.24

Néanmoins, lorsque les lois internationales ont été terriblement violées dans les années 1930, cette volonté a été largement non-justifiée. De plus, suite à la seconde guerre mondiale, la loi internationale n'était plus considérée comme le garant de l'ordre international mais comme protecteur d'un ordre social international au service des besoins humains.

Depuis quelques décennies, il est possible de constater qu'il s'agit d'une prolifération de demande de loi internationale dans tous les domaines de l'activité humaine, de la croissance de juridiction dans la société internationale. Cette situation est amplement favorisée par le développement des activités multilatérales sur l'agenda international, tels que les sommets, les conférences, les assemblées générales, les conseils exécutifs, qui sont généralement conclus sur une déclaration finale au statut incertain. Cependant, comme en fait la remarque Marie-Claude Smouts, cette incertitude donne lieu à l'avènement de situation où il s'agit d'une manque de netteté, en particulier dans le cas des engagements plus politiques que juridiques. La frontière entre droit et non-droit est devenue floue étant donné que le contenu normatif des textes est incertain. Le droit n'énonce plus de certitudes, il s'installe sur des à-peu-près, ce n'est pas l'absence de règles mais une catégorie particulière de règles qui est formée[4]. De ce fait, les obligations sont devenues ouvertes à une reformulation réalisée en fonction du besoin de chacun. Sur les effets de cette diversification du droit internationale les juristes sont divisés. Les débats qui se produisent dans ce cadre se présentent sur la notion de « *soft law* ». Pour les uns, il s'agit d'une relativité du droit international qui reflète l'état de la société internationale, il ne s'agit pas de vérité juridique unitaire dans une société multiculturelle et pour les autres, c'est un outil dynamique du développement du droit exprimant une prise de conscience par la communauté internationale du besoin d'une certaine réglementation. Bien que ces débats se concentrent sur les lacunes du droit international, il est difficile d'attendre du droit international de résoudre tous les problèmes surgis au sein de la société internationale[5].

[4] M.-C. Smouts, **op. cit.**, p.140
[5] M.-C. Smouts, **op. cit.**, p.141

2. La théorie des régimes

Jusqu'aux années cinquante, la réflexion sur l'ordre international et sur la coopération entre les États reposait donc sur la notion de droit international. Cette approche a été transformée à la suite de la deuxième guerre mondiale avec la diffusion de l'internationalisme libéral qui implique la période du « libéralisme encadré (*embedded liberalism*)[6] » des années 1945-1970, succédée par la mondialisation économique. Tout au long de cette période, de différentes approches ont été apportées pour l'idée de coopération internationale mais c'est le concept de 'régimes internationaux' apparu dans les années soixante-dix qui est devenu l'origine des débats relatifs à la problématique de l'ordre dans le système international anarchique[7]. La théorie des régimes s'inscrit dans le courant « néo-institutionnaliste libérale ». Différents courants ont apporté des approches pour la théorie des régimes, mais ce sont celles du courant néo-réaliste qui ont été le plus affluent. Dans ce travail, ce sont les visions de ces deux courants sur la théorie des régimes qui seront étudiés.

Toutefois, la question qui se pose est celle qui cherche à savoir pourquoi ce fut dans les années soixante-dix que les théoriciens ont commencé à se concentrer sur la formation des régimes internationaux. Une approche qui tente à y répondre est celle de la théorie de la stabilité hégémonique, théorie réaliste émise par Charles Kindleberger[8]. Cet auteur, analysant la grande dépression économique de l 'entre deux guerres, conclut que celle-ci est due au fait que chaque pays agissait unilatéralement, étant donné l'absence de règles du jeu, faute de puissance hégémonique capable de respecter de telles règles. D'après cette théorie, non seulement l'absence, mais même le déclin de la puissance prédominante mettent en danger la stabilité économique internationale, ce qui fait référence au contexte politique international des années soixante-dix où surgissent les crises monétaires et énergétiques, avec le déclin relatif des États-Unis défiés par l'Organisation des Pays Exportateurs de Pétrole (OPEP) et rattrapés par la Communauté européenne et le Japon. Autrement dit, d'après la théorie de la stabilité hégémonique, le déclin des

---

[6] L'expression est de J.G.Ruggie, 'International Regimes, Tranactions and Change. Embedded Liberalism in the Postwar Economic Order ' citation dans J. Nye and J. Donahue, **Governance in a Globalizing World**, Cambridge, Brookings Institution Press, 2000, p.22

[7] D. Battistella, **Théories des Relations Internationales,** Paris, Presses de Sciences Po, 2003, p.369

[8] C.Kindleberger, **The World in Depression.1929-1939**,Berkley,California University Press,1973

États-Unis annonce une remise en cause des régimes internationaux établis après la seconde guerre mondiale. Les institutionnalistes néo-libéraux et les néo-réalistes ont tous deux réagis à cette évolution. D'après la théorie néo-libérale institutionnaliste, proposant d'expliquer les régimes internationaux non pas en terme de puissance, mais en terme d'intérêt, le déclin de l'hégémonie ne signifie pas nécessairement la fin de la coopération[9]. Ceci a été contesté par les néo-réalistes, affirmant que la perte du statut hégémonique des États-Unis donnera lieu au changement de l'équilibre des puissances et que les principes libéraux qui gouvernent les régimes établis par les États-Unis seraient défiés. Néanmoins, bien qu'ils aient des directions différentes, ces deux visions consentent sur le besoin d'une conception de régime théorique plus recherchée.

a. Une définition des régimes internationaux

L'établissement d'une définition d'un régime international a été l'objet de longs débats dans la discipline des relations internationales tout au long des années quatre vingt. D'après Stephen Krasner, « *Les régimes internationaux sont des ensembles explicites ou implicites de principes, de normes, de règles et de procédures de prise de décision autour desquels les attentes des acteurs convergent dans un domaine donné des relations internationales. Les principes sont les croyances aux faits, à la causalité et à la rectitude. Les normes sont les standards de comportement définis en terme de droits et d'obligations. Les règles sont des prescriptions et proscription spécifiques vis-à-vis d'une action. Les procédures de décision prévalent les pratiques dans la mise en place et l'exécution des choix collectifs* [10]».

L'établissement de cette notion a apporté plusieurs questions avec elle, dans un premier elle interroge la différence entre les régimes internationaux et les organisations internationales ; et par la suite, les situations durant lesquelles il est possible de parler d'ensembles implicites de principes, de normes, de règles et de procédures de prise décision.

---

[9] R. Keohane, **op.cit.**

[10] S.Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables", in S. Krasner (ed.), **International Regimes**, Ithaca, USA: Cornell University Press, 1983, p.2.

Dans son ouvrage, Les Organisations Internationales (1995), Marie-Claude Smouts énonce que « *toutes les organisations internationales sont des régimes, mais tous le régimes ne donnent pas naissance à des organisations* »[11]. Dans un autre sens, les États coopèrent aussi bien de façon informelle que de façon formelle ; il n'est pas nécessaire de créer une institution bureaucratisée avec un siège, du personnel, etc., pour coordonner des actions dans un domaine donné, même si souvent, des organisations internationales donnent lieu à la concrétisation des régimes : en effet, l'Organisation Mondiale du Commerce (OMC) s'est substitué en 1994 au régime international commerciale du 'General Agreement on Tariffs and Trade' (GATT), de même la Conférence sur la Sécurité et la Coopération en Europe (CSCE) de 1975 s'est transformée en l'Organisation de la Sécurité et la Coopération en Europe (OSCE) après la fin de la guerre froide.

En ce qui concerne la notion d'ensemble « implicite » de principes, normes, règles et procédures de prise décision, Marie-Claude Smouts renvoie à l'existence de régimes tacites, par opposition aux régimes classiques : ainsi le régime monétaire international des taux de change fixes de Bretton Woods a été un régime classique, prescrivant explicitement aux États-membres tel comportement ; à l'inverse, le régime des taux de change flottants qui lui a succédé est un régime tacite, du point de vue qu'il est à l'origine d'une entente régulière entre États pour les comportements à adopter en matière de régulation monétaire, sans qu'il n'y ait cependant de règles de comportement explicites en la matière. [12]

b. La théorie des régimes et les débats néo-libéraux institutionnalistes et néo-réalistes

Les théoriciens de l'institutionnalisme néo-libéral partagent des objectifs similaires avec ceux du néoréalisme. Ils cherchent à expliquer les régularités des comportements en examinant la nature décentralisée du système international. Dans les analyses de deux approches, l'État est considéré comme acteur principal.

---

[11] M.-C.Smouts, **Les Organisations Internationales**, Paris, Armand Collin, 1995, p.27
[12] **Ibid.**

La théorie néo-libérale institutionnaliste se base sur une analogie formée entre le marché économique et le système international. Le point de départ est que l'État est un acteur unitaire et rationnel, cherchant à maximiser ses intérêts donnés et définis en termes égoïstes. Ils n'en déduisent pas la nécessité pour un État de pratiquer une politique rejetant la coopération, car d'après eux, une telle politique peut produire des effets pervers, des résultats inférieurs à ceux théoriquement possibles[13]. Pour illustrer ces propos, ils ont recours à la théorie des jeux et particulièrement à l'analyse du jeu spécifique appelé « dilemme de prisonnier ». Appliqué aux relations internationales, le dilemme du prisonnier permet aux néo-libéraux d'établir le constat qu'il existe « des situations dans lesquelles les acteurs sont incités à ne pas agir de façon unilatérale, où un calcul rationnel égoïste les amène à préférer des actions multilatérales parce que l'action unilatérale est susceptible de mener sur des résultats indésirables ou sous-optimaux »[14]. En d'autres termes, dans certaines situations, les États s'abstiennent à faire cavalier seul alors que la coopération leur aurait permis d'obtenir une plus grande satisfaction de ses intérêts. D'après Keohane, ce sont les barrières à l'information et à la communication en politique qui empêchent la coopération et la création de la discorde même lorsque des intérêts communs existent[15]. Les États préfèrent agir seul lorsqu'ils ne savent pas comment agissent les autres États.

Keohane affirme que la création d'institutions internationales, de régimes internationaux facilitent la coopération et réduisent l'incertitude[16]. D'après l'explication néolibérale, les régimes internationaux existent parce qu'ils facilitent la coopération souple au sein d'un système politique décentralisé et que par là même ils jouent une fonction importante pour les gouvernements. Ils leur permettent d'atteindre des objectifs qui autrement seraient hors de portée, en facilitant les accords intergouvernementaux. Ils augmentent les possibilités de coopération en réduisant les coûts de transactions conformes au principe des régimes. Ils créent les conditions propices aux négociations multilatérales ordonnées, aux comportements étatiques légitimes. Ils facilitent la symétrie et améliorent la qualité de l'information

---

[13] D.Battistella, **Théories des Relations Internationales**, Paris, Presses de Sciences Po, 2003, p.376
[14] A. Stein, "Coordination and Collaboration. Regimes in an Anarchic World" (1982), dans S.Krasner (ed.) **International Regimes**, cité dans D.Battistella, **op.cit.**, p.379
[15] R. Keohane, **op.cit**, p.69
[16] **Ibid**. p.97

dont disposent les gouvernements[17]. Le dilemme du prisonnier permet de même aux néo-libéraux institutionnalistes de démontrer que dans tous les cas, les participants ont intérêt à choisir la coopération plutôt que la défection et que la condition essentielle pour l'apparition de coopération est que les acteurs aient suffisamment de chances de se rencontrer à nouveau pour que l'issue de leur prochaine interaction leur importe[18]. La présence d'une puissance hégémonique n'est donc pas nécessaire dans ces conditions pour créer des régimes internationaux ; ceux-ci sont les résultats d'un optimum collectif. D'après la vision néo-libérale institutionnaliste, à long terme, le comportement coopératif est donc la meilleure stratégie possible, lorsque les États sont dans un jeu d'échanges répété où ils sont tantôt gagnants tantôt perdants et que de toute façon ils auront à rencontrer les autres, ils n'ont pas intérêt à se retirer du jeu et faire cavalier seul. Néanmoins, la perspective des néo-réalistes pour l'institutionnalisation du système international est plus pessimiste.

D'après la vision néo-réaliste, ce n'est pas seulement à la lacune de l'établissement d'un gouvernement central dont fait référence l'anarchie, mais aussi à la difficulté qui émerge en ce qui concerne le renforcement des accords par un pouvoir central. De ce fait, les États se trouvent face au risque où la violation des règles par les autres États n'est possible de contourner puisqu'il n'existe aucune autorité chargée de l'éviter.[19] D'une part, en raison de crainte de violation des règles, les États sont menés à perpétuellement évaluer leurs positions dans le système international au cours des arrangements coopératifs. D'autre part, d'après Kenneth Waltz, la coopération entre les États est difficile car dans la condition d'anarchie, « *le gain relatif est plus important que le gain absolu* » et que « *l'objectif fondamental des États dans une relation quelconque est d'éviter que les autres atteignent des avances dans leurs capacités relatives* »[20].

Les néoréalistes expliquent la présence des régimes par la volonté de l'État hégémonique pour créer et promouvoir ses intérêts à long terme. Ils concluent que la persistance des régimes est liée à la présence d'une puissance hégémonique et que le

---

[17] **Ibid.**,p.63
[18] **Ibid.**
[19] K. Waltz, **Theory of International Politics** (Reading, USA:Addison-Wesley,1979) cité dans R.Keohane, "Neoliberal Institutionalism. A Perspective in World Politics", dans R.Keohane, **International Institutions and State Power.Essays in International Theory**, Boulder, Westview, 1989, p. 21
[20] **Ibid.**,p. 23

déclin de celui-ci, donnerait lieu au déséquilibre de la puissance dans le système internationale, d'où surgira une difficulté de faire appliquer les régimes.

En partant de l'idée que ce sont les attentes des États qui déterminent leur capacité de coopérer, les néoréalistes reprochent à la théorie néo-libérale institutionnaliste de se focaliser sur l'économie internationale pour l'explication de la coopération et des régimes internationaux et de sous-entendre les enjeux relatifs à la sécurité militaire, ce qui reste insuffisant pour la réflexion des attentes[21].

Cependant la notion de « interdépendance complexe » développée par J. Nye et R. Keohane dans les années 1970, remplit la lacune en ce qui concerne le rôle des attentes et de la puissance économique et militaire dans la politique internationale.

Dans l'analyse de coopération internationale, les théories des régimes jouent un rôle important. Comme le souligne Marie-Claude Smouts, le concept de régime permet de désigner et d'étudier des formes de régulations non inscrites dans des textes juridiques qu'il est possible de constater dans la vie internationale. Le concept de régime est aujourd'hui de plus en plus substitué avec celle d'institution. Robert Keohane définit la notion d'institution comme « *un ensemble durable et cohérent de règles formelles et informelles qui prescrivent les comportements, contraignent l'activité et façonnent les attentes des acteurs internationaux* ». D'après cet auteur, les institutions pour une coopération sont représentés sous l'une des formes suivantes : organisations intergouvernementales ou non gouvernementales, régimes internationaux et conventions. [22] Il en est de même pour le multilatéralisme[23] souvent considéré comme synonyme d'institution et de régime.

---

[21] **Ibid.**, p.25
[22] **Ibid.**, p. 3
[23] Le multilatéralisme désigne une forme institutionnelle de coordination des relations entre trois ou plusieurs États sur la base de principes généraux de conduite.

3. La gouvernance mondiale et le multilatéralisme

La coopération multilatérale a été remarquablement étendue, sans précédent, dans la deuxième moitié du XX^{e} siècle. Avec la conférence Bretton Woods en 1944, les régimes clés pour la gouvernance ont été lancés par les différents ministres des pays développés. Les ministres chargés des affaires économiques ont développé le GATT; ceux chargés dea affaires financiares ont démarré le FMI; ceux d'affaires étrangères et de défense se sont réunis pour l'OTAN. [24] Du point de vue de la perspective de la coopération multilatérale, ces modèles sont considérés comme un grand succès. Les États ont conçu les régimes internationaux et ont cédé une partie de leur puissance aux organisations interétatiques afin de faciliter la coopération pour la gestion des affaires dans un domaine spécifique, où ils cherchaient à atteindre leurs propres objectifs dans le cadre d'intérêt commun.

Cependant, ce mode de coopération, en termes de régimes, a engendré une augmentation significative de l'interdépendance, aujourd'hui sous forme de mondialisation. En effet, les régimes s'appliquent au cas par cas, domaine par domaine (*issue area*), ce qui limite de penser la mondialisation dans sa complexité. Cette approche demeure insuffisante pour répondre aux dynamiques du système mondial contemporain. Elle ne permet pas de considérer les situations floues et les effets provisoires qui surviennent. Le concept de gouvernance mondiale, apparu récemment dans la discipline des relations internationales, cherche à répondre à ces lacunes et compléter celui du régime[25].

a. La définition de la gouvernance

Dans son ouvrage, *Governance Without Government* (1992), James Rosenau caractérise la gouvernance comme un ensemble de mécanismes de régulations existant dans une sphère d'activités données et qui fonctionnent alors même qu'ils

[24] J. Nye and J. Donahue, **op. cit.**, p.28
[25] M.-C. Smouts, **Les Nouvelles Relations Internationales,** Paris, Presses de Sciences Po, 1999, p.149

n'émanent pas d'une autorité officielle[26]. Cette approche mais l'accent sur le fait que la gouvernance réside dans les unités du système, elle renvoie donc à la multitude d'acteurs qui ont fait irruption sur la scène internationale ces dernières années. Cette définition de gouvernance est très proche de la notion de régime, mais elle est plus vaste et plus globale. Dans la notion de régime, la coopération internationale réside sur des domaines précis et isolés, alors que la gouvernance prend en compte les relations entre les différents domaines. Une autre définition de la gouvernance est apportée par la *Commission on Global Governance*[27] : c'est « la somme des différentes façons dont les individus et les institutions, publics et privés, gèrent leurs affaires communes. C'est un processus continu de coopération et d'accommodement entre des intérêts divers et conflictuels. Elle inclut les institutions officielles et les régimes dotés de pouvoirs exécutoires tout aussi bien que les arrangements informels sur lesquels les peuples et les institutions sont tombés d'accord ou qu'ils perçoivent être de leur intérêt.[28]»

D'après cette définition, la gouvernance est considérée comme un processus continu de la gestion des affaires internationales. Il ne s'agit pas d'un aboutissement à un résultat fixe face à un problème précis, c'est ce qui distingue la gouvernance des régimes. La régulation n'est pas encadrée par un corps de règles préétablies, elle se fait de manière simultanée par des processus permanents d'échanges, de conflits, de négociations.

Le transnationalisme, qui n'est pas une notion récente, a permis de montrer les configurations complexes de coalitions entre différents acteurs. La gouvernance permet de décrire les modes de gestion des affaires d'intérêt mondial reliant des acteurs hétérogènes n'ayant ni les mêmes capacités ni les mêmes légitimités.

---

[26] J.N.Rosenau, E.O.Czempiel, **Governance Without Government: Order and Change in World Politics**, Cambridge, Cambridge University Press, 1992, p.4

[27] Cette commission s'est réuni suite à la chute du mur de Berlin, leur objectif principale était d'apporter une approche pour l'organisation de la société internationale au cours la période après-guerre froide.

[28] **The Commission on Global Governance, Our Global Neighborhood**, Oxford, Oxford University Press, 1995 citation dans M.-C. Smouts, **Les Nouvelles Relations Internationales**, Paris, Presses de Sciences Po, 1999, p.150

b. Les Intervenants dans la gouvernance

La gouvernance est donc mise en œuvre par des acteurs et des mécanismes d'autorégulation différents qui recomposent le monde actuel dans les domaines les plus divers. A l'adjonction des États, firmes multinationales, O.N.G., réseaux de solidarité, de nouveaux acteurs échappant au contrôle du pouvoir exécutif et législatif des États avec les chutes rapides des coûts de communication qui ont réduit les barrières, sont impliqués dans les différentes activités de la gouvernance. Ces acteurs sont capables de jouer des rôles critiques indépendants ou quasi-indépendants dans ce mécanisme où ils réalisent généralement leurs activités en tant que partie des réseaux auxquelles ils appartiennent.

La notion de réseau complète celle de gouvernance en considérant les liens et les interactions existant entre les acteurs. L'approche en terme de réseau met l'accent sur le rôle des individus, des groupes sociaux, des mécanismes inter-organisationnels dans la structuration de l'espace mondial. Elle montre comment des espaces de mobilisation traversant les espaces nationaux, sont construits et investis par des acteurs privés prenant en charge l'allocation des ressources, la diffusion des valeurs et des pratiques. [29]

Il est donc important de ne pas considérer les relations entre ces acteurs dans la gouvernance de manière isolée. Les activités des États et des organisations interétatiques sont souvent complétées par celles des acteurs privés et des acteurs non gouvernementaux. Les sociétés transnationales fournissent leurs propres formes de gouvernance afin de répondre à l'absence de gouvernance dans un domaine précis. Dans certaines situations, les fonctions législatives des États sont substituées par les activités des firmes transnationales. De manière similaire, les firmes peuvent contourner les institutions juridiques des États d'accueil dans le cas où ils les perçoivent lents ou corrompus. De plus en plus, des contrats commerciaux sont établis avec des dispositions pour arbitrage commercial afin d'isoler les firmes le plus possible des tribinaux nationaux ; et dans ce but, la Chambre de Commerce

[29] B. Badie, M.-C. Smouts, "L'International Sans Territoire : Introduction", **Culture et Conflits**, No.21-22

Internationale joue un rôle important. Plusieurs élaborations de standards critiques sont originaires du secteur privé. Dans le cyberspace par exemple, les codes de conduite réalisés pour des buts commerciaux par les firmes ont des impacts importants sur des sujets comme la protection de la vie privée, les droits de propriété et les droits d'auteurs. Dans ce domaine, les États perdent leur contrôle sur les règlements et le *rule-maker* efficace devient le cyberespace.[30]

Dans certains cas, les États préfèrent se tourner vers une organisation non gouvernementale qu'une organisation interétatique. En particulier lorsqu'il s'agit de la gestion de problèmes se développant de manière rapide où les États considèrent que l'approche massive et lente des organisations interétatiques serait insuffisante pour répondre à ce genre de problème. Effectivement, dans le cas de la gestion des noms de domaines sur Internet par exemple, l'État américain a favorisé la fondation de l'organisation ICANN[31], un O.N.G. qui procède ses activités avec les firmes du secteur privé.

La collaboration des O.N.G.[32] avec les États et les organisations interétatiques bien que ne soit pas récent, est devenu plus fréquent au cours de la dernière décennie du XX^{e} siècle. Les O.N.G. s'imposent aux États et aux organisations interétatiques comme des partenaires indispensables, parfois même spontanément sollicités. Leurs activités principales s'articulent comme apporter des services et informations techniques qu'ils ont pu développer dans un domaine particulier, soit du fait d'une expérience de terrain, ancienne et approfondie, soit par leur capacité d'études savantes faisant autorité, ou bien soit à une combinaison de ces deux facteurs. Face aux États et aux organisations interétatiques, les O.N.G. qui fournissent des services sont capables de définir des priorités, dégager des solutions, susciter l'engagement. Dans ce cadre, les groupes d'experts techniques ou les groupes professionnels offrent des analyses et des informations sophistiquées influençant les négociations. [33]

---

[30] J. Nye and J. Donahue, **op. cit.**, p.30

[31] ICANN (Internet Corporation for Assigned Names and Numbers), association responsable de la régulation des noms de domaines sur Internet et de l'enregistrement des adresses.

[32] D'après la définition donnée par l'Union des Associations Internationales, un O.N.G. est une association composée de représentants appartenant à plusieurs pays et qui est internationale par ses fonctions, la composition de sa direction et les sources de son financement. Elle n'a pas de but lucratif et bénéficie d'un statut consultatif auprès d'une organisation intergouvernementale.

[33] J.Laroche, **Politique Internationale**, Paris, L.G.D.J., 2000, p.135

En outre, dans certains cas, les O.N.G. agissent dans les lobbying et les mobilisations politiques, ce qui leur donnent un rôle important comme détecteurs de mécontentement ou d'insatisfactions. Dans certaines situations, les influences qu'exerce un O.N.G. sur l'agenda d'un certain État, peut être en faveur d'autres États; comme dans le cas où l'organisation *Transparency International* a présenté ses résultats sur la corruption. Néanmoins, dans d'autres cas, les O.N.G. peuvent de même former des coalitions avec certains États en contrepartie d'autres ; comme dans le cas du Traité des Mines Terrestres où le Canada a retiré un soutien contre les Etats-Unis[34].

La gouvernance qui donne donc une large place large aux acteurs sociaux, permet aux différentes composantes d'une société d'exercer leur pouvoir d'expression et de critique. Une action publique internationale qui provient de la diversité des acteurs en relation est formée par la communication des unes avec les autres.[35]

En effet, les institutions internationales affrontent certaines revendications provenant du pouvoir public et en particulier du secteur commercial. Celles qui ont apporté le plus de retentissement ont été la demande croissante de transparence et le manque de démocratie au sein de ces organisations. L'incitation de la transparence et de la remise de compte, sans avoir à exposer tous les accords à une déstructuration, constitue un problème fondamental confronté par la coopération multilatérale et la gouvernance démocratique. Les acteurs sociaux exercent des pressions dans ce but. De plus, la création d'Internet a favorisé l'augmentation du nombre des O.N.G. et la communication entre ces acteurs, donc la société civile mondiale[36] est davantage capable de mobiliser son pouvoir d'expression; les protestations à Seattle en constituent un exemple. Joseph Nye interprète cette face de la gouvernance comme une évolution dramatique de l'*activité sociale transnationale.*

---

[34] J. Nye and J. Donahue, **op.cit.,** p.33

[35] M.-C. Smouts, **Les Nouvelles Relations Internationales**, Paris, Presses de Sciences Po, 1999, p.151

[36] La société civile mondiale est définie par M.Kaldor comme la description d'un processus à travers lequel les individus ont la possibilité de débattre, influencer et négocier un contrat social en cours ou bien un ensemble contrats avec les centres d'autorité politiques et économiques. En d'autres termes, la société civile mondiale comprend toutes les institutions formelles et informelles auxquelles les individus peuvent s'adhérer et par lesquelles leur voix peut être procédé par les décideurs. Dans M. Kaldor, **Global Civil Society**, Cambridge, Polity, 2003.pp78-79

c. La coopération entre les trois secteurs

La gouvernance permet de considérer les possibilités de dialogue et de participation commune entre plusieurs acteurs autour de problèmes d'intérêt collectif. Dans ce contexte, la gestion des affaires mondiales est réalisée par des acteurs variés, de capacité et de légitimité différent, mais chacun ayant des intérêts vis-à-vis du sujet. Dans le domaine de l'environnement, par exemple, la coopération fait intervenir des acteurs aussi divers que des experts scientifiques, les O.N.G. de défense de l'environnement, les entreprises industrielles, les compagnies d'assurances, les administrations techniques, les diplomates, les responsables politiques. La gouvernance permet de décrire ce type de configuration nécessitant les possibilités de dialogue et de participation commune entre différents acteurs autour de problème d'intérêt collectif.

Les activités des organisations internationales sont devenues amplement liées aux alliances que leurs secrétariats et les États dominants établissent avec les acteurs critiques du secteur privé et les organisations non gouvernementales.

Une modalité qui devient de plus en plus explicite dans la coopération internationale c'est la coopération entre les trois secteurs ; les firmes transnationales, les organisations non gouvernementales et les organisations internationales. Le modèle '*global compact*' qui a été proposé par Koffi Annan illustre bien ce cas. Ce dialogue de partenariat a été initié, en juillet 2000, entre l'O.N.U. et le secteur privé, notamment avec les multinationales, les syndicats et les O.N.G. Dans cet espace informel de rencontre et de travail, se sont associées une cinquantaine de firmes et une dizaine d'O.N.G. avec l'objectif affiché de lutter contre les dérives de la mondialisation, en matière de droits de l'homme, de droits sociaux et d'environnement[37]. Il existe d'autres exemples illustrant ce cas, comme la Commission Mondiale sur les Barrages, qui consistait de quatre délégués d'État, quatre de l'industrie privé et quatre d'O.N.G.

[37] www.unsystem.org

Les processus de la coordination pour la gestion des domaines variés de la politique mondiale qui prennent lieu entre les organisations interétatiques, les acteurs du secteur privé et les O.N.G. se présentent sous forme de relation compétitive et coopérative. Notablement, dans la plupart de ces arrangements, les capacités 'soft législatives', c'est-à-dire l'élaboration des '*soft law*' et des normes, se développent plus rapidement que les 'hard législatives' ou bien les capacités exécutives[38]. La notion de gouvernance permet donc d'envisager de nouveaux modes de mise en place de normes sociales et juridiques par la construction d'un droit transnational réalisé par les acteurs privés afin d'établir la concurrence et la bonne marche des affaires. Il est important de souligner que ces lois sont souvent définies par les acteurs dominants.

Comme les régimes, l'approche de gouvernance repose sur le *problem solving,* la nature de la régulation produite et sa convenance aux problèmes de fond ne sont pas mises en question. L'idéologie sur laquelle elle se base est aussi la satisfaction du bien commun qui est censée provenir spontanément de l'échange librement consenti. A cet égard, Robert Cox propose une nouvelle forme de coopération avec le projet du « nouveau multilatéralisme ». Son point de départ est que les institutions ne sont pas adéquates et qu'il n'existe pas de critères communs pour la gestion de la mondialisation et des nouveaux défis planétaires, qu'il ne s'agit plus d'essayer de résoudre les problèmes dans un système où les États resteraient des acteurs dominants. Avec le multilatéralisme qui a été construit par le « haut », les organisations et les institutions ont agi dans cet objectif mais avec un nombre limité d'acteurs non étatiques. Désormais avec le « nouveau multilatéralisme » un ordre mondial est construit en reliant tous les acteurs par le « bas » en repensant la théorie politique, le droit et les relations internationales[39].

Sur la dimension réactive de la coopération internationale un nouvel acteur s'avère important dans l'institutionnalisation des rapports internationaux. Ce sont les communautés de savoir (les communautés épistémiques) conçus en tant qu'un groupe transnational ayant des 'croyances' avec des valeurs communs, des modèles de causalité et des critères de validation, aussi bien qu'un objectif politique qui

---

[38] J. Nye and J. Donahue, **op. cit.**, p.28

[39] M.-C. Smouts, **Les Nouvelles Relations Internationales**, Paris, Presses de Sciences Po, 1999, p.154

agissent dans certains cas de la coordination politique internationale dans lesquels sont présents des incertitudes techniques. Leurs moyens de coopérer avec les États se réalisent par les processus de communication, de circulation des idées et d'apprentissage plutôt que par les jeux de pouvoir.

B. Les communautés épistémiques et l'internationalisation de l'intervention experte

L'évolution de l'expertise comme caractéristique de la gouvernance contemporaine n'est pas nouvelle. Bien que l'existence des experts soit loin d'être un phénomène récent, vu que dès le XVI[e] siècle des individus détenteurs de savoir étaient déjà sollicités pour « *statuer sur des faits...et tenir sur eux un discours de vérité* »[40], l'internationalisation de l'intervention experte apparaît comme caractéristique de notre époque. Aujourd'hui, les autorités politiques sont menées à confronter des incertitudes provenant de sources variées. Parmi les facteurs donnant lieu à la résurgence de ces incertitudes, il est possible de citer premièrement la complexité et la nature technique des problèmes considérés dans l'agenda international –tels que les problèmes monétaire, macroéconomique, technologique, environnemental, sanitaire, démographique–, mais aussi la complexité du système politique international actuel, ce qui est due à l'augmentation du nombre d'acteurs et de leurs interactions, et finalement l'expansion de l'économie globale.

1. Les experts dans la politique internationale

a. Les caractéristiques

Les autorités politiques forcé à faire face à une nouvelle gamme de problèmes de niveau plus étendus, autant en terme de quantité que de complexité et tenu compte que ceux-ci s'alignent à un niveau global, font de plus en plus appel aux experts, venant de différents domaines, afin d'éclaircir les incertitudes qu'ils affrontent, de façon à comprendre les problèmes présents et delà anticiper les courants à venir. Selon la définition de Christiane Restier-Melleray, l'expert présente les

[40] P. Fritch, « Situations d'expertise et de socialisation des savoirs » in : Cresal (Ed.), **Table Ronde**, 14-15 mars 1985, multigraphié, pp.20-21.

caractéristiques suivantes: c'est un individu ou un groupe d'individus ; il ne tient pas de lui-même sa légitimité, celle-ci lui est conférée par une instance d'autorité qui le mandate ; il est choisi en fonction de la compétence qui lui est reconnue ; son activité, faite d'examens, de constats, de vérifications, d'appréciations, d'estimations, est destinée à apporter à son mandataire des éléments permettant la formulation d'un jugement ou d'une décision ; et, enfin, le mandataire est extérieur à l'instance commanditaire de la mission et indépendante de celle-ci[41].

Les experts techniques partagent de plus en plus le pouvoir avec les autorités publiques, les élites traditionnelles économiques et politiques. Autrement dit, l'expert contemporain ne joue pas sur le même registre qu'il y a vingt ans, comme le souligne Luc Rouban. « L'expert des années quatre-vingt-dix n'est pas un administrateur, ou un scientifique agissant comme un administrateur, mais un porte parole d'intérêts politiques, un stratège qui sait associer son problème à d'autres thèmes politiques pour appuyer ou contester les thèses officielles »[42]. On observe donc une instrumentalisation de la science qui n'est plus définie par la politique mais par une combinaison d'intérêts associatifs ou industriels[43]. En revanche, par la suite, Luc Rouban reprend l'idée que les élites politiques conservent toujours le pouvoir dans les processus décisionnels, mais en ajoutant qu'ils justifient de plus en plus leurs décisions sur la base des analyses techniques des experts avec lesquels ils forment une coalition.

Tout en s'alignant dans cette approche, la contribution terminologique de Peter Haas remplit une des lacunes dans cette littérature. Assumant que l'expert tient son autorité des liens impersonnels inscrits dans des savoirs constitués qui l'unissent à un collectif d'appartenance, son intervention n'est pas dissociable de la « communauté épistémique » à laquelle il appartient. Par ce terme Peter Haas désigne un réseau transnational de professionnels (économistes, juristes, médecins, physiciens, etc....) dont l'expertise est reconnue dans un champ de compétence déterminé. Unis par les mêmes connaissances, croyances, valeurs et méthodes, d'autant plus que ceux-ci

---

[41] C. Restier-Melleray, « Experts et expertise scientifique, le cas de la France », **Revue Française de Science Politique**, 1990, 40(4), pp.550-51.
[42] L. Rouban, **La Fin des Technocrates ?**, Paris, Presses de Sciences Po, 1998, p. 72
[43] **Ibid,** p.80.

partagent aussi une égale vision du monde[44]. Encore, selon l'approche de Haas, bien que les conditions systémiques actuelles imposent certaines contraintes sur les actions étatiques, il convient de limiter l'analyse du rôle de ces réseaux d'experts, qu'il nomme communautés épistémiques, en aide prêtée aux autorités étatiques sous forme de propositions de politiques spécifiques dans l'articulation des problèmes complexes, l'identification de leurs intérêts et des points saillants pour la négociation.

En effet, dans le cas étudié dans ce travail, où sont envisagées, au sein de l'Organisation pour la Coopération et le Développement (OCDE), les approches de solution apportées pour le problème de sécurité des systèmes d'information, les États membres, desquels les connaissances demeurent incompétents vis-à-vis du sujet de la sécurité des systèmes d'information, font appel à l'expertise des groupes. Durant les travaux, parmi les différentes communautés épistémiques de domaines variés, le Comité Consultatif Economique (BIAC, Business and Industry Advice Comity) apparaît en tant que conseiller principal dans le domaine des technologies d'information. Néanmoins, les complexités provenant du système international peuvent mener, dans certaines situations, les communautés épistémiques à devenir parties prenantes dans la coopération, alors que celles-ci étaient impliquées initialement en tant que conseiller dans le processus de prise de décision, ce qui est le cas du BIAC.

b. Les experts dans la formulation de politique

Afin de conceptualiser l'expertise dans la réalisation de politique, Claudio Radaelli propose quatre modes de formulation de politique (policy-making) qu'il obtient en croisant deux dimensions (figure 1.1). [45] Il s'agit premièrement de la dimension de la visibilité politique et deuxièmement de la dimension d'incertitude. La visibilité politique peut être de niveau élevé ou peut être de niveau bas en fonction de la familiarité du décideur vis-à-vis du problème, dans un autre sens elle varie par

---

[44] P. M. Haas, "Introduction: Epistemic Communities and International Policy Coordination", **International Organization**, special issue, 46 (1), hiv. 1992, pp. 1-35.

[45] C. M. Radaelli, "The Public Policy of the EU: Whither politics of expertise?", **Journal of European Public Policy**, 1999, 6(5), pp.762-764.

rapport à la fréquentation du problème. Il est possible de considérer ces deux dimensions comme des facteurs qui influencent la capacité des autorités politiques d'avoir recours à l'expertise. Selon cette approche conceptuelle, lorsque les problèmes politiques sont connus par l'opinion publique ou par les décideurs et que l'incertitude est basse, les prises de décision politique s'effectuent de façon envisageable, sans recours à une expertise. Au contraire, c'est-à-dire, lorsque les informations et les idées ne sont pas accessibles de manière évidente, donc lorsque l'incertitude est élevée, tout en laissant la dimension de visibilité politique du problème élevée, il est possible d'observer une activité grandissante des entrepreneurs politiques où les communautés d'experts peuvent gagner de l'influence. Ce mode de politique est en effet celui des 'communautés épistémiques'[46].

Le phénomène d'incertitude est donc central dans l'analyse en vue de la place des communautés épistémiques dans le processus de prise de décision. Ceci pour deux raisons principales ; d'une part, face à l'incertitude, notamment durant les périodes de crise ou face à un problème complexe, le pouvoir des autorités politiques tend à être défié par d'autres acteurs. Ceux-ci peuvent être d'autres acteurs étatiques lorsqu'il s'agit de problèmes de niveau internationale ou bien des acteurs non-étatiques prenant place dans les processus de décision. D'autre part, durant les situations de crise dont les causes ne sont pas clairement identifiables, donc où l'incertitude est présente, les procédures conventionnelles sont souvent suspendues, ce qui à la suite interrompe le fonctionnement des institutions prévalentes. Ainsi, l'incompétence des autorités politiques, en terme de pouvoir, mais aussi celle des institutions face à ce genre de situation ouvre la voie à de nouveaux modèles d'action, notamment la consultation des experts par les autorités politiques.

L'évaluation du processus de quête à l'expertise de la part des autorités politiques engendre deux différentes explications, qui, en fin de compte peuvent ne pas être totalement distinctes l'une de l'autre. La première, interprète ce processus comme aide provenant des experts aux autorités politiques pour la prise de décision dans le but de poursuivre leurs objectifs antérieurement déterminés. Tandis que l'autre suppose que la sollicitation d'expertise de la part des autorités politiques cède une

---

[46] **Ibid.**

place aux experts en tant qu'acteur dans le processus de décision. Par contre, la première explication n'exclut pas la possibilité que les résultats des travaux d'experts peuvent avoir un effet majeur dans certains cas où l'incertitude est présente du côté des autorités politiques, particulièrement dans la prévision de leurs propres intérêts politiques. D'autant plus, lorsque les autorités continuent à solliciter l'aide d'expertise, ce qui a tendance à produire peu à peu une délégation de l'autorité aux experts.

Ainsi, doit-on considérer les experts comme une nouvelle « élite du pouvoir scientifique » ? La définition qu'en donne Philippe Fritch est : professionnel réputé, l'expert est un individu ou groupe d'individus qui tire sa légitimité - non de lui-même- mais de l'instance d'autorité qui l'a mandate[47]. En effet qu'il s'agisse des maladies, des pluies d'acides, du nucléaire, ou comme dans notre cas, de la sécurité des systèmes d'informations, toute situation d'expertise suppose toujours, une demande d'expertise et donc un commanditaire : c'est aussi ce dernier qui fait l'expert.

Compte tenu de l'extension de l'interdépendance économique, donc de l'économie globale, le lien complexe entre les agendas domestiques et internationaux, est en quelque sorte devenu plus difficile pour les autorités à percevoir. Cette situation nécessite l'établissement d'une coordination de la politique des États. En ce qui concerne l'incertitude dans la coordination de la politique internationale, la requête d'information est largement liée à l'interdépendance des États dans leurs choix politiques afin d'acquérir une solution pertinente. Certes, cette forme d'incertitude suscite la demande d'une forme particulière d'information car elle ne consiste pas de l'estimation des attentes des autres ou bien de l'habilité de l'État dans la poursuite de son objectif, mais plutôt de la description du processus physique ou social, leur relation mutuelle avec d'autres processus, et certainement les conséquences de certaines actions. C'est pouquoi une expertise scientifique ou technique considérable devient nécessaire. Ces informations sont donc le produit des interprétations à propos des phénomènes physiques et sociaux.

---

[47] P. Fritch, **op. cit.**, pp.20-21.

Au plan international, lorsqu'un État, une organisation internationale ou tout autre acteur requière une collaboration avec des experts, la maîtrise d'un instrument de connaissance peut devenir une véritable ressource politique. Bien que les experts risquent d'être perçus comme instrument dans les processus de décision, leurs propres ressources est capable de les rendre suffisamment incontournables pour qu'ils soient en mesure d'être parties prenantes. Ils deviennent souvent capables de soumettre les politiques d'États, et ils s'impliquent de manière décisive dans les enjeux globaux.

Peter M. Haas en arrive aussi à ce type de conclusion, dans son analyse du cas de la signature et du contenu du Protocole de Montréal (1987)[48] relatif à l'interdiction des Chlorofluorocarbones (C.F.C.), les experts n'avaient-ils pas simplement fait emploi de conseillers, d'aides à la décision mais ils étaient au contraire apparus plusieurs fois comme les inspirateurs et les négociateurs de la politique. Toujours dans cette problématique, Raymond Hopkins a analysé le rôle des experts qui furent à l'origine d'une nouvelle politique en matière d'aide alimentaire, que les pays développés, les organisations internationales et les O.N.G. concernées ont ensuite mise en œuvre[49].

Toutefois, comme plusieurs études l'ont démontré, les autorités politiques assument toujours garder le contrôle, même en situation de délégation d'autorité au niveau d'expertise. En revanche, l'augmentation de l'incertitude associée au niveau de la gouvernance internationale, a poussé les autorités à recevoir « des recommandations », qui souvent ont abouti en coopération.

c. Les experts en tant que membre de réseaux transnationaux : les communautés épistémiques

On constate donc que de plus en plus, l'usage international de la notoriété des experts travaille à modifier l'autorité des États. Ces phénomènes révèlent des acteurs étatiques de plus en plus contestés par des individus capables d'agréger leurs actions

[48] Le 16 septembre 1987, le Protocole de Montréal qui fut signé par 24 pays, était la première tentative de coopération mondiale pour résoudre le problème de l'appauvrissement de la couche d'ozone rendu tout particulièrement sensible par la découverte, en 1985, d'un trou de la couche d'ozone au-dessus du continent antarctique. Les pays signataires s'engagèrent alors à renoncer à l'emploi de substances tel que les Chlorofluorocarbones responsables de l'appauvrissement de la couche d'ozone.

[49] R. F. Hopkins, "Reform in the International Food Aid Regime: the Role of Consensual Knowledge", **International Organization**, special issue, 46 (1), hiv. 1992, pp. 225-264.

en une action collective aux effets parfois majeurs. Encore convient-il de les envisager, non pas comme des entités autonomisés mais plutôt comme des acteurs immergés au sein des réseaux nationaux et transnationaux.

Il est nécessaire de reprendre la définition de communauté épistémique de Peter Haas afin de distinguer le regroupement des experts pour une action collective. Une communauté épistémique est un réseau de professionnels disposant d'une compétence reconnue dans un domaine particulier et qui revendiquent avec autorité leur connaissance politique dans ce domaine. Même si une communauté épistémique réunit des professionnels de disciplines d'origines variées, ceux-ci partagent : 1) une même croyance dans un ensemble de normes et de principes qui permet de définir une base raisonnée de valeurs pour l'action sociale des membres de la communauté; 2) les mêmes croyances de causalité qui découlent de leur observation des pratiques responsables des principaux problèmes qui se posent dans leur domaine et qui permettent de clarifier les multiples liaisons pouvant exister entre les actions politiques possibles et les résultats désirés; 3) les mêmes notions de validité, c'est-à-dire des critères intersubjectifs et définis de manière interne pour mesurer le poids et la validité d'une connaissance dans leur domaine de compétence; et 4) une même initiative politique, c'est-à-dire un ensemble de pratiques communes associés à un ensemble de problèmes vers lequel leur compétence professionnelle est dirigée, sans qu'il y ait probablement de conviction que le bien-être humain s'en trouvera amélioré "[50].

Les membres des communautés épistémiques possèdent non seulement un ensemble de croyances de causalité et des principes communs, mais aussi une notion de validité et entreprise de politique commune. Leurs revendications d'autorité, dans un domaine particulier sont basées sur la reconnaissance de leur expertise dans ce domaine en compte. D'après P. Haas, ce sont précisément par ces caractéristiques indiquées ci-dessus que sont distingués les communautés épistémiques des autres groupes intervenant dans la coordination politique. Les communautés épistémiques ne consistent pas seulement d'experts en sciences naturelles, mais aussi de ceux en sciences sociales et de tout autres individus venant de différentes disciplines ou professions appartenant à un certain ordre de connaissance reconnu par la société. De

[50] **Ibid.**

plus, leurs croyances de causalité et leurs notions de validité ne sont pas exclusivement basées sur les méthodologies utilisées en science naturelle ; elles peuvent cependant provenir d'une connaissance communet basée sur des méthodes et des techniques propres aux disciplines ou professions desquelles ils font part. C'est par rapport à la nature de la situation nécessitant une intervention que le domaine d'expertise est déterminé. En effet, dans le cas d'une prévention de la diffusion d'une maladie, il est clair que la communauté en compte consisterait d'experts en sciences naturelles, mais d'autres situations peuvent nécessiter une communauté ayant une expertise relative aux disciplines et professions tels que l'ingénieurie et l'économie. Dans le cas étudié dans ce travail, en ce qui concerne le problème de la sécurité des systèmes d'information, il s'agit de l'intervention d'experts dans le domaine de la télécommunication qui sont généralement représentants du secteur privé.

Les communautés épistémiques, se trouvent parmi les fournisseurs d'information ou de recommandation experte. Lorsqu'une demande pour ce genre d'information apparaît, ces réseaux ou communautés de spécialistes capables de produire l'information en compte, émergent et prolifèrent davantage. Ainsi, au fur et à mesure que les autorités politiques sollicitent leurs expertises et d'une façon leur délèguent une part du pouvoir, les membres de ces communautés deviennent de plus en plus puissants. Ce faisant, les membres des communautés épistémiques transnationales acquièrent la disposition d'influencer les intérêts des États, directement en s'identifiant comme autorité centrale de décision, ou bien en éclaircissant la dimension saillante des problèmes ce qui permet aux autorités politiques de devenir capables d'en déduire leurs propres intérêts. Il est tout autant possible que ces communautés épistémiques puissent contribuer à la création des institutions sociales qui pourraient guider les décisions internationales. Et de là, l'influence continuelle de ces institutions peut d'autant plus devenir persistante en terme de coopération des États en vue de solution aux problèmes de niveau globale.

Les réseaux d'experts peuvent intervenir afin d'élucider la relation de causalité dans les processus de crise, et de là estimer les différentes conséquences qui peuvent apparaître suite à divers séries d'actions destinées à être prises. Lorsqu'il s'agit non pas d'une crise, mais plutôt d'une situation complexe due à l'incertitude provenant de la relation causale entre un problème émergeant et toute une série d'évènements

survenues en raison du manque de précaution, comme la mise en marche d'une politique exclusive à la situation, l'aide d'expert joue un rôle semblable à celui joué dans la prise de décision. Ou encore, l'implication des communautés épistémiques peut être tout autant décisive pour les États dans l'évaluation de leurs propres intérêts nationaux. La clarification des relations de causalité liées aux problèmes dont ces derniers se trouvent face à face, les mène souvent à redéfinir leurs propres intérêts ou même à en identifier des nouveaux. Et dernièrement, ces communautés épistémiques assistent à la formulation des politiques. Cette assistance est parfois un mécanisme de légitimation pour les autorités politiques dans la poursuite de politique antérieurement déterminée. Par contre, il se peut que ces experts puissent imposer leur propre discernement relatif à la situation, et ainsi peuvent changer l'objectif initial des autorités politiques. Ainsi, les communautés épistémiques peuvent prendre place dans les divers étapes du processus de prise de décision, comme la détermination des alternatives, la sélection des politiques mais aussi dans l'établissement des coalitions nationales et internationales établies pour le soutien de la mise en œuvre des politiques choisies.

Les communautés épistémiques peuvent être de niveau nationales aussi bien que transnationales relativement à leur domaine d'activité. Celles qui sont nationales par nature peuvent tout autant être indirectement effectif sur le plan international par l'intermédiaire des autorités politiques, pris en compte que ces experts exercent leur influence dans le choix des stratégies poursuivies dans les collaborations transnationales. En revanche, celles qui possèdent une structure internationale sont supposées avoir une influence plus intense mais aussi directe dans ce genre de collaboration. Les idées d'une communauté transnationale peuvent s'établir au sein d'une organisation internationale ou bien au sein d'organismes étatiques variés, par la suite, ces idées ceux-ci peuvent être diffusées à d'autres États par l'intermédiaire des décideurs influencés par ces idées.

d. La distinction entre les communautés épistémiques et les autres groupes

Comme mentionné préalablement, les membres d'une communauté épistémique partagent les notions de validité et de politique commune en plus de leurs opinions

causatives et de leurs principes. Leurs revendications d'autorité, dans un domaine particulier, en politique liée à la connaissance, repose sur le degré de la reconnaissance de leur expertise dans ce domaine. D'après P. Haas, ce sont par ces caractéristiques que sont distinguées les communautés épistémiques des autres groupes impliqués dans le processus de coordination politique qui agissent par l'intermédiaire de leurs savoirs, qu'il nomme comme 'communauté épistémique ressemblant' (epistemic community like). Dans cette catégorie il considère les groupes d'intérêt, les mouvements sociaux, les disciplines et les professions, les législateurs, les organes bureaucratiques et les coalitions bureaucratiques.

De plus, la réputation et le prestige professionnel provenant de leur expertise dans un domaine fortement approuvé par la société ou par les décideurs élites que détiennent les membres d'une communauté épistémique dans un domaine spécifique, leur accordent un accès au système politique et légitiment leurs activités. Leurs connaissances, qui sont entérinées par des examens de validité leur concèdent une influence dans les débats politiques et constituent leur principale ressource de puissance sociale.[51] L'acceptation de leur savoir par les autres est donc un autre point qui fait la distinction entre les membres d'une communauté et les autres acteurs ou groupes et qui limite l'influence et l'entrée de ces autre groupes et acteurs dans les débats politiques.

Afin d'apporter une catégorisation plus explicite en vue de la distinction entre les communautés épistémiques et les 'communautés épistémiques ressemblants', P. Haas fait la distinction en deux dimensions. Dans la première dimension, il considère les croyances basées sur les principes et les croyances de causalité (pouvant être analytiques et normatives) qui peuvent être communes ou non pour les différents groupes de savoir. Dans la deuxième dimension, il fait la distinction par rapport à la connaissance consensuelle et l'emprise de politique (les intérêts) qui peuvent être également communes ou non pour chaque groupe. Les communautés épistémiques se distinguent par exemple des groupes d'intérêt dans le sens qu'ils possèdent des croyances de causalité commune ; une compréhension commune de cause-et-

[51] W. Schluchter, "Modes of Authority and Democratic Control" in V. Meja, D. Misgeld, and N. Stehr, eds., **Modern German Sociology** (New York: Colombia University Press, 1987),p.297, cité dans P.M. Haas, **op. cit.**, p.17

conséquence. Face à des situations où elles sont confrontées à des anomalies qui pourraient ébranler leurs croyances de causalité, les communautés épistémiques se retirent des débats, contrairement aux groupes d'intérêt.

Tableau 1.1. *La distinction entre les communautés épistémiques et les autres groupes*[52]

Croyances de Causalité (*causal beliefs*)

Croyances de Principes (*principled belief*)	*Commun (shared)*	*Non Commun (non shared)*
Commun	Les Communautés Epistémiques	Les Groupes d'intérêt et les mouvements sociaux
Non Commun	Les disciplines et les professions	Les législateurs, les organes bureaucratiques et les coalitions bureaucratiques

La Base de Connaissance (*knowledge base*)

Intérêts	*Consensuel*	*Contesté ou absent*
Commun	Les Communautés Epistémiques	Les Groupes d'intérêt et les mouvements sociaux et les coalitions bureaucratiques
Non Commun	Les disciplines et les professions	Les législateurs et les organes bureaucratiques

[52] P.M. Haas, **op. cit.**, p.18

Néanmoins, la catégorisation précédente présente éventuellement une distinction vis-à-vis des autres communautés scientifiques et des groupes de professions et de discipline. La séparation s'ensuit des engagements partagés d'origines normatives détenues par les membres de la communauté épistémique. Les standards éthiques des communautés épistémiques proviennent de leurs approches basées sur des principes et varient en fonction du sujet entamé et non d'un code professionnel précis. En ce qui concerne les organismes bureaucratiques, ceux-ci mènent leurs efforts afin de préserver leurs missions et leurs budgets, alors que les communautés épistémiques déploient leurs connaissances à des politiques dans leurs objectives normatives.

D'après la catégorisation précédente, ce sont le partage de croyances de causalité et le consensus pour une base de connaissance qui font donc la distinction entre une communauté épistémique et un groupe d'intérêt. Dans certaines situations, la production de l'expertise est utilisée dans des objectifs politiques qui opposent différents acteurs dans un jeu de pouvoir. Dans ce cas, l'expert constitue alors lui-même un groupe d'intérêt. Eve Fouilleux, dans son étude sur l'expertise dans le secteur agricole souligne que : « *L'expertise peut être considérée comme une réponse aux besoins des acteurs politico administratifs en quête d'informations, d'arguments, de conseils nécessaires à leurs stratégies propres liées à l'élaboration du compromis sur le forum des communautés de politique publique, elle peut être également considérée comme un signe des effets d'apprentissage induits par la production scientifique : la sollicitation par les acteurs politico-administratifs d'un groupe d'économistes à produire de l'expertise est d'une certaine manière la manifestation explicite d'un intéressement des acteurs politico administratifs concernés, de leur volonté «d'apprendre» et/ou de leur avancement dans le processus d'apprentissage*»[53].

Donc, contrairement à l'utilisation de l'expertise dans le but d'apprentissage, il est possible d'observer son utilisation par les acteurs politico administratifs, mais aussi des groupes d'intérêt ayant l'objectif d'augmentation de pouvoir. Et ceci, afin d'ouvrir la voie à exercer leur influence sur les autorités politiques dans le but de la mise en oeuvre des réglementations qui seraient en leur intérêts. L'exclusion d'un

[53] E. Fouilleux, "Entre production et institutionnalisation des idées : la réforme de la politique agricole commune", **Revue Française de Science Politique** 50(2) 2000, pp. 277-305

certain groupe d'acteurs de la production de l'expertise jugée utile par les acteurs politico administratifs peut priver ce groupe de son pouvoir de représentation des intérêts. Pierre Lascoumes, dans son étude sur les politiques liées à l'environnement, rappelle ainsi que « la force de la technocratie est moins la capacité d'un corps préexistant d'experts et de décideurs à reproduire sa domination historique sur un secteur que le résultat d'un travail permanent de construction de savoir-faire et de légitimité. »[54].

2. Le rôle des communautés épistémiques dans l'évolution politique

D'après Emmanuel Adler et Peter M. Haas, le processus de l'évolution politique peut être exprimé comme une séquence de quatre étapes principales : l'innovation politique, la diffusion, la sélection et la persistance. [55]

a. L'innovation politique

Les Communautés Epistémiques exercent une influence sur l'innovation politique en :

- encadrant une série de débats politiques cernant un certain problème
- définissant les intérêts Étatiques
- établissant des standards précis

Les objectifs politiques, la conception des intérêts par les États et la conduite de la coordination politique, dans le cas d'un domaine spécifique (tels que la gestion économique d'après guerre ou le contrôle de la pollution), sont liés à l'interprétation du contexte dans lequel des actions particulières sont censées être exécutées. A partir de l'identification de la nature du problème et de l'encadrement du contexte, de nouvelles données et idées sont interprétées. C'est ainsi que les communautés

---

[54] P. Lascoumes, « La technocratie comme extension, cumul et différenciation continus des pouvoirs », dans V. Dubois et D. Dulong (dirs), **La question technocratique : de l'invention d'une figure aux transformations de l'action publique,** Strasbourg, Presses Universitaires de Strasbourg, p. 187

[55] E. Adler and P.M. Haas, "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program", **International Organization**, no.46, Winter 1992, p.375

épistémiques délimitent les débats collectifs politiques et guident les décideurs dans le choix de normes et d'institutions appropriées au sein desquels les problèmes seraient gérés et résolus. Dans un sens, il s'agit d'une restriction de l'intervalle dans lequel les négociations politiques sont susceptibles d'être entamées. Cependant, la façon et le contenu de l'encadrement du contexte peuvent mener à la formation d'un climat favorisant l'acceptation et la diffusion des opinions possédées par les communautés épistémiques.

Les idées susmentionnées sont soutenues par des efforts d'une communauté épistémique d'origine américaine dans un domaine précis. Celle-ci a contribué à l'adoption, à l'échelle internationale, d'un accord sur le contrôle d'armes nucléaires où l'encadrement du sujet était établi vis-à-vis d'une coopération parmi les deux super puissances. Par la suite, cette communauté, avec le soutien des experts soviétiques et en créant une nouvelle communauté épistémique, a joué un rôle primordial dans la formation de la perception des politiciens concernant la sécurité internationale et les intérêts étatiques. En l'absence d'une guerre probable, les anticipations des politiciens relatives à la guerre provenaient de manière directe des conseils théoriques procurés par les communautés. C'est par une présentation de conseil d'expertise et par un encadrement du contexte que les communautés épistémiques ont influencé les anticipations, et par conséquent, le comportement des politiciens. En premier lieu, elles ont persuadé les leaders soviétiques et américains sur la nécessité de prévention d'une guerre nucléaire tout en soulignant le fait qu'un tel choix serait dans leur profit mutuel. Par la suite, elles ont contribué à la génération de nouveaux intérêts dans le domaine de contrôle d'armes. Les idées introduites par les experts de contrôle d'armes sont reflétées dans le traité de missile antiballistique entre les États-Unis et l'Union Soviétique (ABM)[56] et dans bien d'autres accords durant la période de la guerre froide. [57]

---

[56] Le Traité sur la limitation des systèmes de missiles anti-balistiques a été signé par les États-Unis et l'Union Soviétique le 26 Mai 1972. Le traité contraignait les deux parties sur la construction d'un système stratégique national de missile anti-balistique et délimitait d'une manière sévère le développement et le déploiement de missiles de défense.

[57] E. Adler, "The Emergence of Cooperation: National Epistemic Communities and The International Evolution of the Idea of Nuclear Arms Control", **International Organization**, no.46, Winter 1992

En ce qui concerne d'autres domaines, tel que le cas des télécommunications, les communautés épistémiques ont joué un rôle similaire dans l'encadrement du problème et par conséquent elles ont influencé les sélections adoptées par les États. Le régime de télécommunication se dressait originalement sur les notions de 'monopole naturel' et était vigoureusement sous l'influence des perceptions des économistes. Hormis l'influence d'une communauté épistémique d'ingénieurs envisageant la conception et la coordination des standards et les équipements relatifs à la télécommunication, le régime n'aurait cependant pu se diriger vers l'établissement d'accords multilatéraux éventuels.[58]

L'influence exercée par les communautés épistémiques sur l'innovation politique se présente aussi bien dans l'établissement de standards et dans le développement de régulations en plus de leur habileté d'encadrer les problèmes. Dans le travail de Raymond Hopkins concernant les réformes réalisées dans le domaine du régime international d'aide alimentaire, une communauté épistémique internationale composé de spécialistes en développement économique, d'économistes d'agriculture et d'administrateurs d'aide alimentaire, se charge de l'établissement d'un nouveau régime. D'après les principes initiaux du régime, l'aide alimentaire était destinée à être réalisée par les surplus des stocks de donneurs, à supplémenter le commerce régulier d'importation en alimentation dans les pays bénéficiaires et à être attribué en tant qu'engagement à court terme lié aux objectifs politiques et économiques des donateurs. Néanmoins, les principes précités ainsi que les arguments et les critiques divers apportés par les communautés épistémiques les ont amené à affirmer que l'aide alimentaire constitue un effet adverse dans la réduction de la production locale dans le pays bénéficiaire. En conséquence il s'agit d'une aggravation de la faim au lieu d'un soulagement. La communauté épistémique a en premier lieu développé et proposé des idées qui éviteraient les effets néfastes, pour un approvisionnement plus efficace d'aide alimentaire. Par la suite, elle a favorisé l'établissement de réformes ayant comme objectif de mener l'aide alimentaire en tant que fondement pour le développement économique des pays bénéficiaires. Les idées de la communauté épistémique internationale ont joui d'un soutien provenant des organisations

---

[58] P.F. Cowhey, "The International Telecommunications Regime", **International Organization**, no.44, Spring 1990, pp.169-200

internationales et des gouvernements des pays bénéficiaires aussi bien de celui des pays donateurs.[59]

b. La diffusion de politique

D'après Peter Haas, la communication internationale et le processus de socialisation, qui sont favorisés par les communautés épistémiques, jouent un rôle primordial dans la diffusion des idées innovatrices et des politiques d'innovations.[60] En effet, dans le cas où ces idées demeureraient limitées au sein d'un groupe, d'une organisation internationale ou d'un État national elles ne pourraient avoir des effets structurels. Bien que les membres des communautés épistémiques soient souvent engagés à des initiatives au niveau national, ils diffusent leurs conseils politiques à l'échelle transnationale en les communiquant au sein des institutions scientifiques et des organisations internationales par l'intermédiaire de conférences, de publications et divers méthodes d'échange d'information. Les liens transnationaux permettent d'exercer des pressions concurrentes sur les États par les membres d'une communauté, même si une telle action n'eut été planifiée préalablement de manière formelle. D'après E. Adler et P. Haas, la diffusion des innovations intellectuelles permet une redéfinition des anticipations, une tentative de consensus, d'où la coordination du comportement vis-à-vis des gouvernements. Les études de certains cas[61] entrepris dans ce domaine démontrent qu'il subsiste différentes méthodes et voies de diffusion d'information.

Dans le cas entrepris par Drake et Nicolaïdis, où ils étudient le rôle joué par une communauté épistémique d'experts composé d'experts dans le domaine des services,

---

[59] R.F. Hopkins., **op. cit.**, pp 225-264

[60] E. Adler and P.M. Haas, **op. cit.**, p. 380

[61] Il s'agit des cas entrepris dans le volume 46 de la revue International Organisation, 'The emergence of cooperation : national epistemic communities and the international evolution of the idea of nuclear arms control', "Ideas, Interests, and Institutionalization: 'Trade in Services' and the Uruguay Round", "Whalers, Cetologists, Environmentalists, and the International Management of Whaling", "Whalers, Cetologists, Environmentalists, and the International Management of Whaling", "Reform in the International Food Aid Regime: the Role of Consensual Knowledge", "A World Economy Restored: Expert Consensus and the Anglo-American Postwar Settlement".

intervenant au cours de la ratification de l'Accord Général sur les Echanges dans les Services (GATS) en 1986 –qui avait d'importantes implications pour l'économie mondiale- au sein du GATT. Cet accord était le résultat d'une initiative de mise en place d'un nouveau régime sur l'échange internationale dans le domaine des services. Lorsque la question sur les échanges en service, les États membres du GATT, qui disposaient d'un savoir limité sur le sujet, se montraient douteux sur les conséquences qu'apporteraient un accord multilatéral destiné à libéraliser les échanges dans le domaine du service vis-à-vis de leurs intérêts nationaux et leurs institutions. Durant leurs analyses des problèmes sur le service et leurs interactions avec les autorités politiques, les membres de la communauté épistémique sont parvenus à persuader les États sur les propriétés d'échange commune que possèdent les transactions des services internationaux et les avantages potentiels qu'apporterait l'abolition des barrières non tarifaires appliquées aux pays développés aussi bien qu'aux pays en voie de développement. De plus, en favorisant les négociations au sein du GATT et en apportant une aide aux pays membres dans la redéfinition de leurs intérêts, les membres de la communauté détenaient un rôle instrumental dans la spécification d'une série d'options politiques à être considérée par les États. Toutefois, lorsque les États ont conçus leurs intérêts qui ont été justifiés, leurs choix politiques étaient désormais menés par l'influence des dynamiques de puissance et de négociation plutôt que par une influence directe des communautés épistémiques.[62] Ce cas illustre également la manière dont les idées provenant d'une communauté épistémique se diffusent à partir d'un groupe limité composé d'acteurs nationaux vers un groupe plus large, en atteignant éventuellement les États nécessaires pour la coordination effective des dispositions.

De plus, le rôle joué par les membres des communautés épistémiques en vue de la coordination politique, de manière directe ou indirecte, se présente par la diffusion des idées et l'influence exercée sur des acteurs variés tels que les organisations nationaux ou internationaux, gouvernements bureaucrates et décideurs, les corps législatifs et corporatifs et le public. Certaines conclusions sont déduites à ce niveau.

---

[62] W.J. Drake, K. Nicolaidas, "Ideas, Interests, and Institutionalization: 'Trade in Services' and the Uruguay Round", **International Organization**, no.46, Winter 1992

Premièrement, dans le cas où une communauté épistémique acquiert une puissance au sein d'un État ou d'une organisation internationale, son influence à l'échelle internationale varie en fonction de l'influence que détient l'État ou bien l'organisme en question vis-à-vis des autres. Ceci perd sa validité dans les cas où la communauté détient une influence sur plusieurs États par l'intermédiaire de sa place au niveau transnationale, il s'agirait désormais d'une convergence informelle en vue des préférences politiques.

Deuxièmement, dans le cas où les idées des communautés épistémiques sont, dans un sens incrusté dans les organismes d'un État, ces idées peuvent avoir une influence directe sur la mise en place de standards et de développement de dispositions.
Ensuite, dans le cas où les membres d'une communauté épistémique influencent initialement les parties qui jouent un rôle primordial au cours des négociations vis-à-vis d'un problème spécifique, ils détiennent désormais un impact direct sur la définition de l'agenda et un impact indirect sur les pressions exercées par l'État hégémonique sur les États plus petits. L'étude entamée par P. Haas, sur la prohibition des chlorofluorocarbones (CFC) en raison de leur effet néfaste sur la couche statosphérique de l'ozone, démontre les efforts effectués par une communauté épistémique composée de scientifiques spécialistes sur l'atmosphère. Les membres de cette communauté, suite à un processus de rassemblement des données nécessaires, les diffusent aux gouvernements et aux producteurs de CFC, et par conséquent leur donnent une assistance dans la formulation de dispositions industrielles, vis-à-vis de la consommation et la production du CFC, au niveau national et international.[63] Le fait que les idées présentées par les membres de la communauté étaient préalablement approuvées par les États-Unis et par le producteur principal de CFC (DuPont), ceci a transformé l'environnement dans lequel les décisions politiques ont été envisagées par les autres gouvernements et entreprises. Néanmoins, dans le cas contraire, lorsque les communautés pénètrent dans le gouvernement ou bien dans l'organisme exécutif d'un acteur détenant une puissance plus inférieure, leur influence se délimite à un niveau national. Toutefois, dans certaines situations les communautés exercent une pression sur les États plus petits afin de promouvoir la mise en vigueur des accords collectifs.

---

[63] P.M. Haas, "Banning Chlorofluorocarbons: Epistemic Community Efforts to Protect Stratospheric Ozone", **International Organization**, no.46, Winter 1992

Finalement, le nombre des membres d'une communauté épistémique n'est pas déterminant dans l'acquisition d'un impact sur la politique internationale. Ce qui gagne une importance dans ce cas, ce sont l'expertise et la considération que détiennent les membres, leur capacité d'influence par leur discipline et leur habileté d'atteindre les acteurs principaux au cours du processus de la coordination politique. La considération du temps joue un rôle important en ce qui concerne l'impact des communautés. En effet, au cours des situations de crise, les décideurs saisissent de manière plus immédiate les limitations qui surviennent dans la compréhension du problème et ils deviennent conscients de la nécessité de conseil de la part de communautés épistémiques composés d'experts ou bien ils augmentent leur confiance envers les communautés déjà présents. Les crises et les nouvelles évolutions ont non seulement l'effet d'accélérer la diffusion du processus mais aussi prêtent une situation d'urgence à la réévaluation des dispositions politiques en cours.

c. La sélection de politique

E. Adler suggère que les communautés épistémiques contribuent à la génération de politique mais pas de manière indépendante.[64] Les facteurs politiques, et les considérations relatives, tels que le degré de familiarité et d'incertitude du décideur vis-à-vis du problème en question, émergent en tant que critères notables dans la l'évaluation des conseils provenant des communautés épistémiques.

Dans le cas où il n'existe pas de dispositions préalablement définis et les décideurs demeurent peu familiers du problème, une communauté épistémique contribue par encadrer le problème et définir les intérêts des décideurs, comme cités préalablement. Par la suite, elle peut de même apporter un nouvel encadrement institutionnelle lorsqu'il s'agit de situations où il s'agit d'une institution au sein de laquelle des solutions à un problème seraient générées à une échelle internationale. En présence de ces conditions, l'influence exercée par la communauté devient maximale au cours des stages d'innovation, de diffusion et de sélection politique. D'autre part, lorsque

[64] E. Adler and P.M. Haas, **op. cit.**, p.381

les décideurs sont plus familiers vis-à-vis du problème, ils font appel à l'expertise de la communauté dans le but de justifier leurs agendas préexistants.

En d'autres termes, les décideurs favorisent la pénétration de certaines communautés épistémiques à travers des canaux politiques traditionnels alors qu' ils évitent l'entrée d'autres dans l'arène politique.[65] En effet, les communautés exprimant des idées proches à la tendance commune ont meilleure chance d'acquérir une influence comparée à celles de caractère réformiste.

Les études entamées sur ce sujet démontrent que les communautés d'experts sont capables de favoriser la légitimation des accords qu'ils justifient avec leurs approches de causalité sur le sujet. Dans le cas étudié par M.J. Peterson, concernant la gestion de la pêche de baleines, un groupe d'intérêt économique d'administrateurs de l'industrie de baleine, une communauté épistémique d'experts de cétologistes et une coalition de lobby d'environnementalistes exercent une influence sur les décideurs au cours des processus de négociations.[66] Les idées apportées par les cétologistes concernant la protection de certaines espèces ont acquis un impact retardé, alors qu'un tel compromis n'avait été considéré par les décideurs.

D'après E. Adler, bien que, en général, l'influence exercée par les communautés épistémiques sur le processus de décision demeure dans les limites des politiques nationales, et que celles-ci se concentrent plutôt sur les détails à fournir vis-à-vis de la coordination des régulations -au lieu d'établir un espace plus large de politique à gérer- , elles s'avèrent néanmoins effectifs dans la détermination de nouveaux modèles de comportement destinés pour les décideurs, en identifiant les politiques qui seraient capables de satisfaire la majorité.[67] Dans l'étude de R.Hopkins, sur le l'aide alimentaire, cité préalablement, les communautés épistémiques, conscients de la signification, pour les fermiers américains, des revenus provenant de l'exportation, ils ont habilement canalisé leur énergie vers les sujets tels que l'utilisation efficace du budget alloué à l'aide alimentaire et par conséquent ont évité les problèmes où la nécessité de l'aide alimentaire serait remise en question.

---

[65] **Ibid.** p.381

[66] M.J. Peterson, "Whalers, Cetologists, Environmentalists, and the International Management of Whaling", **International Organization**, no.46, Winter 1992

[67] E. Adler and P.M. Haas, **op. cit.**, p.382

Comme dans la diffusion politique, dans la sélection de politique, la capacité des communautés épistémique de guider les décideurs à l'adoption de nouvelles tendances politiques varie également en fonction de la période. Les études de cas démontrent que suite aux changements survenus dans les conditions économiques et militaires, les politiciens montrent la tendance d'accepter plus facilement les approches apportées par les communautés épistémiques. Dans l'étude du cas concernant le contrôle d'armes, l'existence de la parité stratégique a encouragé les idées sur la sélection politique concernant le contrôle d'armes par les États-Unis aussi bien que par l'Union Soviétique. Les idées d'une communauté épistémique choisi par l'État américain afin de constituer une base au cours des processus de négociations avec l'Union Soviétique, ont d'abord été diffusés à l'Union Soviétique puis ont formé les fondements du Traité de limitaion des missiles anti-balistiques (ABM).[68] L'existence des doutes au sujet des politiques économiques isolationnistes, qui étaient liées à la défaillance de celles-ci en 1930, a donné lieu à une acceptation des idées incorporées dans l'accord de Bretton Woods.[69]

d. La persistance de politique

Les nouvelles idées et politiques gagnent un statut de conformisme une fois qu'elles sont institutionnalisées. Ceci peut se présenter par le processus de socialisation, et souvent par les efforts persistants apportés par les communautés épistémiques. [70] Comme le suggère Hopkins dans son analyse sur le régime d'aide alimentaire, « Une fois que les transformations concernant les principes et les pratiques d'aide alimentaire surgissent, ils ont gagné un caractère irréversible ».[71]

Un des facteurs affectant la période de temps pendant laquelle une communauté épistémique reste influente est le degré de consensus existant parmi les membres de la communauté. Dans le cas de l'étude sur les télécommunications, le collapse du

---

[68] E. Adler, **op.cit.**
[69] W.J. Drake and K. Nicolaidas, **op. cit.**
[70] E. Adler and P.M. Haas, **op. cit.**, p. 384
[71] R.F. Hopkins, **op. cit.**, pp 225-264

consensus entre les communautés épistémiques a poussé les régimes à s'éloigner des normes et opinions amenés par celles-ci. [72]

Lorsque le consensus prenant lieu au sein d'une communauté épistémique périt, celui-ci perd son autorité et par conséquent, l'importance attachée par les décideurs à leurs conseils s'atténue. Les crises de niveaux économiques, politiques affectent également l'autorité et l'influence accordées à une communauté épistémique. En effet, lorsque les approches apportées par les experts n'est pas satisfaisante, les décideurs sont menés à chercher conseil auprès de nouveaux groupes d'experts. Incontestablement, les idées justifiées montrent la tendance de subsister comparé à celles qui sont réfutées.

Face à l'accroissement des problèmes de nature complexe et technique d'intérêt national et particulièrement global, les autorités politiques confrontés à une situation d'incertitude font donc appel à des spécialistes, des experts dans différents domaines politiques. Dans ce chapitre, ont été présenté les caractéristiques principales des réseaux d'experts, les communautés épistémiques, ainsi que leurs principes d'intervention aux problèmes, et leurs contributions à l'évolution politique. Dans ce cadre, dans le chapitre suivant sera analysé l'impact d'une organisation agissant en tant que réseau d'expert sur les processus de décisions au sein d'une organisation interétatique en ce qui concerne le problème de la cybercriminalité.

[72] P.F. Cowhey, **op. cit.**, pp 169-200

DEUXIEME PARTIE

Le problème de la sécurité des systémes d'information et de réseau :

L'approche de l'OCDE avec la contribution du BIAC

A. L'impact d'internet et le problème de la cybercriminalité

L'émergence mondiale d'un espace économique, social, culturel c'est-à-dire dans l'espace informationnel où les activités sont désormais décentralisées, l'information devient accessible par l'intermédiaire d'une large variété de média en particulier par Internet, atteignant les individus et les organisations publiques et privés. En effet, avec l'adoption d'une norme commune qui permet la liaison de tous les ordinateurs existants, Internet donne la possibilité de communiquer des données d'une manière universelle. Les technologies d'information et de télécommunications s'unissant autour d'Internet ont aujourd'hui modifié les processus administratifs et organisationnels des organisations publiques et privées aussi bien que la communication entre les individus.

Cependant, dû à la dimension transnationale d'Internet, les activités commerciales et financières ont été affectées par l'apparition des crimes sophistiqués et des activités illégales mises à exécution par des acteurs malveillants qui sont capables de provoquer des dommages considérables. Avant d'envisager les approches de solution à cet égard, il est nécessaire de considérer les caractéristiques de cet instrument et son rôle dans les différents domaines de la société.

1. Internet : définition et caractéristiques

L'Internet est issu du réseau militaire Arpanet qui avait été élaboré pour le Pentagone dans les années soixante. Initialement, il s'agissait en cas d'attaque nucléaire de permettre aux ordinateurs à communiquer, alors même qu'une base-relais pouvait être frappée. La technique mise en place était celle des 'paquets' à savoir que le message circulait par morceaux qui étaient envoyés de façon quasi-aléatoire sur un réseau d'ordinateurs qui les relayaient en fonction de la fluidité et de la disponibilité des ordinateurs en présence.[73] Cette architecture fonctionne toujours, elle a ensuite été étendue aux centres de recherches universitaires, puis à tous les types d'usagers

[73] Définition du Federal Networking Council, http://www.fnc.gov/Internet_res.html

dans le monde entier. En d'autres termes, Internet est un instrument composé de 'réseaux de réseaux' détenus et opérés par des organisations publiques et privés et qui permet le transfert d'information d'une manière accélérée à coût effectif durant la distribution des services commerciaux, sociaux et financiers. [74]

L'expansion à l'accès de cet instrument au delà des cadres académiques et militaires est largement due à la diffusion des ordinateurs personnels, à la libéralisation des services de télécommunication et aux initiatives de régulation au niveau national aussi bien qu'internationale. Ces évolutions ont par conséquent modifié la manière de fonctionnement des États, des organisations militaires, des entreprises aussi bien que la vie des individus.

2. La place d'Internet dans les institutions publiques

La conception et l'utilisation des nouvelles technologies étaient initialement sous l'initiative des institutions publiques et militaires grâce à leur avantage en capacités économiques. Les gouvernements les ont par la suite adopté à leurs environnements administratifs et opérationnels. Bien que les technologies de l'information et des communications soient utilisées dans ce domaine depuis une période de cinquante ans, une notion qui est apparue dans ce cadre récemment est celle de la gouvernance électronique.

La '*e-gouvernement*', qui a aujourd'hui une place importante dans les programmes des États[75], est une initiative de transformation qui vise à transférer les services que les gouvernements rendent aux citoyens et aux entreprises sur l'environnement d'Internet. L'objectif est l'amélioration de la qualité des services, de renforcer le lien entre pouvoirs publics et populations avec l'ouverture de l'accès à l'information, afin de générer ainsi une démocratie plus forte, plus responsable et plus participative.[76]

---

[74] Malgré certaines additions technologiques de niveau mineures, l'architecture n'a pas subit des changements significatifs. Le nombre d'ordinateurs connectés était de quatre au début et est monté à 23 en 1971, à 111 en 1977 et à presque 4 millions en 1994 et 513 millions en 2001.

[75] Les travaux dans ce domaine sont de même entamés au niveau communautaire, les initiatives du Conseil de l'Europe en représentent une instance significative.

[76] Site du Conseil de l'Europe, www.coe.int

D'après Kate Oakley, conseiller dans le domaine de l'économie du savoir, la gouvernance électronique a une place importante vis à vis des dirigeants pour des raisons essentielles ; elle favorise l'adoption de technologies numériques qui sont essentielles pour la compétitivité économique, elle permet au gouvernement de redéfinir son rôle et de conduire davantage son action sur la population, elle permet d'«interconnecter» les informations et donc de gouverner avec plus d'efficacité et elle peut réduire les coûts sans compromettre pour autant la qualité des services publics.[77]

Les travaux pour la mise en place de mécanisme de paiement des taxes par l'intermédiaire d'Internet, de la part des départements de sécurité sociale et fiscale, constituent un exemple dans ce but. Ces services, réservés aux individus aussi bien qu'aux institutions commerciales, ont favorisé la revendication de documents et d'informations et la poursuite des procédures bureaucratiques par l'intermédiaire des formes remplis en ligne et par courrier électronique.[78]

La participation des citoyens aux procédures administratives fait de même partie des initiatives de l'e-gouvernement. Le vote électronique, bien que la participation des électeurs soit très faible, la contribution des citoyens à de multiples activités comme la planification, les jurys ou les panels de citoyens portant sur des questions extrêmement diverses en constituent des volontés dans ce cadre.

De plus, la mise en place d'un réseau physique entre les différentes unités des institutions a permis d'assembler les différentes sources d'information nécessaires pour les travaux d'analyse et de synthèse et d'offrir un meilleur service en donnant accès à une gamme d'informations beaucoup plus large dont beaucoup dépassaient le cadre de la collectivité locale. Cette volonté constituait le second objectif essentiel de ces institutions, tout en considérant que dans le secteur public, les données collectées de manière personnalisée constituent avant tout des ressources sociales et doivent être utilisées pour le bénéfice de la collectivité. Cette collection peut se réaliser par l'usage d'instruments organisationnels variés, parmi lesquels les partenariats avec le secteur privé, d'autres secteurs publics ou d'autres organisations de la société civile

---

[77] http://www.digital-eu.org, 'Qu'est ce que l'e-gouvernance', K. Oakley, 10-11 juin, 2002

[78] B.Loader, **The Governance of Cyberspace : Politics, Technology and Global Restructuring**, New York, Routeledge, 1999, p. 21

qui associent des systèmes et l'expérience technologique du secteur privé et les services et les valeurs du secteur public et les sources de la société civile.[79]

Au cours du temps, le développement et la mise en place des systèmes informatiques sont passés des institutions publiques et militaires aux grandes entreprises. En particulier, la vague de privatisation dans le champs de la télécommunication initié dans les années 1980 et accéléré dans les années 1990, a donné lieu à l'expansion de l'accès de ces technologies au niveau des individus. Ainsi, face à cette prolifération en matière d'utilisateurs, les institutions publiques étaient menées à améliorer la qualité de leurs systèmes dans le but de répondre aux demandes. Avec la pression croissante exercée sur les États en ce sujet, ceux-ci étaient conduits à transformer ce potentiel en forme de solutions pratiques.

Internet a apporté une contribution significative à l'égard d'autres services publics. En ce qui concerne les services de santé, avec l'établissement des infrastructures et des solutions logicielles, un partage d'information parmi les professionnels médicaux a pu être élaboré grâce à l'accès aux bases de données à distance. Les travaux concernant la mise en place de standards pour cartes de patients et bases de données à un niveau international pour une surveillance plus avancée des patients en constituent parmi les activités réalisées dans ce cadre[80].

Les organisations militaires, dotées de ces services ont amélioré leurs capacités de commande, de contrôle et de manœuvre grâce à l'éminence de l'information. Les forces armées sont aujourd'hui capables d'être engagées dans des guerres 'à base réseaux' dont les capacités de manoeuvres et de précision d'attaque reposent sur la supériorité de logistiques et d'informations. De plus, en procurant des informations concernant leurs activités et leurs missions par l'intermédiaire de leurs sites web, ces institutions militaires, en particulier aux États-Unis et en Europe, ont mis en place un environnement d'interaction avec le public. De cette manière, ils ont établi une image qui présente une accessibilité des forces armées vis-à-vis des individus[81].

---

[79] Le site du quartier 'London Borough of Wandsworth' a été l'un des premiers sites à proposer des applications de planification en ligne et, en liaison avec la police métropolitaine, il informera les résidants de la situation du quartier en matière de criminalité par le biais d'un bulletin électronique.
[80] B.Loader, **op. cit.**, p. 34
[81] **Ibid.**, p. 36

Les organisations d'espionnages ont de même bénéficié des apports d'Internet, particulièrement en ce qui concerne l'emmagasinement des données non traitées et la distribution des rapports aux fonctionnaires militaires et d'État. L'accès aux informations disponibles au public et nécessaires pour l'évaluation des données sur l'espionnage, nommé comme 'espionnage source libre', était devenu relativement plus simple et moins coûteux. D'autant plus, les organisations d'espionnage se sont également engagées dans la mise en place de réseaux 'solides' à travers Internet afin de pouvoir partager l'information et les données à des niveaux de classification variés sans avoir recours a créer des réseaux ad-hoc[82].

Internet se trouve désormais au centre des nouvelles activités et des services des institutions gouvernementales, militaires, de santé et d'espionnage. Ce moyen de communication améliore l'efficacité des coûts, des services et des opérations dans un espace compétitif avec le secteur privé. D'autre part, les implications d'utilisation d'Internet pour la livraison et la provision des services et des biens à travers le commerce électronique sont plus différentes.

3. Internet et le commerce électronique

En plus des changements dans les dynamiques entre les institutions étatiques et les individus, Internet a apporté des transformations significatives au champ économique et commercial. Ces nouveaux environnements sont caractérisés par le terme de 'commerce électronique'.

Dans sa définition restreinte, le commerce électronique désigne l'ensemble des échanges commerciaux dans lesquels l'achat s'effectue sur un réseau de télécommunication, recouvre aussi bien la simple prise de commande que l'achat avec paiement, et concerne autant les achats de biens que les achats de services, qu'ils soient eux-mêmes en ligne (services d'information, jeux...) ou non. Dans une définition plus large, on peut inclure dans le 'commerce électronique' l'ensemble des usages commerciaux des réseaux. [83]

---

[82] **Ibid.**, p.39
[83] D. Tapsscot, **The Digital Economy**, New York, McGraw-Hill, 1998, p.11

Afin d'élucider l'impact d'Internet dans le domaine de l'économie il est nécessaire de distinguer le commerce entre les entreprises (Business to Business ou B2B) et le commerce avec les particuliers (Business to Consumer ou B2C) en tant que deux subdivisions du commerce électronique. Deux nouveaux segments font également leur apparition : le Business to Administration (B2A) et le Consumer to Consumer (C2C) qui regroupent respectivement les échanges entre entreprises administration et ceux entre particuliers[84].

Le commerce électronique B2B démontre comment Internet a modifié la façon dont les entreprises gèrent leurs chaînes de demandes, font l'exploration de nouveaux marchés et élaborent des services supplémentaires. Comme dans le cas des institutions gouvernementales et militaires, les entreprises de tailles variées font bénéfice des potentialités associées à cette nouvelle forme de commerce. En effet, grâce à l'infrastructure d'Internet, les entreprises sont capables de revendiquer un flux constant d'approvisionnements pour la production de leurs biens. Ils ont obtenu la possibilité d'unir leurs forces pour la gestion de leur processus d'acquisition, pour l'assurance d'une cohérence entre les tarifs et la diminution des coûts et pour d'autres procédures en matière d'administration et de régulation. Il en fut de même dans le cas des fournisseurs, qui à leur tour ont pu s'unifier pour la vente de leurs produits et services à leurs clients potentiels de manière plus efficace[85].

Bien que le commerce électronique B2B représente une large partie des activités réalisées sur Internet, le B2C est aujourd'hui d'avantage mis en avant par les médias. Cette expression désigne la vente par les entreprises de biens de consommation mu (comme des livres, fleurs, disques, etc..) et de services (logiciel, voyage et tickets, etc..) directement aux consommateurs par l'intermédiaire du réseau en ligne. Les biens et services sont procurés aux consommateurs soit par livraison soit par téléchargement. Dans cette catégorie sont aussi considérées les entreprises d'enchères en ligne[86] et celles permettant le partage des contenus des fichiers localisés sur les ordinateurs inclus dans le réseau.

---

[84] **Ibid.** p. 11
[85] **Ibid.**,p.21
[86] Les sites www.e-bay.com et www.qxl.com en constituent des exemples dans ce domaine.

Internet a donc affecté et bien souvent modifié les façons dont les États, les institutions militaires et les associations commerciales fournissent leurs services et effectuent leurs opérations. Cependant, la diffusion d'Internet à une dimension mondiale a apporté des dangers et des risques qui n'étaient pas anticipés.

4. Internet et la criminalité

Comme il a été présenté dans les paragraphes précédents, le caractère transnational d'Internet a couvert, d'une manière très rapide, les activités dans les domaines publics aussi bien que commerciaux. Les résultats montrent que le secteur privé et public sont confrontés à des conséquences néfastes provenant des activités criminelles qui augmentent d'une manière croissante.

Avant d'envisager les aspects des activités criminelles sur Internet, il est important de noter que ceux-ci sont en grande partie favorisés par l'architecture technique d' Internet. En effet, à l'origine, Internet était destiné à assister à l'échange d'information parmi un nombre restreint d'individus, d'organisations administratives et d'instituts de recherche. Son infrastructure n'était pas conçue pour une utilisation dans les domaines commerciaux et sociaux. L'instauration de la sécurité dans ces systèmes qui ne constituait pas une priorité auparavant a crée une situation qui a rigoureusement changé avec l'arrivé d'une large masse d'utilisateurs individuels et commerciaux au début des années 1990. Bien que la criminalité dans le domaine des systèmes d'information et de réseau ne soit pas un phénomène récent, les malveillances survenues au long des années 1970 et 1980 n'avaient pas apporté des conséquences difficiles à contourner[87].

Le terme « cybercriminalité » fait référence aux intrusions illégales dans les ordinateurs et les réseaux, aux sabotages de données et d'informations, aux fraudes effectués en ligne, aux manipulations sans autorisation des informations et à la distribution de matériaux illégales[88]. Les activités de cybercriminalité peuvent varier

[87] B. Loader, **Cybercrime: Law Enforcement, Security and Surveillance in the Information Age**, New York, Routledge, 2000, p. 15
[88] **Ibid.** p. 9

en fonction de leur typologie. Il existe différents types d'infractions qui sont regroupées d'après leurs points communs.

La première catégorie est celle des infractions de contenu, qui réfère à la publication et la diffusion de matériels illégaux, où il est possible de citer les actes liés à la pornographie enfantine et la propagande raciste. La pornographie enfantine est devenu objet de trafic international. Selon le responsable de la Division française pour la répression des atteintes aux personnes et aux biens (DNRAPB), '350 à 500.000 clichés à caractère pédophile' circulent par messageries et sont consultables sur Internet. D'après la police fédérale allemande, en l'espace d'un an, le nombre de sites pornographiques infantiles en langue allemande a augmenté de 100% et l'un d'entre eux a accueilli la visite de 500 000 internautes en très peu de temps. Les associations de lutte contre le racisme et la xénophobie observent une prolifération importante de sites haineux et racistes sur Internet[89]. En 1995, il y s'agissait d'environs 160 sites de cette nature basés aux Etats-Unis. Aujourd'hui, il y en a plus de 2 500 qui à l'abri du premier amendement de la constitution américaine préservant la liberté d'expression, diffusent leur propagande haineuse, les textes révisionnistes et autres objets du culte nazi. Certains experts recensent actuellement quelque 4 000 sites racistes accessibles sur la toile qui incitent ouvertement à la violence. [90]

Un autre type d'infraction est l'atteinte aux droits des auteurs qui augmente de manière croissante. Avec, la multiplication des échanges entre internautes de fichiers contenant des morceaux de musiques ou des albums entiers, des films, des livres fait entrer chacune de ces personnes dans la sphère de la cybercriminalité.

L'atteinte contre les systèmes ou les données informatiques constituent une autre activité criminelle tels que la pénétration à un système informatique et le placement d'un virus -qui est un mini programme qui se réplique automatiquement à travers un autre programme et se propage à l'insu de l'utilisateur à la vitesse d'une infection virale. Certains virus informatiques ont la capacité d'effacer fichiers et disques, et facilement de déclencher la destruction de données ou de systèmes entiers d'une valeur colossale en raison de l'interconnexion des réseaux. L'incrimination des actes

[89] Dans le site de l'organisation américaine Hatewatch, www.hatewatch.org, sont répertoriés une liste de site révisionnistes et racistes.
[90] www.coe.int

de fraude et de faux est souvent très élevé. Récemment, des groupes organisés en Ukraine et Russie ont 'piraté' plus de 40 sites américains, détournant les numéros d'au moins un million de cartes de crédit[91].

5. L'impact de la cybercriminalité

Les statistiques de la revue 'Information Week' confirment qu'en 2001, plus de trois quarts des entreprises participant à l'enquête ont été atteint par les attaques cyber. De plus les recherches envisagées par le Forum de Sécurité d'Information (ISF), un groupe comprenant plus de cent grandes entreprises, démontrent que plus de 90% de leurs membres ont été affecté par les incidents générales provenant d'Internet. La majorité de ces interruptions étaient des intrusions de codes non souhaités dans le réseau, les virus.[92] L'impact de ces activités malveillantes sur les entreprises s'est présenté en terme de déception d'opérations, de complication de et de perte de réputation.

Incontestablement, les organisations politiques, militaires et commerciales constituent les principaux groupes atteints par la cybercriminalité, effectué par les acteurs tels que les hackers, les organisations terroristes, les groupes extrémistes de pression, les organisations criminelles, les entreprises internationales et les institutions d'espionnage étrangères.

Les hackers sont des groupes organisés ou des groupes d'individus capables de pénétrer aux systèmes d'information et de réseau par l'exploitation de leurs vulnérabilités intrinsèques. Bien qu'ils portent des motivations variées justifiant leurs actions comme par exemple expérimenter les faiblesses des systèmes, ceux-ci causent des ruptures aux systèmes d'information et de réseau à travers le monde.

Les groupes terroristes et les associations de crimes organisés sont parmi les bénéficiers des défaillances provenant d'Internet et des autres systèmes de réseau.

---

[91] Ibid.

92 ISF, Information Security Forum, www.securityforum.org, Le Forum sur la Sécurité d'Information est une association qui est réuni la connaissance et l'expérience des plus importantes organisations dans le monde afin d'apporter des solutions aux problèmes causés par la sécurité d'information.

Leurs objectifs sont de nature politique et économique. De plus, Internet donne lieu à l'établissement des canaux de communication à travers lesquels ils sont capables de coordonner les activités de leurs membres bien qu'ils soient dispersés géographiquement.[93]

Les associations de crime international constituent une autre source de menace. Par le moyen d'Internet, ils accomplissent de manière plus discrète leurs activités tels que le blanchiment d'argent, l'accumulation de revenus ou bien l'établissement de sources de revenus par l'intermédiaire de jeux d'argent, d'activités de pornographie, de vente de drogue[94].

Dans ce cadre, les entreprises internationales peuvent eux aussi constituer une menace importante vis-à-vis de la sécurité des systèmes d'informations et de réseaux. Ces organisations commerciales tentent de faire des intrusions dans les réseaux afin d'atteindre, d'une manière illégale, les données et aux informations de leurs concurrents.

Finalement, les organisations étatiques d'espionnage sont ceux qui sont sur le plus haut niveau de risque en vu des intrusions externes possibles pouvant être réalisées par les réseaux étrangers.

La cybercriminalité est donc capable de frapper aussi bien les pouvoirs publics que les firmes et les individus. Il est donc nécessaire de prendre en compte les dommages considérables qui y sont causés. Compte tenu la dimension transnationale d'Internet, il est important de savoir si les États sont en mesure de surveiller les flux d'information qui circulent et d'établir une réglementation dans le but de détourner la cybercriminalité.

6. Les restrictions liées à une solution au niveau national

---

[93] B. Loader, **Cybercrime: Law Enforcement, Security and Surveillance in the Information Age**, New York, Routledge, 2000

[94] **Ibid.**

Les approches des États pour réglementer les activités dans le cyberspace ont d'abord été de considérer le réseau dans le cadre de leurs frontières comme de leurs lois. Du point de vue de la dimension juridique, la capacité dont disposent les États pour la mise en place d'un dispositif de contrôle des crimes dans le cyber-espace est largement inappropriée[95]. D'après Guy de Vel, actuellement Directeur Général des Affaires Juridiques du Conseil de l'Europe, il s'agit de l'existence de plusieurs enjeux dans ce cadre qui peuvent mener Internet à demeurer un espace de non-droit; tels que l'inconvénient à l'application du droit pénal qui est conçu pour le monde physique aux délits commis dans le monde virtuel et l'insuffisance des règles juridiques de sauvegarder les droits individuels et les valeurs et principes fondamentaux auxquelles sont attachées les sociétés lorsque les êtres humains évoluent dans le cyber-espace. [96]

En ce qui concerne le problème du contrôle des flux par exemple, devant une émission sur Internet, un État se trouve en confrontation à deux cas : soit le message est émis à partir de son propre territoire, soit il provient d'un point extérieur à celui-ci, par l'intermédiaire du réseau. Dans le premier cas, bien que le cyberespace ne constitue pas une zone de non-droit, l'État est face à un problème technique : il lui est impossible de confisquer les duplications du document illégal téléchargé par des milliers de personnes, du point de vue matériel. Dans le deuxième cas, c'est-à-dire lorsque l'émetteur se trouve placé hors du territoire national de l'État, il ne peut se protéger contre des émissions lancées ou connectées en dehors de son territoire. En d'autres termes, si le serveur, c'est-à-dire l'ordinateur contenant des informations consultables à distance par d'autres ordinateurs, est situé sur le territoire d'un autre État ou, dans des zones ne relevant d'aucune autorité étatique, il est impossible pour l'État victime d'engager aucune action, sauf pouvoir consentir une coopération juridique efficace avec l'État d'où provient l'émission.[97]

---

[95] J.Laroche, **Politique Internationale**, Paris, L.G.D.J., 2000, p.102

[96] A consulter le texte entier du discours donné à l'occasion de la Conférence sur la Cybercriminalité ayant lieu à Budapest, le 20-21 novembre 2001, sur http://www.coe.int/T/F/Com/Dossiers/Themes/Cybercriminalite/DiscoursDeVel.asp

[97] J.J. Lavenue, « Cyberspace et droit international : pour un nouveau jus communicationis », **Revue de la Recherche Juridique : droit prospectif**, 21 (66), 1996, p.815, pris par J. Laroche, **op. cit.**, p.105

En effet, la caractéristique transnationale d'Internet et sa structure décentralisée apparaissent comme des obstacles insurmontables par les États individuellement et les systèmes juridiques nationaux apparaissent largement inadaptés.

7. L'établissement de la sécurité des systèmes d'information : une approche

Compte tenu des caractéristiques d'Internet, sa structure décentralisée, le contrôle de cet instrument et l'établissement d'un environnement de sécurité par les États ne semblent donc pas envisageables dans le cadre de territoires nationaux. L'entreprise de réglementations se montre comme un obstacle car les systèmes juridiques nationaux apparaissent largement inadaptés. Un contrôle des sources d'émission nécessiterait des accords juridiques avec une coopération des États au niveau internationale. Afin d'établir une stratégie commune concernant le renforcement de la sécurité sur les réseaux informatiques, des travaux variés ont été entamées par certaines organisations internationales; et le projet de convention débattu au sein du Conseil de l'Europe et les conférences réalisés sous le toit du G8 [98] peuvent être cités dans ce cadre.

Comme présenté ultérieurement, la cybercriminalité affecte le secteur privé aussi bien que les États. D'autre part, les infrastructures des télécommunications qui étaient maîtrisées par des opérateurs publics sont désormais détenues en grande partie par les entreprises privées suite à la vague de privatisation dans les années 1990. Il devient donc incontournable pour les États de solliciter l'expertise des entreprises privées dans la mise en place d'un cadre pour la sécurité sur Internet.

---

[98] Le Conseil de l'Europe s'est attaché à élaborer une convention capable de répondre aux défis que pose la criminalité informatique. La Convention sur la Cybercriminalité, apparu à la suite d'un travail ayant duré quatre ans, a été adoptée le 8 novembre 2001 par le Comité des Ministres du Conseil de l'Europe, lors de sa 109ème session au niveau ministériel. Elle vise avant tout à garantir la sécurité du réseau et de ses utilisateurs et détermine trois principaux axes de réglementation : l'harmonisation des législations nationales concernant la définition des crimes, la définition des moyens d'enquêtes et de poursuites pénales adaptés à la mondialisation des réseaux et la mise en place d'un système rapide et efficace de coopération internationale. Les 44 pays membres du Conseil de l'Europe ont participé à l'élaboration de ce texte ainsi que le Canada, les Etats-Unis, le Japon -observateurs auprès de l'organisation- et l'Afrique du Sud qui ont pris une part très active dans le processus.
Quant aux travaux dirigés au sein du G8, au début de l'an 2000, les responsables de cette organisation se sont réfutés à créer une « cyberpolice mondiale » afin de ne pas porter atteinte à leur souveraineté lors d'une conférence consacrée au renforcement de la sécurité sur les réseaux d'information.

D'autre part, comme il a été mentionné préalablement la difficulté du contrôle du cyberespace provient largement de l'architecture d'Internet, étant donné que ce réseau avait été conçu au départ pour la liaison d'un nombre limité d'ordinateurs. Son infrastructure technique n'est pas en effet convenable à la façon dont en est fait l'usage aujourd'hui. Par conséquent, pour une approche de solution, la contribution d'une expertise technique dans ce domaine s'avère indispensable.

L'Organisation de Coopération et de Développement économique (OCDE) a entreprit dans ce cadre des travaux afin d'apporter une approche pour la sécurité des systèmes d'information. L'élaboration des Lignes directrices régissant la sécurité des systèmes d'information constitue une volonté dans cet objectif.

B. L'approche de solution proposée au sein de l'OCDE et l'intervention du BIAC

1. L'initiative pour l'élaboration des lignes directrices régissant la sécurité des systèmes d'Information au sein de l'OCDE

Le 26 Novembre 1992, le Conseil de l'Organisation pour la Coopération et le Développement Economique (OCDE) a approuvé la Recommandation du Conseil concernant les Lignes directrices pour la sécurité des systèmes d'information qui a été adopté par les 24 pays membres[99]. L'objectif de ce document était de souligner l'importance des risques liés aux systèmes d'information et de réseaux, tout en faisant appel à la nécessité de surveillance et de standard au niveau international. Ceci était toutefois entrepris dans le but d'apporter des ripostes aux défaillances causées par les systèmes d'information et aux crimes informatiques, et delà encourager la prise de conscience par les autorités à ce sujet.[100] Par conséquent, dans ce cadre, une série de normes, dénommées comme 'principes' ont été introduit par l'OCDE ayant pour objectif d'accorder une assistance aux organisations publiques et privées lors de leurs activités de réglementation en ce qui concerne la sécurité des systèmes d'information et de réseaux.[101]

Cet acte officiel est, entre autres, le résultat de toute une série de processus de décisions ayant impliqué les membres du Groupe d'Expert qui a été créé en 1990 par le comité de la Politique de l'Information, de l'Informatique et des Communications (PIIC) de l'OCDE suite à la décision du Secrétariat. Le Groupe d'Experts était composé de délégués d'États, d'académiciens originaires des domaines tels que droit, mathématiques et informatique et de représentants du secteur privé tels que les fournisseurs et les utilisateurs des biens et services en matière d'informatique et de communication. Le Groupe d'Experts s'est réuni à cinq occasions durant une période

---

[99] OECD, **Guidelines Security for Information Systems**, 1992
[100] C. Axsmith, **The OCDE Guidelines for the Security of Information Systems : A look to the future**, from 16th national security agency/national institute for standards and technology (NSA/NIST) National Computer Security Conference, 20-23, September 1993, p 308
[101] **Ibid.**, p. 20.

de vingt mois et a remis le texte final au comité PIIC en octobre 1992.[102] Suite à la confirmation du comité PIIC, le texte des Lignes Directrices régissant la sécurité des systèmes d'information a été transmis au Conseil de l'OCDE. Les lignes directrices ont été réexaminées et mises à jour en 1997 et en 2001 consécutivement afin de refléter les réseaux d'informations caractérisé par Internet[103]. Elles ont été adoptées par des organisations du secteur public et privé auxquelles elles ont servi de base pour l'élaboration de procédures réglementaires variées liées au domaine de sécurité des systèmes d'information. A ce titre, le 'Standard Britannique pour la Gestion de la Sécurité de l'Information' qui a été élaboré en 1994 et qui a servi de modèle à de nombreux pays européens dans l'élaboration de leurs standards dans ce domaine, a été formé à partir du cadre des Lignes Directrices[104].

Cependant, cette volonté de riposter aux conséquences négatives causées par les fraudes et les défaillances informatiques a engendré une implication imposante de l'expertise du secteur privé dans ce domaine étant donné que l'infrastructure des technologies d'information est conçue, établie, et mise en fonctionnement par ces derniers. Par conséquent, le comité consultatif économique et industriel auprès de l'OCDE, le BIAC, qui regroupe les représentants du secteur privé, a joué un rôle déterminant au cours des processus de négociation. Ce groupe a pu présenter un encadrement du point de vue technique du problème mais il a de même annoncé ses intérêts et ses inquiétudes parmi les représentants des États, ce qui les différencie des réseaux d'experts, des communautés épistémiques. C'est pourquoi dans ce travail, ce groupe sera considéré dans la catégorie de 'communauté épistémique ressemblant' de Peter Haas.

L'intérêt principal du BIAC était la réalisation d'une coopération avec les États pour la conception de standards communs du point de vue technique et gestionnaire et de codes de conduite appropriés au domaine de la sécurité des systèmes d'information et de réseaux. Toutefois, pour la mise en place d'une règlementation commune, d'un point de vue technique les deux parties furent menées à ouvrir leurs systèmes de

---

[102] OECD, **Guidelines for the Security of Information Systems,** 1992, p.3
[103] OECD, **Guidelines for the Security of Information Systems: Towards a Culture of Security**, 2002
[104] OECD, **Report of the Ad-Hoc Meeting of Experts on Information Infrastructure, Issues Related to Security of Information Systems and Protection of Personal Data and Privacy**, Paris, 1996, OECD Working Papers 1022-2227 v.4, no 38, p.53

réseaux. Ainsi, ceci est apparu comme sujet principal de débat au cours des négociations vu le caractère confidentiel des informations appartenant aux États.

Avant d'entamer l'étude du processus de négociation qui se s'est achevé par la réalisation des Lignes directrices, il est important de montrer les évolutions qui ont incité le BIAC à gagner une telle influence, particulièrement dans le domaine des technologies d'information et de communication, au sein de l'OCDE. Dans la suite du travail sera présenté l'étude des rapports entre une organisation internationale qui est un acteur de type étatique et une organisation non gouvernementale qui est un nouveau type d'acteur agissant dans le nouveau fonctionnement du système internationale. Afin de comprendre à quel niveau ceux-ci interagissent il est important d'expliciter les caractéristiques structurelles propres à chacune de celles-ci.

2. L'OCDE : origines et structures

L'OCDE, officiellement fondé en Septembre 1961, est née de l'Organisation Européenne de Coopération Economique (OECE). L'OECE est issue du Plan Marshall et de la Conférence des Seize (Conférence de coopération économique européenne) qui a pris place pour l'établissement d'une organisation permanente chargée d'assurer la mise en oeuvre d'un programme de relèvement commun et, en particulier, de superviser la répartition de l'aide. Le premier objectif de l'Organisation dont le siège a été fixé à Paris, était de préparer le Programme européen de relèvement qui justifiait l'effort américain. A cet égard, de graves difficultés avaient apparues du côté de certains pays bénéficiaires qui s'étaient avérés incapables de s'entendre sur une harmonisation préalable de leurs programmes à long terme. L'OECE a commencé à décliner après 1952, conséquence de la fin inattendue du Plan Marshall et d'un changement d'orientation au profit de l'OTAN. Cependant elle a continué à entamer d'autres programmes en faveur de la productivité, financés en grande partie par les États-Unis. Lorsque cette reconstruction était en grande partie complétée, les États concernés ont reconnu l'existence de nouveaux défis économiques, sociaux et environnementaux nés de l'interdépendance et de la

mondialisation d'où l'OECE a été remplacée par l'Organisation de Coopération et de Développement Economiques (OCDE), une organisation mondiale.[105]

Les objectifs de cette nouvelle organisation étaient établis dans sa convention. L'OCDE s'attendait à réaliser la plus forte expansion possible de l'économie et de l'emploi et une progression du niveau de vie dans les pays membres, tout en maintenant la stabilité financière, et à contribuer ainsi au développement de l'économie mondiale. Il était de même chargé de contribuer au développement économique dans les pays membres, ainsi que ceux non membres, en voie de développement économique et à contribuer à l'expansion des échanges à l'échelle mondiale sur une base multilatérale et non discriminatoire conformément aux obligations internationales. [106]

La convention de l'OECE avait attribué un grand nombre de responsabilités aux États membres. Ils étaient particulièrement destinés à promouvoir l'efficacité économique et la libéralisation des échanges. En 1961, l'OCDE se composait des pays européens Membres originaires de l'OECE auxquelles ont rejoint les États-Unis et le Canada. Entre temps, les pays comportant des objectifs similaires étaient tout autant invités à participer. En 1973, les membres de l'OCDE comprenaient le Japon, l'Australie, la Nouvelle Zélande et la Finlande. Pendant les années 1990, l'organisation accueillait le Mexique, l'Hongrie, la République Tchèque, la Pologne et la Corée du Sud.[107]

La structure et les activités de l'OCDE sont considérablement similaires à celles des autres organisations internationales. L'OCDE comprend deux branches principales: le Conseil et les Comités; et le Secrétariat qui sont liés par le Secrétaire général qui est le président du Conseil.

---

[105] Historique de l'OCDE disponible sur http://www.oecd.org/document/53/0,2340,en_2649_201185_1876917_1_1_1_1,00.html

[106] Voir art. 1 et art. 2 de la Convention relative à l'OCDE, disponible sur http://www.oecd.org/document/44/0,2340,en_2649_34483_1915884_1_1_1_1,00.html

[107] Actuellement, les membres de l'OCDE sont : l'Allemagne, l'Autriche, la Belgique, le Canada, le Danemark, l'Espagne, les Etats-Unis, La France, la Grèce, l'Irlande, l'Islande, l'Italie, le Luxembourg, la Norvège, les Pays-Bas, le Portugal, la Suède, la Suisse, la Turquie et le Royaume-Uni, le Japon, la Finlande, l'Australie, la Nouvelle-Zélande, le Mexique, la République Tchèque, la Hongrie, la Corée et la Pologne. La Commission des Communautés européennes participe de même aux travaux de l'OCDE (article 13 de la Convention de l'OCDE.

L'organisme le plus élevé est le Conseil qui rassemble sous un toit un représentant de chaque pays membre, ainsi qu'un représentant de la Commission européenne. Une fois par an, il se réunit à niveau ministériel et régulièrement par l'intermédiaire des représentatifs permanents de l'organisation, les ambassadeurs de tous les pays membres. Le Conseil encourage la réflexion sur les objectifs d'ensemble de l'Organisation et sur sa direction future aussi bien que les travaux préparatoires entrepris par le Secrétariat. Il est responsable, de manière continue, de sujets de politique étrangère d'ordre collectif, y compris dans le domaine crucial des relations avec les pays non membres. Bien qu'il lui soit possible de prendre des décisions opposantes envers les pays membres, la grande majorité des actions du Conseil sont constitués de recommandations et de résolutions. Les Recommandations font spécifiquement référence aux activités de l'organisation même et représentent d'autant plus des demandes d'information de la part des pays membres[108]. Ils sont des actions proposées par le Conseil pour la considération des pays membres 'afin que ceux-ci pourront être mis en exécution, s'il est considéré opportun'.[109] Les Lignes directrices régissant la Sécurité des Systèmes d'Informations sont considérés dans cette catégorie.

Les comités au sein de l'OCDE sont des groupes spécialisés dans des domaines spécifiques tels que la politique économique, le commerce international, la science et la technologie, l'aide au développement ou les marchés financiers. Ils sont composés de spécialistes représentant les pays membres qui se réunissent et échangent des informations dans ce cadre. Ces représentants peuvent provenir soit des administrations nationales, soit des délégations permanentes auprès de l'OCDE à Paris. L'OCDE compte environ 200 comités, groupes de travail et sous-groupes techniques. Quelque 40 000 experts, qui sont généralement de hauts responsables des administrations nationales, qui participent chaque année aux réunions des comités de l'OCDE pour examiner les travaux réalisés par le secrétariat, et pour y apporter leur concours et suggérer de nouveaux travaux. Les comités font régulièrement appel aux participations extérieures de la part des entreprises (par le biais du Comité consultatif économique et industriel auprès de l'OCDE, le BIAC) et du travail (par la

---

[108] La Structure de l'Organisation consulter sur http://www.oecd.org/document/3/0,2340,en_2649_201185_2504067_1_1_1_1,00.html

[109] Voir article 5 de la Convention de l'OCDE disponible à http://www.oecd.org/document/44/0,2340,en_2649_34483_1915884_1_1_1_1,00.html

Commission syndicale consultative auprès de l'OCDE, le TUAC) ainsi que d'autres organisations non gouvernementales spécialisées. [110]

Le secrétariat est composé d'économistes, de statisticiens, de scientifiques, de conseillers juridiques, d'administrateurs et de personnel administratif qui secondent le travail des comités à l'aide de recherches, d'analyses, de collecte de données et de recommandations d'ordre politique. Le Secrétaire général est le lien important entre les pays Membres et le soutien technique. Il préside le Conseil et il gère le travail du secrétariat. [111]

L'OCDE est financée par ses pays membres. Le Conseil décide du montant du budget annuel ainsi que du programme de travail à entreprendre. Les contributions nationales au budget annuel sont fondées sur une formule qui est liée à la taille de chaque pays ainsi qu'à son économie. Les pays peuvent aussi faire des contributions volontaires pour des programmes ou projets spécifiques. Tous les pays ont une voix égale à l'OCDE, sans qu'il soit tenu compte de leur taille ou de leur contribution budgétaire.[112]

Comme il a été décrit précédemment, les Lignes directrices régissant la sécurité des systèmes d'information et de réseaux ont été élaboré par le Groupe Expert Ad-Hoc créé par le comité de la Politique de l'Information, de l'Informatique et des Communications (PIIC) par le rassemblement de différents acteurs parmi lesquels le BIAC fut le membre le plus affluent. D'où s'avère la nécessité de présenter dans un premier temps le PIIC et par la suite une étude plus détaillée du BIAC.

3. Le comité de la politique de l'information, de l'informatique et des communications au sein de l'OCDE (PIIC)

Le comité de la Politique de l'Information, de l'Informatique et des Communications (PIIC) a été fondé, en 1982, comme un organe consultatif de l'OCDE afin d'offrir aux pays membres la possibilité de suivre les problèmes de politique de

[110] Les Activites générales de l'OCDE disponible sur http://www.oecd.org/document/59/0,2340,en_2649_201185_2504123_1_1_1_1,00.html
[111] **Ibid.**
[112] **Ibid.**

l'information, de l'informatique et des communications de niveau national et international. La responsabilité de ce comité est d'examiner les questions liées au développement et à l'application des technologies dans le domaine des systèmes et services de l'information, de l'informatique et des communications, qui se posent aux États. Ces questions peuvent être relatives au commerce électronique et aux infrastructures d'information, aussi bien qu'aux impacts de ces problèmes sur l'économie et la société en général. D'autant plus, son rôle est aussi de renforcer la coopération dans ce domaine entre les pays membres et, dans certains cas, entre les pays membres et non-membres[113].

Le Comité est en particulier chargé de promouvoir entre les pays membres les échanges d'expériences sur le développement et l'application des technologies dans le domaine des systèmes et services de l'information, de l'informatique et des communications ainsi que sur les politiques nationales et internationales. Ses activités comprennent également l'analyse des évolutions dans ce domaine et d'informer les États membres sur les principales conséquences.

D'autre part, le comité est aussi responsable de soutenir le développement des infrastructures du domaine d'information, du commerce électronique, de la sécurité de l'information et de la protection de la vie privée aux niveaux national et international.

Le Comité maintient d'étroites relations de travail avec les autres organes appropriés de l'OCDE, avec les organismes régionaux et les autres organisations internationales qui poursuivent des activités dans le domaine de la politique de l'information, de l'informatique et des communications. Le Comité développe aussi, dans les cas nécessaires, un partenariat avec le secteur privé, les organisations syndicales et les groupes de défense de l'intérêt du public.[114]

Les États des pays industrialisés qui sont souvent faces aux problèmes politiques et aux décisions défiantes trouvent la possibilité de les débattre au sein de l'OCDE. Le comité consultatif économique et industriel auprès de l'OCDE (BIAC) agit dans le but d'élucider les questions relatives au domaine de l'industrie en tant que conseiller.

---

[113] OECD, **DSTI/ICCP/IIS**(2003)1/REV2, consulter sur http://www.oecd.org/dataoecd/38/19/2504315.pdf

[114] **Ibid.**

Il régit de même les relations formelles de l'OCDE avec les organisations non gouvernementales, les milieux d'affaires et les syndicats. Cependant, dans le cas de la sécurité des systèmes d'information, étant donné que l'expertise est détenue par le secteur privé, le BIAC apparaît en tant que détenteur principale de l'expertise dans ce domaine au sein de l'OCDE. Il est nécessaire de souligner que dans ce travail, le BIAC n'est pas considéré en tant qu'une communauté épistémique mais comme une communauté épistémique ressemblant (épistémic community like). Le trait qui le différencie de ces communautés est le fait que cette organisation dont le rôle est de fournir l'information et qui est formé d'experts et de représentants de l'industrie agit dans le but de protéger les intérêts d'un groupe précis, le monde des entreprises privées. Comme il le sera démontré dans la suite, dans l'élaboration des Lignes directrices pour la sécurité des systèmes d'information et de réseau, grâce à son expertise dominante dans ce domaine le BIAC a trouvé la possibilité d'agir en tant que la partie la plus influente.

4. Le comité consultatif économique et Industriel auprès de l'OCDE (le BIAC)

En mars 1962, le Conseil de l'OCDE a adopté une décision prévoyant des consultations avec les organisations internationales non gouvernementales, et a reconnu la Commission syndicale consultative auprès de l'OCDE (TUAC) comme étant la plus représentative du monde du travail et le Comité consultatif économique et industriel auprès de l'OCDE (BIAC)[115] comme étant le représentatif des milieux d'affaires.

Le BIAC se compose d'associations professionnelles et patronales des pays Membres de l'OCDE, et est donc représentatif des milieux d'affaires et de l'industrie dans le monde industrialisé. Comme l'OCDE, ses origines sont liées aux activités de l'OECE qui datent des années 1940. La reconstruction de l'Europe de l'Ouest et la création d'un nouvel environnement constituait les préoccupations majeures du comité d'entreprises. De plus, son objectif, était d'acquérir la possibilité de contrôler ces développements et d'y attribuer une influence. Par conséquent, au cours de la

[115] L'extension de BIAC est 'Business and Industry Advice Comity'

fondation de l'OCDE, les confédérations des employeurs des États membres se sont réunies sous le toit d'une organisation.[116]

Le BIAC tire principalement l'origine de son influence par la participation active des organisations d'employeurs d'économies puissantes comme les États Unis, la France, le Royaume Uni et l'Allemagne. Les échanges d'information entre le BIAC et l'OCDE se réalisent sous forme de consultations formelles et informelles à de niveaux variés. Le BIAC poursuit ses travaux par l'intermédiaire d'un réseau formé par des commités et des experts spécialisés dans des domaines variés. Ces groupes qui sont formés à base thématique sont destinés à se concentrer aux domaines comme l'éducation, l'emploi, les affaires sociaux, les investissements internationaux, la fiscalité et les progressions dans le champ de technologies d'information afin de pouvoir surveiller les activités de l'OCDE. [117]

A l'origine, le BIAC était plutôt toléré que encouragé par l'OCDE.[118] Toute fois, depuis les années 1970, l'influence de cette organisation a gagné une importance sérieuse, en particulier dans les champs politiques relatifs aux domaines des échanges, et de la libéralisation financière. Au commencement, son rôle dans le domaine de technologies d'information et de communication était principalement de fournir l'information revendiquée. Dans les années 1970, le BIAC a conduit une étude au sujet de l'impact de l'accroissement de l'utilisation des systèmes automatisés par les administrations gouvernementales. Il a également pris la responsabilité de donner des instructions concernant les développements dans le domaine de technologies de réseaux et de systèmes informatiques aux fonctionnaires représentatifs des pays membres. Son rôle en tant que conseiller et instructeur a permis au BIAC de participer à la constitution des Lignes directrices régissant la protection et la vie privée dans les années 1970, document qui démet les fondements des Lignes directrices régissant la sécurité des systèmes et réseaux d'information. Les relations avec le BIAC sont devenues un élément important du fonctionnement propre de l'OCDE. Elles sont basées sur un climat de confiance et d'acceptation mutuelle. [119]

---

[116] http://www.biac.org/Framebia.htm
[117] Ibid.
[118] Ibid.
[119] Relations avec le BIAC et le TUAC à consulter sur http://www.oecd.org/document/60/0,2340,fr_2649_201185_1910972_1_1_1_1,00.html

5. Le fonctionnement de la relation entre le BIAC et l'OCDE

Le BIAC participe à l'ensemble des activités de l'OCDE par des contacts informels comme par le biais du Programme travailleurs/ employeurs qui sont complétés par des contacts plus formels sur les plans aussi bien politique que technique. Le Programme travailleurs/employeurs de l'OCDE (LMP) géré par la Division des relations publiques, offre un autre cadre de contacts. Il comprend six réunions annuelles : deux avec des experts syndicaux, deux avec des experts patronaux, et deux auxquelles participent des experts des deux camps. Ces sessions permettent d'explorer avec des membres du personnel de l'OCDE des sujets d'actualité liés au programme de travail de l'OCDE. A chaque réunion, un rapport est rédigé par un rapporteur indépendant. Des consultations techniques permettent à des organes spécialisés du BIAC d'échanger leurs points de vue avec des groupes de travail émanant des comités de l'OCDE et avec le Secrétariat sur des sujets d'intérêt mutuel[120].

Les consultations avec le BIAC ont lieu dans le cadre de la Commission de liaison (du Conseil) avec les organisations internationales non gouvernementales, qui est présidée par le Secrétaire général et ouverte à tous les pays Membres. Des réunions distinctes se tiennent avec le BIAC chaque année. Ces consultations, auxquelles les membres du Secrétariat participent également, sont habituellement centrées sur un thème assez large lié aux travaux de l'OCDE, et sont organisées par la Division des relations publiques[121].

D'autres consultations concernant l'action des pouvoirs publics ont lieu entre le BIAC et le président ou les vice-présidents des comités de l'Organisation. Ces occasions de consultations revêtent une importance particulière lorsqu'elles ont lieu avec les responsables des comités de l'OCDE qui se réunissent au niveau des ministres, y compris à l'occasion de la réunion ministérielle annuelle du Conseil.[122]

---

[120] **Ibid.**
[121] **Ibid.**
[122] **Ibid.**

6. Les activités de l'OCDE dans le domaine de la sécurité des systèmes d'information précédent à l'élaboration des Lignes directrices et le rôle du BIAC

Les Lignes directrices régissant la protection et la vie privée peuvent être considérées comme le point de départ des activités en matière de recherche et de réglementation de l'OCDE dans le champ de sécurité des systèmes d'information. En 1982, l'OCDE a mis en discussion la relation entre la dépendance et la vulnérabilité ayant lieu dans une société d'information lors d'un séminaire réalisé avec la participation des membres d'organisations gouvernementales et d'entreprises.[123] Etant donné que les domaines de finance et d'échange internationaux sont amplement supportés par l'infrastructure fournie par les systèmes d'information, les thèmes des discussions étaient expressément consacrées aux conséquences qu'apportent à l'économie les vulnérabilités provenant de ces systèmes. En 1982, l'OCDE a lancé une enquête sur les implications économiques et politiques de la cybercriminalité dont l'accroissement a été contesté par les États et les entreprises. Il a été aperçu, immédiatement que les États membres ne montraient pas une volonté nécessaire pour l'adoption d'une approche internationale commune à l'encontre de cette nouvelle vague d'activités criminelles.[124] En 1986, un rapport important concernant le crime informatique a été élaboré, soulignant la nature croissante des crimes réalisés sur les réseaux d'information, aussi bien que le besoin pour une coopération plus renforcée qui permettrait d'affronter ces menaces. [125]

Ces activités de recherche étaient menées en raison des transformations sur le marché international de télécommunication et d'information dues à la privatisation et libéralisation de ces services dans les pays comme les États-Unis et le Royaume-Uni. Ce qui a poussé, par conséquent, les entreprises à devenir des acteurs indépendants ayant des intérêts commerciaux spécifiques différemment de leur rôle en tant que clients des services de télécommunications publics. Particulièrement, les objectifs essentiels du secteur privé étaient de promouvoir des services d'informations et de

---

[123] OCDE **Rapport Annuel 1982**, citation dans **OECD Observer,** "Computer Crime", no. 164, June-July 1990, p. 9-20
[124] OECD Observer, "Computer Crime", no. 164, June-July 1990, p. 9-20
[125] **Ibid.**

télécommunication à un marché mondial, c'est la raison pour laquelle se manifeste la nécessité de normes internationales.[126]

Ces conclusions étaient examinées officiellement lors d'une réunion du Comité de la Politique de l'Information, de l'Informatique et des Communications (PIIC) de l'OCDE en 1987, rassemblant les ministres et les hauts officiels gouvernementaux responsables des secteurs d'information et de télécommunication. Bien que cet évènement était désigné aux représentants étatiques, le BIAC était autorisé de présenter la perspective relative à la communauté d'entreprise. Il a commencé par exercer une pression sur les États Membres de l'OCDE d'accélérer le processus d'acquisition en matière d'équipements de services d'information et d'ordinateurs et de promouvoir la compétence ouverte et gratuite par l'intermédiaire de l'élimination des actions commerciales peu équitables pratiquées par les anciens monopoles de télécommunication. Le BIAC a de même suggéré la nécessité du retrait des régulations nationales qui s'opposent aux intérêts et objectifs spécifiques des entreprises dans leur voie menant à un succès commercial et financier à l'échelle mondiale. Et bien au-delà, le BIAC a proposé l'établissement de standards internationaux et des approches reflétant la nature globale des systèmes d'information et des réseaux.[127]

Au cours de cette réunion, le comité représentatif des entreprises cherchait à indiquer ses désaccords relatifs aux sujets suivants : la protection du caractère confidentiel des données, la croissance des fraudes informatiques et des flux d'informations soumis à aucune restriction à travers les réseaux internationaux et les systèmes informatiques. Le BIAC visait à être plus engagé parmi les fonctionnaires membres du comité (PIIC), responsable de la mise en œuvre des dispositions dans ce domaine, c'est-à-dire parvenir à faire écouter sa propre voix dans ce domaine. L'élaboration des Lignes directrices régissant la Sécurité des Systèmes d'Information constitue un exemple d'une évolution où les représentants d'entreprises, sous le toit du BIAC parviennent à annoncer leurs intérêts et leurs inquiétudes parmi les représentants des États et la Comité PIIC au sein de l'OCDE. Cette action est reflétée d'une manière

---

[126] **Ibid.**

[127] BIAC, **Annual Report 1987,** citation dans **OECD Observer,** "Computer Crime", no. 164, June-July 1990, p. 9-20

directe dans les Lignes directrices où il est indiqué explicitement que cet acte est adressé au secteur public aussi bien que privé.[128]

L'OCDE a donc envisagé de nombreuses activités concernant l'information, l'informatique et les technologies de réseaux qui ont constitué une base pour l'élaboration des Lignes directrices. L'implication du BIAC dans ce domaine est montrée comme les conséquences de la privatisation dans ces marchés et du nombre croissant des fraudes informatiques. Cependant, il est important de présenter une analyse du processus de négociation qui a mené à l'élaboration du texte finale des Lignes directrices régissant la sécurité des systèmes d'informations et de réseaux qui a impliqué la participation des États, du BIAC et des experts.

7. Le processus de négociation pour l'élaboration des lignes directrices

Les processus de négociations qui ont mené à l'acceptation des Lignes directrices par le Conseil de l'OCDE en Novembre 1992, avaient été lancés durant une réunion du comité PIIC en 1988. Les travaux sur ce sujet ont été entamés suite à la proposition du secrétariat de l'OCDE de considérer le problème de sécurité de l'information.[129] Cette demande a aussitôt reçu un support provenant de tous les pays, ce qui est un aspect important étant donné que les prises de décisions dans l'OCDE sont basées sur le consensus de tous les États membres.

Cependant, la perception du problème par les différents États-membres était variée. Les complexités provenant des éléments composants de la sécurité de l'information n'étaient pas exactement conçues de la même manière. La connaissance des représentants des États membres était limitée dans ce domaine, ce qui était en grande partie liée au fait que les recherches conduites dans le champ des technologies de l'information étaient restreintes aux domaines d'espionnage et de défense jusqu'au début des années 1990, époque où se sont répandus les ordinateurs et les technologies de réseau. Afin d'entamer des travaux efficaces à ce sujet, il était donc nécessaire d'améliorer le niveau de connaissance technique des représentants des

[128] OECD, **Guidelines Security for Information Systems**, 1992
[129] **Ibid.**, p.12

États membres dans ce sujet. D'autre part, un autre point à être élucidé pour les représentants des États membres était la manière dont le sujet de sécurité des systèmes d'informations était mené par les entreprises d'un point de vue juridique et administrative ; étant donné qu'à partir de la fin des années 1980, les services d'information, de télécommunication et de réseau ont subi une libéralisation et une privatisation dans certains États membres de l'OCDE.

Suite à cette première réunion, afin de constituer un encadrement initial du problème, le secrétariat de l'OCDE avait été convoqué pour la préparation d'un rapport détaillé concernant les problèmes législatifs et administratifs liés au problème de la sécurité des systèmes d'information et de présenter une synthèse générale sur les différentes expériences nationales des États membres. [130] Les découvertes ont été présentées sous forme de rapport officiel l'année suivante par le secrétariat de l'OCDE. [131] Les sujets principalement discutés dans le rapport étaient les implications commerciales et gestionnaires de la sécurité des systèmes d'information et le rôle des institutions gouvernementales dans cet environnement. De plus, des aspects essentiels liés à ce sujet étaient aussi accentués tels que les fonctionnalités de l'intégrité et de la disponibilité des systèmes d'information et de réseau, et le caractère confidentiel lié au transfert et à l'emmagasinage des donnés à travers ces systèmes. Un autre point important qui avait été mentionné était la nécessité de renforcer la confiance envers les technologies d'information et de réseau.[132] Durant la préparation de ce rapport, le secrétariat de l'OCDE a mené ses travaux en envisageant des entretiens avec les représentants des États membres mais aussi avec ceux des grandes entreprises. Les études de cas comprenaient également les institutions privées internationales en plus des institutions publiques. Le rapport soulignait particulièrement l'importance des entreprises pour la gestion du problème de sécurité de l'information et la dépendance du contrôle de la sécurité à celles-ci.[133] En effet, la disponibilité et l'intégrité continuelle des systèmes d'information et de réseau sont primordiales pour les entreprises dans l'accomplissement de leurs objectifs commerciales et financières. La participation des entreprises devient donc inévitable dans ce domaine.

---

[130] OCDE, **Rapport Annuel-1988**, cité dans Committee for Information, Computer, Communication Policy (ICCP)-OECD, **Information Network Security: A Project Report, OECD Document n.ICCP**, 1989

[131] Committee for Information, Computer, Communication Policy (ICCP)-OECD, **Information Network Security: A Project Report, OECD Document n.ICCP**, 1989

[132] **Ibid.**, p.9.

[133] **Ibid.**, p.8.

Un autre point qui avait été relevé était la dépendance croissante des organisations publiques et privées aux systèmes de réseaux confrontés de plus en plus à des perturbations. Malgré ces défis, les résultats de l'enquête avaient démontré que les organisations considérées dans les études de cas ne disposaient pas de niveaux suffisants pour la sécurité et la protection de leurs systèmes d'information et de réseaux. A cet égard, pour surmonter ces défaillances, il avait été suggéré dans le rapport que l'établissement d'organisations commerciales responsables des bases de contrôle pour la sécurité de l'information pourrait apporter une approche de solution. De plus, tout en soulignant que certaines caractéristiques de la sécurité de l'information débordent la capacité d'une organisation individuelle afin d'apporter une solution, le rapport s'entame en mentionnant la nécessité d'une coopération entre les entreprises et les États pour envisager ce sujet. [134]

Au cours des travaux, les représentants des entreprises ont bien accentué les implications provenant des divergences variées parmi lesquels peuvent être citées principalement les régulations nationales et l'insuffisance des services de sécurité procuré par les fournisseurs de télécommunication. Un point révélant qui a été mentionné et qui a été attribué aux organisations était la nécessité pour celles-ci d'équilibrer les éléments liés à la sécurité de l'information aux autres priorités tels que les coûts afin de surmonter les conséquences négatives du problème. Les organisations publiques et privées étaient donc menées à minimiser les effets négatifs provenant de la mauvaise utilisation des systèmes d'information en préparant les procédures nécessaires qui assisteraient à une réparation du système au cas de pénétrations illégales par des acteurs comme les hackers aux systèmes d'ordinateurs et de réseaux.[135] Afin de réaliser ces objectifs, la nécessité des mesures techniques, tels que systèmes de cryptographie, signatures digitales, messages d'authentification, logiciels de contrôle d'accès, et des procédures administratives étaient déterminées. [136] [137]

---

[134] **Ibid.**, p.5.
[135] **Ibid.**, p.19-20
[136] La cryptographie est la procédure de transformer des informations lisibles (texte) en des informations que seules les personnes autorisées peuvent lire. Au cours de ce processus, l'information est codée (chiffrée) de façon à ce que seul le destinataire puisse lire ou altérer le message. Il peut être intercepté mais n'est intelligible que pour la personne qui est capable de le décoder (déchiffrer). Le chiffrement et le déchiffrement nécessitent une formule mathématique (ou algorithme) pour convertir les données lisibles en un format codé et une clé. Une clé est un nombre unique, combiné avec du

Après avoir fourni un encadrement général concernant les aspects techniques et administratifs du sujet, le secrétariat de l'OCDE et les membres du comité de PIIC ont présenté une analyse des problèmes spécifiques relatifs à la sécurité de l'information destinée à être examinée par les représentants des États et des entreprises conjointement. De cette façon, un environnement approprié a été établi pour les processus de prise de décision où les complexités techniques et gestionnaires du problème qui constituaient un obstacle étaient minimisées.

Dans ce cadre, le secrétariat de l'OCDE et le comité de PIIC ont revendiqué une attention particulière vis-à-vis des politiques spécifiques et essentiels à envisager à cet égard ; comme la vie privée pour les données personnelles, les signatures digitaux pour les contrats électroniques, les fraudes et les défaillances provenant des systèmes d'information et de réseau, et finalement la question de juridiction pour les crimes informatiques.[138] Le point important, en particulier était l'indication de la nécessité de la préparation d'un ensemble unique à l'échelle internationale de Lignes directrices pour la sécurité de l'information pour les États et les entreprises. [139] Finalement dans le rapport, il a été conclu que la nature globale du problème nécessitait la réalisation d'une coopération au niveau international. Cette coopération devait prendre place entre les États et les entreprises et devait être basée sur le partage des expériences sur le sujet de ces derniers.[140]

---

texte pour produire un message chiffré ou une signature électronique. Les signatures électroniques, comme les signatures manuscrites, sont utilisées pour identifier les auteurs/co-signataires d'un e-mail ou d'autres données électroniques. Les signatures électroniques sont créées et vérifiées grâce aux certificats numériques. Des législations reconnaîssant et donnant une valeur légale aux signatures électroniques, la même valeur que les signatures manuscrites sont etablies au plans nationals et internationals. Pour signer des informations, pour opérer des transactions de façon sécurisée, la possesion d'un unique certificat numérique est necessaire. Les signatures électroniques offrent des fonctions telles que : authentification, confidentialité & intégrité des données et non-répudiation. L'authentification est la vérification de l'identité d'une personne (ou d'un hôte: serveur et client). Cela garantit l'identité de la personne qui a signé les données et qui a participé à une transaction et que celle-ci n'a pas été falsifiée. Cela permet de déterminer de façon irrévocable l'utilisateur qui tente d'accéder à un système grâce à la confirmation de son identité. Les logiciels de contrôle d'accès sont responsables de contrôler les entres et les sortis des transactions aux systèmes de réseau.

[137] Committee for Information, Computer, Communication Policy (ICCP)-OECD, **Information Network Security: A Project Report, OECD Document n.ICCP**, 1989, pp. 35-41

[138] **Ibid.**, p.35-41

[139] **Ibid.**, p.61

[140] Les principaux domaines d'expérience mentionnés pour les systèmes d'information étaient déterminés comme le domaine militaire et de défense pour les États et particulièrement le secteur bancaire pour le secteur privé.

Les points présentés dans ce rapport ont donné lieu à des discussions parmi les représentatifs des États membres. Certains aspects mentionnés nécessitaient une interprétation plus approfondie des aspects politiques contournant le problème c'est la raison pour laquelle le rapport a été soumis à l'évaluation des groupes d'experts par les représentatifs des États membres. L'objectif des groupes d'experts était d'examiner les conclusions déduites dans le rapport et de guider les représentants des États membres pour leurs suggestions d'instructions politiques au sein de l'OCDE. [141] On peut donc constater que dans certaines situations les États font appel à une expertise individuelle afin de concevoir la convenance des politiques élaborées par d'autres experts au sein d'une organisation internationale.

Le comité de PIIC, présidé par les États-Unis s'est réuni l'année suivante, en 1990, afin de discuter quelles seraient les politiques à envisager suivant le rapport de Sécurité de Réseau d'Information. [142] Cette réunion se distinguait des autres par le fait qu'il s'agissait d'une participation directe des représentatifs de la communauté des entreprises. Sous l'invitation du secrétariat, les membres de grandes entreprises tel que l'IBM ont contribué initialement en présentant leurs perceptions et de leurs perspectives sur les aspects de la sécurité et de l'assurance de l'information[143]. L'objectif principal du secrétariat était la réalisation d'un consensus parmi les États membres pour l'élaboration de Lignes directrices qui seraient acceptées par les représentants des entreprises.

Suite à cette réunion, les représentants des États membres se sont consentis sur la création par le comité de PIIC d'un groupe d'expert ad hoc qui serait responsable de l'élaboration de lignes directrices pour la sécurité des systèmes d'information. Ce groupe était composé des délégués d'États, des académiciens originaires des domaines tels que le droit, les mathématiques et l'informatique et des représentants du secteur privé réunis sous le toit du BIAC.[144] Comme il sera démontré dans la suite, aux cours des processus de négociation le principal sujet de désaccord était lié au sujet du caractère confidentiel des donnés et son implication sur la sécurité nationale. La majorité des membres de cette communauté détenait une connaissance

---

[141] OECD, **Guidelines for the Security of Information Systems** 1992, p.19
[142] **Ibid.**, p.21
[143] **Ibid.**, p.21
[144] OECD, **Guidelines for the Security of Information Systems,** 1992, p.3

étendue sur les détails des aspects techniques liés à la sécurité de l'information, en particulier sur la protection des données. Par conséquent, au cours des processus de négociation durant la préparation des Lignes directrices, les membres de cette communauté d'experts ont principalement apporté des solutions techniques et gestionnaires concernant la protection et le caractère confidentiel des systèmes d'information et de réseau. Ces principes se distinguaient en effet des objectifs des entreprises et de ceux des États qui étaient préférablement concentrés sur les questions de disponibilité et de l'intégrité des systèmes de réseau.

Les représentants des entreprises étaient réunis sous le toit du BIAC. L'intérêt commun de cette délégation était la réalisation d'une coopération dans le but de concevoir un document où seraient reflétés leurs intérêts et leurs objectifs. Les représentants des entreprises comme l'IBM et le Digital Equipement avaient participé aux processus de négociation en tant que membres du BIAC. Leur intérêt principale était la conception de standards communs du point de vue technique et gestionnaire et de codes de conduite appropriés dans le domaine de la sécurité des systèmes d'information et de réseaux.[145] Les autres représentants du BIAC étaient originaires d'entreprises transnationales des champs pharmaceutique et financière comme le Ciba-Geigi et le Groupe Midland. Similairement à l'IBM et au Digital, l'attente de ces entreprises était la mise en place de normes internationales pour la sécurité de l'information et des réseaux.[146]

Dans l'établissement d'un environnement solide pour les flux d'information, au-delà de leur volonté pour la protection de leurs secrets industriels, un des soucis majeurs des entreprises était les risques existant pour les provisions financières et les validations des signatures électroniques, des éléments importants dans la gestion des opérations de ces industries. D'autres membres du groupe de BIAC étaient composés des entreprises de consultant dont les objectifs étaient semblables à celles citées auparavant, tel que la mise en place de normes à l'échelle mondiale pour la sécurité des systèmes d'informations et de réseaux qui favoriseraient leurs activités d'audit de manière plus effective. [147]

---

[145] **Ibid.**, p.6.
[146] **Ibid.**
[147] **Ibid.**

En raison de la nature complexe du problème de sécurité des systèmes d'information et de réseaux, les négociations qui ont mené à l'élaboration du texte final des Lignes directrices ont pris lieu suite à cinq réunions réalisées par le groupe d'expert, entre la période janvier 1991 et septembre 1992. [148]

Comme mentionné préalablement, les divergences des opinions entre les représentants des États membres et celles des entreprises reposaient principalement sur les questions liées au caractère confidentiel des informations, l'accessibilité et l'ouverture de leurs systèmes aux solutions technologiques comme l'encryptage par exemple. La préoccupation des États convergeait sur les effets potentiels qu'auraient ces revendications sur la sécurité nationale puisque l'ouverture de leurs systèmes d'informations pouvait apporter des conséquences inattendues. Dans ce cadre, un nouveau groupe d'experts a été assigné afin d'évaluer l'impact sur la sécurité nationale des activités du secrétariat de l'OCDE et du comité PIIC, avant la première réunion du Groupe d'Expert. Ce travail a permis d'accélérer le processus de négociation.[149] Au cours de la première réunion, les différentes interprétations des participants sur l'ouverture de l'accès à l'information ont immédiatement donné lieu à des débats. Il s'agissait d'une revendication du partage d'information entre les différents acteurs, les États et les entreprises en particulier, concernés par le problème de sécurité et d'assurance de l'information.[150] Le partage de l'information était donc primordial pour l'élaboration des technologies et des procédures relatives à la gestion du problème de sécurité de l'information. D'autre part, dans cette première forme du texte des Lignes directrices, les tâches attribuées aux États et aux entreprises étaient exprimés de la manière suivante ; « les États sont menés à mettre en place des mesures législatives et administratives, des pratiques et des institutions pour établir la sécurité des systèmes d'informations et la sécurité des donnés », alors que « les entreprises sont menés à établir des codes de conduite, des procédures et des institutions pour assurer la sécurité des systèmes d'information ».[151] Considérant la dépendance des États et des entreprises aux technologies d'information et aux réseaux globaux, la nécessité de partager l'information entre ces derniers pour des fins engendrant des solutions vis-à-vis de la sécurité, a été un aspect exclusivement

---

[148] **Ibid.**, p.3
[149] ICCP-OECD, **Ad-Hoc Meetings on Experts on the Security of Information Systems-Draft Guidelines for the Security of Information Systems. DSTI/ICCP/AH (90)(REV1)**(20), 1991. p.8
[150] **Ibid.**, p 9
[151] **Ibid.**, p.11

souligné par le secrétariat de l'OCDE au cours des négociations pendant la première réunion avec le groupe d'expert.

Cette approche où le caractère confidentiel de l'information et son implication sur la sécurité nationale sont évoqués, n'a pas trouvé une approbation par les États, au cours de la deuxième réunion. Ceci a donné lieu à l'emprise de révision, par cette occasion, les représentants des États-Unis ont proposé qu'il serait convenable d'ajouter la phrase suivante : « *chaque État a la responsabilité exclusive d'assurer la sécurité des données, de l'information et des systèmes d'information au cas de situations jugés nécessaires pour la protection de ses intérêts nationaux* » dans le texte des lignes directrices. [152] De cette manière, les réactions provenant des États liées sur la question des frontières nationales ont été amplement amoindries. Cependant, les représentants du BIAC ont immédiatement réagi à cette suggestion car leur objectif principal pour la question de sécurité était l'établissement de politiques communes, basées sur les Lignes directrices prenant lieu entre le secteur privé et public. D'après ces derniers, il n'était pas rationnel qu'un État soit responsable individuellement de la gestion du problème de sécurité de l'information qui est d'aspect global. De plus, cette mesure formait un obstacle pour la coordination des économies nationales, la protection des échanges, la protection de la vie privée des données et de la propriété intellectuelle aussi bien qu'industrielle ; alors que ces objectifs avaient été envisagés dans la forme initiale des lignes directrices.[153] Essentiellement, cette demande de la part des États d'une responsabilité particulière dans le domaine de sécurité et de l'assurance de l'information n'a pas trouvé le soutien indispensable de la part des autres acteurs, en particulier du BIAC.

Des solutions appropriées ont été apportées par la suite au cours des réunions suivantes du groupe expert pour ces conflits liés à la question de confiance en relation avec la sécurité nationale. Au cours de la troisième réunion, dans ce but des différentes approches ont été proposées par les délégués des États et les représentants du BIAC. D'abord, ils ont suggéré que les Lignes directrices ne devraient pas être appliquées aux systèmes d'information et de réseau spécifique qui concernent la

---

[152] ICCP-OECD, **Ad-Hoc Meetings on Experts on the Security of Information Systems-Draft Guidelines for the Security of Information Systems. DSTI/ICCP/AH (90)(REV2)**(20), 1991. p.4
[153] **Ibid.**, p.7

souveraineté des États, tels que les environnements militaires et d'espionnage. Ensuite, ils ont affirmé que les déviations possibles qui proviendraient de l'application des Lignes directrices pour raison de sécurité nationale pouvaient apparaître mais seulement en conformité avec la loi. Finalement, dans la dernière proposition, il était exprimé que « *les lignes directrices ne sont pas habilitées d'affecter le droit de tout État de prendre action, en conformité avec ses lois nationales, dans l'intérêt de la sécurité nationale, dans le but de lutter contre le crime, pour la sûreté économique de la nation* ».[154] Dans un autre sens, les États pouvaient concevoir des solutions techniques relatives à la sécurité d'information strictement confidentielle pour les situations impliquant les réseaux militaires et d'espionnage.

Par la suite, au cours de la quatrième réunion, qui a pris place pour les processus de négociation, une nouvelle possibilité d'alternative qui confirme la relation entre le caractère confidentiel de l'information et la sécurité nationale a été proposée ; celle-ci était reliée à une loi spécifique et proposait que les Lignes directrices devaient être toujours soumises aux demandes des lois nationales et ne devraient pas être appliquées aux systèmes d'information liés à la sécurité nationale et l'ordre publique.[155]

Et finalement, durant la cinquième réunion, les désaccords ont abouti à une fin avec l'initiative d'une délégation d'États menés par les États-Unis, qui ont suggéré de citer les mesures sur le sujet du caractère confidentiel et ses implications sur la sécurité nationale dans le texte de la Recommandation du Conseil de l'OCDE au lieu de les citer dans celui des Lignes Directrices[156]. Cependant, cette approche a été contestée par la délégation du BIAC qui avaient affirmé que les États pouvaient restreindre lorsqu'ils envisageraient nécessaire leurs accès aux solutions techniques et gestionnaires liés à la sécurité de l'information, sous le prétexte de sécurité nationale. C'est la raison pour laquelle ils ont revendiqué l'ajout de la phrase « en conformité avec la loi » à la division en question. Cette suggestion provenant du BIAC a été

---

[154] ICCP-OECD, **Ad-Hoc Meetings on Experts on the Security of Information Systems-Draft Guidelines for the Security of Information Systems. DSTI/ICCP/AH (90) 21 (REV3).** p.2, 1991
[155] ICCP-OECD, **Ad-Hoc Meetings on Experts on the Security of Information Systems-Draft Guidelines for the Security of Information Systems. DSTI/ICCP/AH (90) 21 (REV4).** p.3, 1992
[156] ICCP-OECD, **Ad Hoc Meeting on Experts on the Security of Information Systems-Summary Record of the Fifth Meeting of the Ad-Hoc Meeting on Experts on Guidelines for the Security of Information Systems. DSTI/ICCP/AH/M (92)**, 1992, p.5

acceptée par le Groupe d'Expert, par conséquent le consensus concernant le texte final des Lignes directrices a été atteint. [157]

Au départ, les Lignes directrices étaient conçues pour être appliquées à tout système d'information et de réseau sous l'utilisation des organisations publiques aussi bien que privés. En particulier, comme il avait été accentué par les représentants des États et des membres du BIAC originaire des États-Unis, la diffusion de ce document constituait un point essentiel. De plus, dans le but d'éviter l'élaboration d'un document similaire, les États membres de l'OCDE étaient convoqués à prendre les précautions nécessaires. [158] En ce qui concerne les déviations possibles pouvant prendre lieu durant l'exécution des Lignes directrices, celles-ci devaient être communiquées aux parties prenantes. [159] Cette explication comporte une importance par le fait que les dispositions et les approches procédurales qui sont établies initialement dans le but d'apporter une solution pour la question de la sécurité de l'information peuvent dans la suite être élaborées de façon à répondre aux intérêts des entreprises. L'objectif des entreprises, comme il a été mentionné précédemment à plusieurs reprises, était en effet la mise en place d'une série de normes qui favoriseraient le partage de l'information et la connaissance technique détenue par les différentes parties, dans le but d'améliorer l'intégrité et la disponibilité des systèmes d'information et de réseau à une échelle internationale. Une dernière réunion du Groupe d'Experts s'est réalisée finalement afin de conclure le texte final des Lignes directrices et la partie de la Recommandation, avant d'être adopté et publié par le Conseil en Novembre 1992.

Au cours de ces processus de négociations, les principaux soucis des États provenaient de leurs doutes en ce qui concerne le caractère confidentiel pour les procédures techniques et gestionnaires sur la sécurité nationale, en particulier celles liées aux domaines militaires et d'espionnage. D'autre part, au cours des négociations, les États ont réagi tout en considérant la dépendance croissante de leurs infrastructures économiques et sociales et de leurs activités administratives aux systèmes d'information et de réseaux qui sont désormais détenus par les acteurs privés suite à la libéralisation rapide et la privatisation des secteurs de

---

[157] **Ibid.**
[158] **Ibid.**, p.5
[159] **Ibid.**, pp.12-13

télécommunication. En ce qui concerne le cas des représentants du BIAC, ils ont réussi à faire inclure leurs intérêts sur l'intégrité pour la protection de la vie privée des données personnelles et la protection de la propriété intellectuelle et individuelle, ainsi que la disponibilité des systèmes d'information et des réseaux au texte finale des Lignes directrices, en particulier en conjonction avec le partage du savoir au niveau mondial sur les aspects techniques et gestionnaires des procédures. Néanmoins, dans ce contexte, ils ont évalué l'importance du caractère confidentiel dans le domaine de sécurité nationale.

Afin de mesurer l'impact des Lignes directrices parmi les États membres, suite à l'adaptation de celles-ci, le comité du PIIC a entamé une enquête parmi les États membres de l'OCDE. Les résultats ont démontré qu'une série d'activités - tels que l'établissement de législation et de développement de standards- visant à favoriser l'exécution des Lignes directrices à l'échelle nationale et internationale, avaient été initiés par les États membres.

Les Lignes directrices sur la sécurité qui ont été achevées en 1992 puis réexaminées en 1997 ont été mises à jour en 2001 par le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP), afin de refléter les réseaux d'informations caractérisé par Internet, dans le cadre d'un mandat donné par le Comité PIIC, et accéléré suite à la l'évènement du 11 septembre.[160]

8. Les lignes directrices régissant la sécurité des systèmes d'informations et de réseaux : vers une culture de la sécurité

Les présentes 'Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité' ont été adoptées sous la forme d'une Recommandation du Conseil de l'OCDE lors de sa 1037ème session, le 25 juillet 2002.[161] Afin de contribuer aux travaux relatifs aux révisions des lignes directrices, le BIAC a préparé un document dans lequel sont énoncés un certain nombre de problèmes et de champs à considérer par l'OCDE et les pays membres.

---

[160] OECD, **Guidelines for the Security of Information Systems: Towards a Culture of Security,** 2002

[161] OCDE, **Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité**, p 28

Depuis 1992, date à laquelle l'OCDE a rendu publique les Lignes directrices régissant la sécurité des systèmes d'information, le degré d'utilisation des systèmes et des réseaux d'information et l'environnement des technologies de l'information ont subi une évolution importante dans son ensemble. Ces évolutions constantes ont offert des avantages significatifs mais requis également que les gouvernements, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'information, portent une plus grande attention à la sécurité.

L'objectif principal des Lignes directrices était de renforcer la disponibilité, la confidentialité et l'intégrité des systèmes d'information et d'améliorer la perception de confiance envers les instruments de communication. Afin d'aboutir à cet objectif, l'OCDE cherchait à développer la conscience générale concernant les risques liés aux systèmes d'information, de plus, à établir des normes qui permettront la mise en place d'un cadre international de mesures de prises de décisions, de pratiques et procédures pour la sécurité. Les Lignes directrices font appel à une harmonie internationale de standards techniques, de méthodes et de codes, de plus à la promotion d'expertise en vu de sécurité d'information.[162]

En effet, dans le document, la nécessité d'une coopération effective au niveau nationale aussi bien qu'internationale entre le secteur privé et public est soulignée. Finalement, comme indiqué dans le texte de la Recommandation de l'OCDE en annexe aux Lignes directrices, les dispositions cités dans cet acte ne sont pas destinées à affecter les droits de souveraineté des États en matière de sécurité nationale et d'ordre public mais de demeurer à l'initiative des lois nationales.

Dans les Lignes directrices, les objectifs et les normes liées à sécurité des systèmes d'information sont invoqués comme principes. Les présentes Lignes directrices s'adressent à l'ensemble des parties prenantes à la nouvelle société de l'information, et suggèrent le besoin d'une prise de conscience et d'une compréhension des questions de sécurité accrues, ainsi que la nécessité de développer une « culture de la sécurité ».

---

[162] OECD, **Guidelines for the Security of Information Systems,** 1992

Ces Lignes directrices répondent à un environnement en constante évolution en faisant appel à un développement d'une culture de la sécurité – ce qui signifie la nécessité de porter une attention importante à la sécurité lors du développement des systèmes d'information et des réseaux et d'adopter de nouveaux modes de pensée et de comportement lors de l'utilisation de ces systèmes dans le cadre des échanges. Les Lignes directrices marquent de même une rupture nette avec un temps où la sécurité n'intervenait que trop souvent de façon incidente dans la conception et l'utilisation des réseaux et systèmes d'information. Les parties prenantes sont de plus en plus tributaires des systèmes d'information, des réseaux et des services qui leur sont liés, c'est la raison pour laquelle ceux-ci doivent être fiables et sécurisés. Seule une approche prenant dûment en compte les intérêts de toutes les parties prenantes et la nature des systèmes, réseaux et services connexes peut permettre d'assurer une sécurité efficace. [163]

En ce qui concerne les rôles des partis prenantes pour assurer la sécurité, il est souligné que chacun, en fonction du rôle respectif, doit être sensibilisé aux risques liés à la sécurité ainsi qu'aux parades appropriées, doit assumer ses responsabilités et prendre des mesures de nature à améliorer la sécurité des systèmes et réseaux d'information. [164]

Pour l'instauration d'une culture de la sécurité, une nécessité à la fois d'une impulsion et d'une large participation se traduisant par une priorité renforcée donnée à la planification et la gestion de la sécurité, ainsi que par une compréhension de l'exigence de sécurité par l'ensemble des participants est considérée. Les questions de sécurité doivent être un sujet de préoccupation et de responsabilité à tous les niveaux du gouvernement et des entreprises et pour l'ensemble des parties prenantes.

L'objet principal des Lignes directrices était d'encourager parmi l'ensemble des parties prenantes une culture de la sécurité en tant que moyen de protection des systèmes et réseaux d'information et de promouvoir une plus grande confiance envers les systèmes et réseaux d'information. Afin d'accomplir ces objectifs, l'OCDE visait le renforcement de la sensibilisation aux risques pour les systèmes et

---

[163] OCDE, **Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité**, p 27

[164] **Ibid.**

réseaux d'information, aux politiques, pratiques, mesures et procédures disponibles pour faire face à ces risques, ainsi qu'à la nécessité de les adopter et de les mettre en œuvre. C'est dans ce but qu'il considère de créer un cadre général de référence qui aide les parties prenantes à comprendre la nature des problèmes liés à la sécurité, et à respecter les valeurs éthiques dans l'élaboration et la mise en œuvre de politiques, pratiques, mesures et procédures cohérentes pour la sécurité des systèmes et réseaux d'information.

Les Lignes directrices font appel à une harmonie internationale nécessitant la prise en considération de la sécurité en tant qu'objectif important parmi toutes les parties prenantes nécessitant la coopération et le partage d'information appropriées pour l'élaboration et la mise en œuvre des politiques, pratiques, mesures et procédures pour la sécurité.

Finalement, le document de Recommandation, figurant en annexe aux Lignes directrices, indique que les dispositions mentionnées dans cet acte sont d'application volontaire et n'affectent pas les droits souverains des États.

Ces objectifs peuvent être atteints par les États et les entreprises, comme suggéré par le document, en établissant de nouvelles politiques, pratiques, mesures et procédures ou de modifier celles qui existent pour refléter et prendre en compte les 'principes' ou normes de sécurité d'information mentionnée dans les Lignes directrices.

Tout d'abord, les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité puisque que les défaillances de sécurité peuvent gravement porter atteinte aux systèmes et réseaux sous leur contrôle mais aussi, du fait de l'interconnectivité et de l'interdépendance, à ceux d'autrui (*le Principe de Sensibilisation*). Il est nécessaire que ces parties prenantes soient responsables de la sécurité des systèmes et réseaux d'information (*le Principe de Responsabilité*). Du fait de l'interconnectivité des systèmes et réseaux d'information et de la propension des dommages à se répandre rapidement et massivement, il est conseillé aux parties prenantes de réagir avec promptitude et dans un esprit de coopération (échange d'information et mise en place des procédures pour une

coopération rapide et efficace) pour prévenir, détecter et répondre aux incidents de sécurité (*le Principe de Réaction*). Une conduite éthique est donc indispensable et les parties prenantes doivent s'efforcer d'élaborer et d'adopter des pratiques exemplaires et de promouvoir des comportements qui tiennent compte des impératifs de sécurité et respectent les intérêts légitimes des autres parties prenantes (*le Principe de Éthique*). La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique et notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des informations de caractère personnel, l'ouverture et la transparence (*le Principe de Démocratie*). L'évaluation des risques permet de déceler les menaces et vulnérabilités, une fois réalisée permettra de déterminer le niveau acceptable de risque et facilitera la sélection de mesures de contrôles appropriées pour gérer le risque de préjudices possibles pour les systèmes et réseaux d'information compte tenu de la nature et de l'importance de l'information à protége, les parties prenantes doivent donc procéder à des évaluations des risques (*le Principe d'Évaluation des risques*). [165]

Les systèmes, réseaux et politiques doivent être conçus, mis en œuvre et coordonnés de façon appropriée afin d'optimiser la sécurité et les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information. La conception et l'adoption de mesures de protection et solutions appropriées afin de prévenir ou limiter les préjudices possibles liés aux vulnérabilités et menaces identifiées. Les mesures de protection et solutions doivent être à la fois techniques et non techniques et être proportionnées à la valeur de l'information dans les systèmes et réseaux d'information de l'organisation (*Le Principe de Conception et mise en œuvre de la sécurité*). [166]

Il est important que la gestion de la sécurité soit fondée sur l'évaluation des risques et soit dynamique et globale afin de couvrir tous les niveaux d'activités des parties prenantes et tous les aspects de leurs opérations. Elle doit inclure également des réponses aux menaces émergentes et couvrir la prévention, la détection et la résolution des incidents, la reprise des systèmes, la maintenance permanente, le

[165] **Ibid.**
[166] **Ibid.**

contrôle et l'audit. Les politiques de sécurité des systèmes et réseaux d'information, les pratiques, mesures et procédures en matière de sécurité doivent être coordonnées et intégrées pour créer un système cohérent de sécurité. Les exigences de la gestion de la sécurité sont fonction du niveau de participation, du rôle de la partie prenante, des risques en jeu et des caractéristiques du système (*Le Principe de Gestion de la sécurité*). [167]

Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité. Etant donné que des vulnérabilités et menaces nouvelles ou évolutives sont constamment découvertes, tous les aspects de la sécurité doivent être continuellement revu, réévalué et modifié pour faire face à ces risques évolutifs (*Réévaluation*).[168]

9. L'application des lignes directrices aux procédures de régulations

Le développement des lignes directrices régissant la sécurité des systèmes d'information a permis aux États aussi bien qu'aux firmes privées de réviser leurs procédures de régulation relatives à la sécurité des systèmes d'information et d'en élaborer de nouvelles. Ces efforts ont été réalisés dans les procédures de législation, d'autorégulation tels que les standards, les codes de conduite et de ligne de conduite.

Plusieurs pays de l'OCDE avaient déjà arrangé des législations spécifiques concernant la sécurité des systèmes d'information. L'adoption des lignes directrices leur a permis de remplir les lacunes et d'améliorer leur système législatif consacré à ce domaine. A titre d'exemple, 'l'Acte de Fraude et d'Abus Informatique' des Etats-Unis qui a été modifié en septembre 1994, s'adresse spécifiquement au crime

[167] **Ibid.**
[168] **Ibid.**

informatique. Dans sa nouvelle forme, révisé sur la base des lignes directrices, la loi a recouvert en particulier l'accès non autorisé aux réseaux et aux ordinateurs[169].

En ce qui concerne l'autorégulation, il existe plusieurs formes de mesures adoptées par les firmes ou l'industrie dans ce but comme les lignes de conduite internes ou les principes, les codes de conduite et les standards. Les standards au niveau nationale et internationale peuvent être considérés comme une combinaison des autorégulations et des 'régulations des marchés'. Dans ce cadre, l'approche prise par l'Australie était d'incorporer les principes des lignes directrices de l'OCDE dans l'avant propos des standards promulgués et d'indiquer la convenance des standards aux lignes directrices. De plus, ces standards ont été utilisés avant que la législation a été décrétée, de cette façon leurs applicabilités aient pu être testés[170].

Les codes de conduite permettent de développer et d'établir une politique transparente dans un domaine précis et dans certains cas ils peuvent être établis sous le toit de la législation. A titre d'exemple, il est nécessaire de mentionner l'initiative au Royaume-Uni pour l'élaboration du Standard Britannique pour la Gestion de la Sécurité en matière d'Information, dont la première phase était la mise en place du *Code de Pratique pour la Gestion de la Sécurité en matière d'Information*, ce qui complète les lignes directrices de Sécurité de l'OCDE. Le code avait était élaboré par le département d'Echanges et d'Industrie, les Institutions de Standards Britanniques et un groupe composé des grandes entreprises multinationales afin de fournir une approche pratique aux organisations pour une gestion sure de leurs ressources en matière de technologies d'information. Ce code qui a été adopté comme Standard Britannique en 1994, a servi de modèle dans bien d'autres pays dans la mise en place de leurs propres codes[171].

---

[169] OECD, **Report of the Ad-Hoc Meeting of Experts on Information Infrastructure, Issues Related to Security of Information Systems and Protection of Personal Data and Privacy**, Paris, 1996, OECD Working Papers 1022-2227 v.4, no 38, p.50

[170] **Ibid.**, p.52

[171] **Ibid.**, p.53

CONCLUSION

Le caractère transnational d'Internet constitue un obstacle pour les États d'envisager le problème de la cybercriminalité dans le cadre de leurs territoires nationaux. Pour la mise en place d'une stratégie commune concernant le renforcement de la sécurité sur les réseaux informatiques, des travaux variés ont été entamés par certaines organisations internationales. En effet, les intrusions illégales réalisées par des réseaux illicites sur Internet et les flux de l'information qui y circule surpassent les frontières étatiques. Par conséquent la réglementation et le contôle dans ce nouvel espace nécessite des accords juridiques avec une coopération des États au niveau international. De plus, la difficulté du contrôle du cyberespace provient largement de l'architecture d'Internet, ce qui nécessite une expertise technique dans ce domaine.

Dans ce cadre, afin d'accorder une assistance aux organisations publiques et privées lors de leurs activités de réglementation en ce qui concerne la sécurité des systèmes d'information et de réseaux, l'Organisation de Coopération et de Développement économique (OCDE) a établi un document : les Lignes directrices pour la sécurité des systèmes d'information et de réseau. L'objectif de ce document était de souligner l'importance des risques liés aux systèmes d'information et de réseaux, tout en faisant appel à la nécessité de surveillance et de standard au niveau international.

L'élaboration des lignes directrices a été réalisée suite à une série de processus de négociation prenant lieu entre les membres d'un groupe d'expert. Ce groupe était composé de délégués d'États, d'académiciens originaires des domaines tels que droit, mathématiques et informatique et des représentants d'entreprises réunis sous le toit du comité consultatif économique et industriel (BIAC). Toutefois parmi les membres de ce groupe, c'est le BIAC qui a été le plus influant.

Le rôle principal du BIAC, composé d'associations professionnelles des pays Membres de l'OCDE est d'agir dans le but d'élucider les questions relatives au domaine de l'industrie en tant que conseiller au sein de l'OCDE. Cependant, son

implication dans le domaine de l'information, l'informatique et les technologies de réseaux est plus différente. Ceci est dû au fait que les infrastructures des télécommunications sont désormais détenues en grande partie par les entreprises privées suite à la vague de privatisation dans les années 1990, alors qu'elles étaient maîtrisées par des opérateurs publics. Les entreprises privées sont donc responsables de la conception, de l'établissement et de la mise en fonctionnement des infrastructures des technologies d'information. C'est la raison pour laquelle le BIAC apparaît en tant que détenteur principale de l'expertise et du savoir dans ce domaine parmi les autres membres du Groupe d'Expert. Toutefois, le BIAC n'est pas considéré comme une communauté épistémique mais plutôt catégorisé comme une 'communauté épistémique ressemblant' (épistémic community like) considérant la classification de Peter Haas en ce qui concerne les différent groupes de savoir. Le trait qui le différencie des communautés épistémiques est le fait que cette organisation dont le rôle est de fournir l'information et qui est formé d'experts et de représentants de l'industrie agit dans le but de protéger les intérêts d'un groupe précis, celui des entreprises privées.

L'intérêt commun des représentants du BIAC était la réalisation d'une coopération avec les États pour la mise en place d'une série de normes et de de standards communs qui favoriseraient le partage de l'information et la connaissance technique détenue par les différentes parties, dans le but d'améliorer l'intégrité et la disponibilité des systèmes d'information et de réseau à une échelle internationale. Toutefois, d'un point de vue technique, la conception d'une règlementation commune, nécessitait l'ouverture à l'accès des systèmes de réseaux détenus par les deux deux parties, ce qui a constitué le sujet principal des débats au cours des processus de négociations.

La préoccupation des États convergeaient sur les effets potentiels qu'auraient ces revendications sur la sécurité nationale puisque l'ouverture de leurs systèmes d'informations pouvait apporter des conséquences inattendues, particulièrement sur les réseaux militaires et d'espionnage. Sur ce fait, suite à plusieures révisions de cette approche, bien qu'il eut été proposé par les représentants des États membres de laisser l'initiative aux États d'assurer eux-mêmes la sécurité des données et des systèmes d'information dans les cas jugés nécessaires pour la protection de leurs

intérêts nationaux, cette suggestion n'a pas trouvé le support du BIAC dont objectif principal était l'établissement de politiques communes.

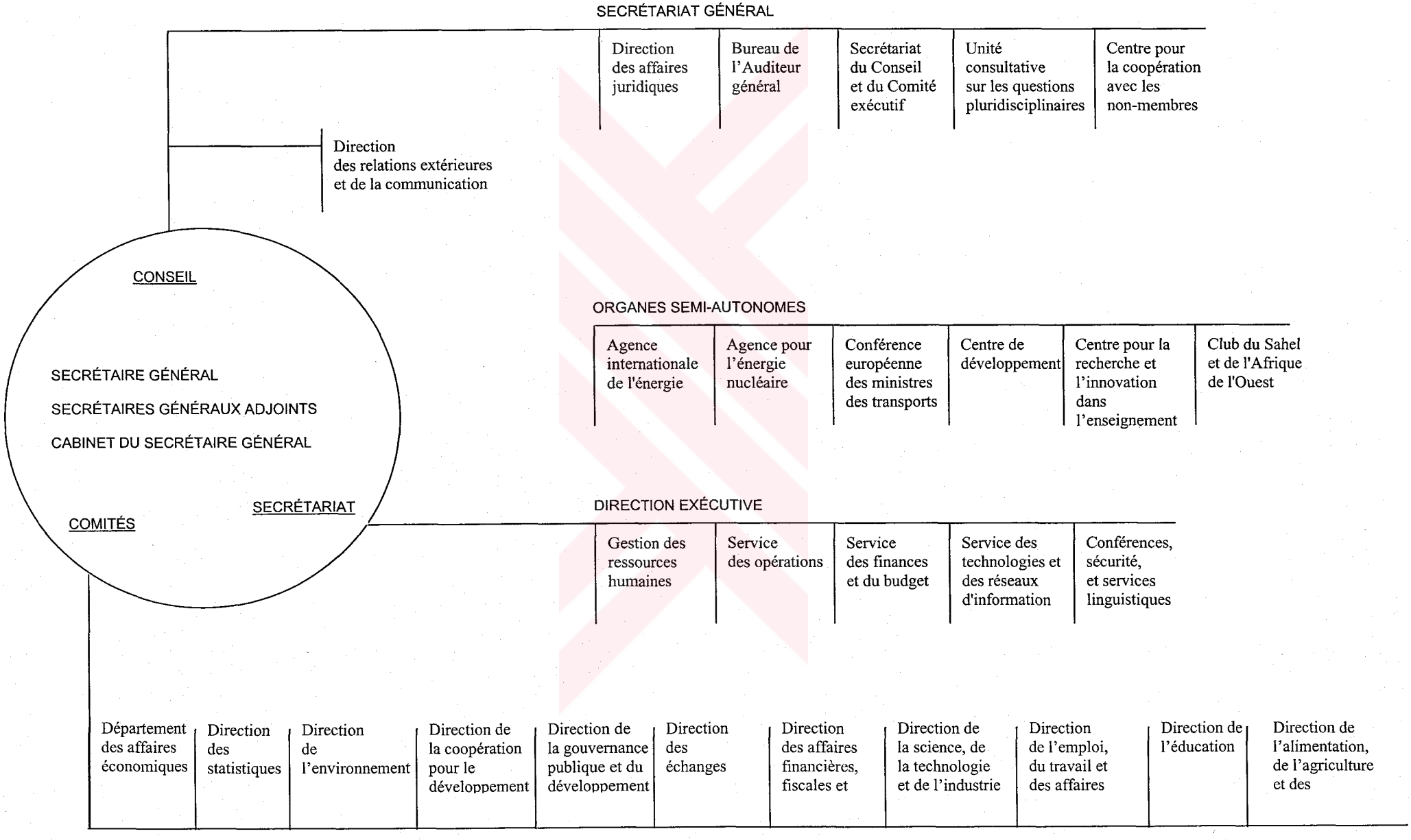
Les négociations ont pris fin par la décision de citer les mesures liées au sujet du caractère confidentiel et de ses implications sur la sécurité nationale dans le texte de la Recommandation du Conseil de l'OCDE au lieu de les citer dans celui des Lignes directrices mais tout mettant en place, avec la proposition du BIAC, les dispositions limitant les États de ne pas restreindre l'ouverture aux solutions techniques et gestionnaires de leurs systèmes liés à la sécurité de l'information, sous le prétexte de sécurité nationale.

Au cours des négociations, les États ont réagi tout en considérant la dépendance croissante de leurs infrastructures économiques et sociales et de leurs activités administratives aux systèmes d'information et de réseaux qui sont désormais détenus par les acteurs privés. En ce qui concerne le cas des représentants du BIAC, ils ont réussi à faire inclure leurs intérêts liés à l'intégrité et la disponibilité des systèmes d'information et de réseau pour la protection de la vie privée des données personnelles et la protection de la propriété intellectuelle au texte finale des Lignes Directrices, en particulier en conjonction avec le partage du savoir au niveau mondial des aspects techniques et gestionnaires des procédures.

Ainsi, pour répondre aux problèmes du système mondial contemporain l'approche de coopération interétatique demeure insuffisante. Dans le cadre du concept de gouvernance mondiale, la coordination de la politique internationale implique la coopération qui fait intervenir des acteurs hétérogènes ayant des capacités et des légitimités différentes. Dans les cas où sont présents des incertitudes techniques les réseaux d'experts, les communautés épistémiques jouent un rôle déterminant avec leurs effets d'influencer les résultats par l'intermédiaire du savoir souvent évoqué sous forme d'apprentissage et circulation des idées. Cependant, contrairement à l'utilisation de l'expertise dans le but d'apprentissage, il est possible d'observer son utilisation par les groupes d'intérêt ayant l'objectif d'augmentation de pouvoir. Et ceci, afin d'ouvrir la voie à exercer leur influence sur les acteurs étatiques dans le but de la mise en oeuvre des réglementations qui seraient en leur intérêts.

ANNEXES

ANNEXE 1: Organigramme de l'OCDE

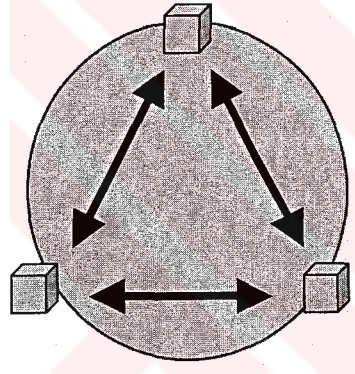


ANNEXE 2 : L'Organisation de l'OCDE

Conseil

Supervision et direction stratégique

Représentants des pays membres et de la Commission européenne ; décisions prises par consensus



Comités

Discussion et mise en œuvre

Représentants des pays membres et/ou à statut d'observateur travaillent de concert avec le Secrétariat sur des dossiers spécifiques

Secrétariat

Analyses et propositions

Secrétaire général
Secrétaires généraux adjoints
Directions

ANNEXE 3 :

LES LIGNES DIRECTRICES RÉGISSANT LA SÉCURITÉ DES SYSTÈMES ET RÉSEAUX D'INFORMATION : *VERS UNE CULTURE DE LA SÉCURITÉ*

PRÉFACE

Le degré d'utilisation des systèmes et réseaux d'information et l'environnement des technologies de l'information dans son ensemble ont évolué de façon spectaculaire depuis 1992, date à laquelle l'OCDE a rendu publiques ses *Lignes directrices régissant la sécurité des systèmes d'information.* Ces évolutions constantes offrent des avantages significatifs mais requièrent également que les gouvernements, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'information (parties prenantes), portent une bien plus grande attention à la sécurité. Des ordinateurs personnels toujours plus puissants, des technologies convergentes et la très large utilisation de l'Internet ont remplacé ce qui était autrefois des systèmes autonomes aux capacités limitées, dans des réseaux essentiellement fermés. Aujourd'hui, les parties prenantes sont de plus en plus interconnectées et les connexions franchissent les frontières nationales. De surcroît, l'Internet est le support d'infrastructures vitales telles que l'énergie, les transports et les activités financières et joue un rôle majeur dans la façon dont les entreprises conduisent leurs activités, dont les gouvernements assurent des services aux citoyens et aux entreprises et dont les citoyens communiquent et échangent des informations. La nature et le type des technologies constituant l'infrastructure des communications et de l'information ont également sensiblement évolué. Le nombre et la nature des dispositifs d'accès à cette infrastructure se sont multipliés et diversifiés pour englober les terminaux d'accès fixes, sans fil et mobiles et une proportion croissante des accès s'effectue par l'intermédiaire de connexions « permanentes ». Par voie de conséquence, la nature, le volume et le caractère sensible de l'information échangée ont augmenté de façon significative.

Du fait de leur connectivité croissante, les systèmes et réseaux d'information sont désormais exposés à un nombre croissant et à un éventail plus large de menaces et

vulnérabilités, ce qui pose de nouveaux problèmes de sécurité. Les présentes Lignes directrices s'adressent donc à l'ensemble des parties prenantes à la nouvelle société de l'information, et suggèrent le besoin d'une prise de conscience et d'une compréhension des questions de sécurité accrues, ainsi que la nécessité de développer une « culture de la sécurité ».

I. VERS UNE CULTURE DE LA SÉCURITÉ

Ces Lignes directrices répondent à un environnement en constante évolution en appelant au développement d'une culture de la sécurité – ce qui signifie porter une attention très grande à la sécurité lors du développement des systèmes d'information et des réseaux et adopter de nouveaux modes de pensée et de comportement lors de l'utilisation des systèmes et réseaux d'information et dans le cadre des échanges qui y prennent place. Les Lignes directrices marquent une rupture nette avec un temps où la sécurité n'intervenait que trop souvent de façon incidente dans la conception et l'utilisation des réseaux et systèmes d'information. Les parties prenantes sont de plus en plus tributaires des systèmes d'information, des réseaux et des services qui leur sont liés, lesquels doivent tous être fiables et sécurisés. Seule une approche prenant dûment en compte les intérêts de toutes les parties prenantes et la nature des systèmes, réseaux et services connexes peut permettre d'assurer une sécurité efficace. Chaque partie prenante a un rôle important à jouer pour assurer la sécurité. Les parties prenantes, en fonction de leurs rôles respectifs, doivent être sensibilisées aux risques liés à la sécurité ainsi qu'aux parades appropriées, doivent assumer leurs responsabilités et prendre des mesures de nature à améliorer la sécurité des systèmes et réseaux d'information. L'instauration d'une culture de la sécurité nécessitera à la fois une impulsion et

une large participation et devrait se traduire par une priorité renforcée donnée à la planification et la gestion de la sécurité, ainsi que par une compréhension de l'exigence de sécurité par l'ensemble des participants. Les questions de sécurité doivent être un sujet de préoccupation et de responsabilité à tous les niveaux du gouvernement et des entreprises et pour l'ensemble des parties prenantes. Les présentes Lignes directrices offrent un fondement aux efforts en vue d'instaurer une culture de la sécurité dans l'ensemble de la société. Les parties prenantes seront ainsi

à même d'agir pour que la sécurité devienne partie intégrante de la conception et de l'utilisation de tous les systèmes et réseaux d'information. Les Lignes directrices proposent que toutes les parties prenantes adoptent et encouragent une « culture de la sécurité » qui guide la réflexion, la décision et l'action concernant le fonctionnement des systèmes et réseaux d'information.

II. BUTS

L'objet des Lignes directrices est de :

– Promouvoir parmi l'ensemble des parties prenantes une culture de la sécurité en tant que moyen de protection des systèmes et réseaux d'information.

– Renforcer la sensibilisation aux risques pour les systèmes et réseaux d'information, aux politiques, pratiques, mesures et procédures disponibles pour faire face à ces risques, ainsi qu'à la
nécessité de les adopter et de les mettre en œuvre.

– Promouvoir parmi l'ensemble des parties prenantes une plus grande confiance dans les systèmes et réseaux d'information et dans la manière dont ceux-ci sont mis à disposition et utilisés.

– Créer un cadre général de référence qui aide les parties prenantes à comprendre la nature des problèmes liés à la sécurité, et à respecter les valeurs éthiques dans l'élaboration et la mise en
œuvre de politiques, pratiques, mesures et procédures cohérentes pour la sécurité des systèmes et réseaux d'information.

– Promouvoir parmi l'ensemble des parties prenantes, la coopération et le partage d'informations appropriés pour l'élaboration et la mise en œuvre des politiques, pratiques, mesures et procédures
pour la sécurité.

– Promouvoir la prise en considération de la sécurité en tant qu'objectif important parmi toutes les parties prenantes associées à l'élaboration et la mise en œuvre de normes.

III. PRINCIPES

Les neuf principes exposés ci-après se complètent et doivent être considérés comme un tout. Ils s'adressent aux parties prenantes à tous les niveaux, y compris politique et opérationnel. Aux termes des Lignes directrices, les responsabilités des parties prenantes varient selon le rôle qui est le leur. Toutes les parties prenantes, peuvent être aidées par des actions de sensibilisation, d'éducation, de partage d'informations et de formation de nature à faciliter une meilleure compréhension des questions de sécurité et l'adoption de meilleures pratiques en ce domaine. Les efforts visant à renforcer la sécurité des systèmes et réseaux d'information doivent respecter les valeurs d'une société démocratique, en particulier le besoin d'une circulation libre et ouverte de
l'information ainsi que les principes de base de respect de la vie privée des individus.

1) Sensibilisation

Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

La sensibilisation aux risques et aux parades disponibles est la première ligne de défense pour assurer la sécurité des systèmes et réseaux d'information. Les systèmes et réseaux d'information peuvent être exposés à des risques tant internes qu'externes. Les parties prenantes doivent comprendre que les défaillances de sécurité peuvent gravement porter atteinte aux systèmes et réseaux sous leur contrôle mais aussi, du fait de l'interconnectivité et de l'interdépendance, à ceux d'autrui. Les parties prenantes doivent réfléchir à la configuration de leur système, aux mises à jour disponibles pour ce dernier, à la place qu'il occupe dans les réseaux, aux bonnes pratiques qu'elles peuvent mettre en œuvre pour renforcer la sécurité, ainsi qu'aux besoins des autres parties prenantes.

2) Responsabilité

Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

Les parties prenantes sont tributaires de systèmes et réseaux d'information locaux et mondiaux interconnectés. Elles doivent comprendre leur responsabilité dans la

sécurité de ces systèmes et réseaux et en être, en fonction du rôle qui est le leur, individuellement comptables. Elles doivent régulièrement examiner et évaluer leurs propres politiques, pratiques, mesures et procédures pour s'assurer qu'elles sont adaptées à leur environnement. Celles qui développent, conçoivent et fournissent des produits et services doivent prendre en compte la sécurité des systèmes et réseaux et diffuser des informations appropriées, notamment des mises à jour en temps opportun de manière à ce que les utilisateurs puissent mieux comprendre les fonctions de sécurité des produits et services et leurs responsabilités en la matière.

3) Réaction

Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

Du fait de l'interconnectivité des systèmes et réseaux d'information et de la propension des dommages à se répandre rapidement et massivement, les parties prenantes doivent réagir avec promptitude et dans un esprit de coopération aux incidents de sécurité. Elles doivent échanger leurs informations sur les menaces et vulnérabilités de manière appropriée et mettre en place des procédures pour une coopération rapide et efficace afin de prévenir et détecter les incidents de sécurité et y répondre. Lorsque cela est autorisé, cela peut impliquer des échanges d'informations et une coopération transfrontières.

4) Éthique

Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

Les systèmes et réseaux d'information sont omniprésents dans nos sociétés et les parties prenantes doivent être conscientes du tort qu'elles peuvent causer à autrui par leur action ou leur inaction. Une conduite éthique est donc indispensable et les parties prenantes doivent s'efforcer d'élaborer et d'adopter des pratiques exemplaires et de promouvoir des comportements qui tiennent compte des impératifs de sécurité et respectent les intérêts légitimes des autres parties prenantes.

5) Démocratie

La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.

La sécurité doit être assurée dans le respect des valeurs reconnues par les sociétés démocratiques, et notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des informations de caractère personnel, l'ouverture et la transparence.

6) Évaluation des risques

Les parties prenantes doivent procéder à des évaluations des risques.

L'évaluation des risques permet de déceler les menaces et vulnérabilités et doit être suffisamment large pour couvrir l'ensemble des principaux facteurs internes et externes, tels la technologie, les facteurs physiques et humains, les politiques et services de tierces parties ayant des implications sur la sécurité. L'évaluation des risques permettra de déterminer le niveau acceptable de risque et facilitera la sélection de mesures de contrôles appropriées pour gérer le risque de préjudices possibles pour les systèmes et réseaux d'information compte tenu de la nature et de l'importance de l'information à protéger. L'évaluation des risques doit tenir compte des préjudices aux intérêts d'autrui ou causés par autrui rendus possibles par l'interconnexion croissante des systèmes d'information.

7) Conception et mise en œuvre de la sécurité

Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.

Les systèmes, réseaux et politiques doivent être conçus, mis en œuvre et coordonnés de façon appropriée afin d'optimiser la sécurité. Un axe majeur, mais non exclusif, de cet effort doit être la conception et l'adoption de mesures de protection et solutions appropriées afin de prévenir ou limiter les préjudices possibles liés aux vulnérabilités et menaces identifiées. Les mesures de protection et solutions doivent être à la fois techniques et non techniques et être proportionnées à la valeur de l'information dans les systèmes et réseaux d'information de l'organisation. La sécurité doit être un élément fondamental de l'ensemble des produits, services, systèmes et réseaux et faire partie intégrante de la conception et de l'architecture des systèmes. Pour l'utilisateur final, la conception et la mise en œuvre de la sécurité consistent essentiellement à sélectionner et configurer des produits et services pour leurs systèmes.

8) Gestion de la sécurité

Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

La gestion de la sécurité doit être fondée sur l'évaluation des risques et être dynamique et globale afin de couvrir tous les niveaux d'activités des parties prenantes et tous les aspects de leurs opérations. Elle doit inclure également, par anticipation, des réponses aux menaces émergentes et couvrir la prévention, la détection et la résolution des incidents, la reprise des systèmes, la maintenance permanente, le contrôle et l'audit. Les politiques de sécurité des systèmes et réseaux d'information, les pratiques, mesures et procédures en matière de sécurité doivent être coordonnées et intégrées pour créer un système cohérent de sécurité. Les exigences de la gestion de la sécurité sont fonction du niveau de participation, du rôle de la partie prenante, des risques en jeu et des caractéristiques du système.

9) Réévaluation

Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

Des vulnérabilités et menaces nouvelles ou évolutives sont constamment découvertes. Toutes les parties prenantes doivent continuellement revoir, réévaluer et modifier tous les aspects de la sécurité pour faire face à ces risques évolutifs.

RECOMMANDATION DU CONSEIL CONCERNANT LES LIGNES DIRECTRICES REGISSANT LA SECURITÉ DES SYSTÈMES ET RÉSEAUX D'INFORMATION : *VERS UNE CULTURE DE LA SECURITÉ*

LE CONSEIL,

Vu la Convention relative à l'Organisation de Coopération et de Développement Économiques, en date du 14 décembre 1960, et notamment ses articles 1 b), 1 c), 3 a) et 5 b) ;

Vu la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, en date du 23 septembre 1980 [C(80)58(Final)] ;

Vu la Déclaration sur les flux transfrontières de données adoptée par les gouvernements des pays Membres de l'OCDE le 11 avril 1985 [C(85)139, Annexe] ;

Vu la Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie, en date du 27 mars 1997 [C(97)62/FINAL] ;

Vu la Déclaration ministérielle relative à la protection de la vie privée sur les réseaux mondiaux, en date des 7-9 décembre 1998 [C(98)177/FINAL, Annexe] ;

Vu la Déclaration ministérielle sur l'authentification pour le commerce électronique, en date des 7-9 décembre 1998 [C(98)177/FINAL, Annexe] ;

Reconnaissant que les systèmes et réseaux d'information sont de plus en plus utilisés et cquièrent une valeur croissante pour les gouvernements, les entreprises, les autres organisations, et les utilisateurs individuels ;

Reconnaissant que le rôle toujours plus important que jouent les systèmes et réseaux d'information dans la stabilité et l'efficience des économies nationales et des échanges internationaux, ainsi que dans la vie sociale, culturelle et politique, et l'accentuation de la dépendance à leur égard imposent des efforts particuliers pour protéger et promouvoir la confiance qui les entoure ;

Reconnaissant que les systèmes et réseaux d'information et leur expansion à l'échelle mondiale se sont accompagnés de risques nouveaux et en nombre croissant ;

Reconnaissant que les données et informations conservées ou transmises sur des systèmes et réseaux d'information sont exposées à des menaces du fait de divers moyens d'accès sans autorisation, d'utilisation, d'appropriation abusive, d'altération, de transmission de code malveillant, de déni de service ou de destruction, et exigent des mesures de protection appropriées;

Reconnaissant qu'il importe de sensibiliser davantage aux risques pesant sur les systèmes et réseaux d'information ainsi qu'aux politiques, pratiques, mesures et procédures disponibles pour faire face à ces risques, et d'encourager des comportements appropriés en ce qu'ils constituent une étape essentielle dans le développement d'une culture de la sécurité ;

Reconnaissant qu'il convient de revoir les politiques, pratiques, mesures et procédures actuelles pour aider à faire en sorte qu'elles répondent de façon adéquate aux défis en constante évolution que posent les menaces auxquelles sont exposés les systèmes et réseaux d'information ;

Reconnaissant qu'il est de l'intérêt commun de promouvoir la sécurité des systèmes et réseaux l'information par une culture de la sécurité qui encourage une coordination et une coopération internationales appropriées en vue de répondre aux défis posés par les préjudices que des éfaillances de la sécurité sont susceptibles de causer aux économies nationales, aux échanges
internationaux, ainsi qu'à la participation à la vie sociale, culturelle et politique.

Reconnaissant en outre que les *Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité*, figurant en annexe à la présente Recommandation, sont d'application volontaire et n'affectent pas les droits souverains des États ;

Et reconnaissant que l'objet de ces Lignes directrices n'est pas de suggérer qu'il existe une solution unique quelconque en matière de sécurité, ou que des politiques, pratiques, mesures et procédures particulières soient adaptées à une situation donnée, mais plutôt de fournir un cadre plus général de principes de nature à favoriser une meilleure compréhension de la manière dont les parties prenantes peuvent à la fois bénéficier du développement d'une culture de la sécurité et y contribuer ;

PRÉCONISE l'application de ces *Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* par les gouvernements, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'information ;

RECOMMANDE aux pays Membres :

D'établir de nouvelles politiques, pratiques, mesures et procédures ou de modifier celles qui existent pour refléter et prendre en compte les *Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* en adoptant et promouvant une culture de la sécurité, conformément auxdites Lignes directrices ;

D'engager des actions de consultation, de coordination et de coopération, aux plans national et international, pour la mise en œuvre des Lignes directrices ;

De diffuser les Lignes directrices dans l'ensemble des secteurs public et privé, notamment auprès des gouvernements, des entreprises, d'autres organisations et des utilisateurs individuels, pour promouvoir une culture de la sécurité, et encourager toutes les parties intéressées à adopter une attitude responsable et à prendre les mesures nécessaires en fonction des rôles qui sont les leurs ;

De mettre les Lignes directrices à la disposition des pays non membres, le plus rapidement possible et de manière appropriée ;

De réexaminer les Lignes directrices tous les cinq ans, de manière à promouvoir une coopération internationale sur les questions liées à la sécurité des systèmes et réseaux d'information ;

CHARGE le Comité de la politique de l'information, de l'informatique et des communications de l'OCDE d'apporter son soutien à la mise en œuvre des Lignes directrices. La présente Recommandation remplace la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes d'information du 26 novembre 1992 [C(92)188/FINAL].

HISTORIQUE DE LA PROCÉDURE

Les Lignes directrices sur la sécurité ont été achevées en 1992 puis réexaminées en 1997. L'examen actuel a été entrepris en 2001 par le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP), dans le cadre d'un mandat donné par le Comité de la politique de l'information, de l'informatique et des communications (PIIC), et accéléré suite à la tragédie du 11 septembre. La rédaction a été entreprise par un Groupe d'experts du GTSIVP qui s'est réuni à Washington, DC, les 10 et 11 décembre 2001, à Sydney les 12-13 février 2002 et à Paris les 4 et 6 mars 2002. Le GTSIVP s'est réuni les 5-6 mars 2002, les 22-23 avril 2002 et les 25-26 juin 2002. Les présentes *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* ont été adoptées sous la forme

d'une ecommandation du Conseil de l'OCDE lors de sa 1037ème session, le 25 juillet 2002.

BIBLIOGRAPHIE

A) OUVRAGES

Documents

OECD, Proceedings of the OECD/BIAC forum on Internet Content Self Regulation, OECD Working Papers 1022-2227 v.6, no 100, Paris, 1998

OECD, Information Infrastructure in OECD Countries, OECD Working Papers 1022-2227 v.4, no 100, Paris, 1996

OECD, Report of the Ad-Hoc Meeting of Experts on Information Infrastructure, Issues Related to Security of Information Systems and Protection of Personal Data and Privacy, OECD Working Papers 1022-2227 v.4, no 38, Paris, 1996

OECD/ICCP Committee, Global Information Infrastructure, Global Information Society (GII-GIS) Statement of Policy Recommendations, no 35,Paris, 1996

OECD, Special Session on Information Infrastructure "Towards Realisation of the Information Society", OECD Working Papers 1022-2227, Paris, 1996

OECD, Information Technologies Policy, Organisational Structures in Member Countries, no 43, Paris, 1996

OECD, Symposium on International Technology Co-operation (Conference), no 51, Paris, 1994

OECD, Global Information Infrastructure-Global Information Society (GII-GIS), Policy Requirements, no 82, Paris, 1997

OECD, "Dismantling the Barriers to Global Economic Commerce", an International Conference organised by the OECD and the Government of Finland in Cooperation with the European Commission, The Government of Japan and the Business Advisory Committee to the OECD, Turku, Finland, 19-21 November 1997, Paris

OECD, The OECD Workshop on Telecommunications Infrastructure Competition (Conference), Paris, 1995

OECD, Privacy Protection in a Global Networked Society, an OECD International Workshop with the Support of the Business Advisory Committee to the OECD, Paris 16-17 February 1998

OECD, Guidelines for the Security of Information Systems, 1992

OECD, Guidelines for the Security of Information Systems: Towards a Culture of Security, 2002

OECD-ICCP, Information Network Security: A Project Report, OECD Document n.ICCP, 1989

OECD-ICCP, Ad-Hoc Meetings on Experts on the Security of Information Systems-Draft Guidelines for the Security of Information Systems. DSTI/ICCP/AH (90)(REV1)(20), 1991

OECD-ICCP, Ad-Hoc Meetings on Experts on the Security of Information Systems-Draft Guidelines for the Security of Information Systems. DSTI/ICCP/AH (90)(REV2)(20), 1991

OECD-ICCP, Ad-Hoc Meetings on Experts on the Security of Information Systems-Draft Guidelines for the Security of Information Systems. DSTI/ICCP/AH (90) 21 (REV3) 1991

OECD-ICCP, Ad-Hoc Meetings on Experts on the Security of Information Systems- Draft Guidelines for the Security of Information Systems. DSTI/ICCP/AH (90) 21 (REV4) 1992

OECD-ICCP, Ad Hoc Meeting on Experts on the Security of Information Systems- Summary Record of the Fifth Meeting of the Ad-Hoc Meeting on Experts on Guidelines for the Security of Information Systems. DSTI/ICCP/AH/M (92), 1992

AXSMITH Christine, The OCDE Guidelines for the Security of Information Systems : A look to the future, from 16th national security agency/national institute for standards and technology (NSA/NIST) National Computer Security Conference, 20-23, September 1993

BATTISTELLA Dario, *Théories des Relations Internationales*, Paris, Presses de Sciences Po, 2003

BAUMAN Zygmunt, *Globalisation: The Human Conséquences*, Cambridge, Polity, 1998.

CLARK Ian, *Globalization and International Relations Theory*, New York, Oxford Univ. Press, 1999.

FOX Jeremy, *Chomsky and Globalisation*, USA, Totem Books, 2001

GIDDENS Antony, *Runaway World:How Globalization is Reshaping our Lives*, Profile, London,1999

GIDDENS Antony, *Siyaset, Sosyoloji ve Toplumsal Teori*, Istanbul, Metis, 2000.

HOBSBAWM Eric, *The Age of Capital*, England, Abacus, 2001.

KALDOR Mary, *Global Civil Society*, Cambridge, Polity, 2003.

KAMARK Elaine Ciulla and NYE Joseph S. Jr., *Governance.com: Democracy in the Information Age*, Washington, Brookings, 2002.

KEOHANE Robert O. and NYE Joseph S., *Transnational Relations and World Politics*, Cambridge, Harvard University Press, 1971

KEOHANE Robert, *After Hegemony. Cooperation and Discord in the World Political Economy*, Princeton, Princeton University Press, 1984

KEOHANE Robert O. and NYE Joseph S., *Power and Interdependence*, New York, Longman, 2001.

KEOHANE Robert O., *International Institutions and State Power. Essays in International Theory,* London. Westview Press. 1989

LAROCHE Josepha, *Politique Internationale*, Paris, L.G.D.J., 2000.

LOADER Brian, *The Governance of Cyberspace : Politics, Technology and Global Restructuring*, New York, Routeledge, 1999.

LOADER Brian, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, New York, Routledge, 2000

NYE Joseph S. Jr. and DONAHUE John D., *Governance in a Globalizing World*, Cambridge, Brookings Institution Press, 2000

NYE Joseph S. Jr, *Understanding International Conflicts: An Introduction to Theory and History*, New York, Longman, 2003.

ROSENAU James N. and CZEMPIEL Ernst O., *Governance Without Government: Order and Change in World Politics,* Cambridge, Cambridge University Press, 1992

ROSENAU James N. and SINGH J.P., *Information Technologies and Global Politics*, Albany , State University of New York Press, 2002.

ROUBAN Luc, *La Fin des Technocrats?*, Paris, Presses de Sciences Po, 1998

SMOUTS Marie.-Claude, *Les Organisations Internationales*, Paris, Armand Collin, 1995

SMOUTS Marie-Claude, *Les Nouvelles Relations Internationales*, Paris, Presses de Sciences Po, 1999

TAPSSCOT Don, *The Digital Economy*, New York, McGraw-Hill, 1998

WALTZ Kenneth, *Theory of International Politics*, London, Addison-Wesley, 1979

Mémoires

VALERI Lorenzo, *Dot.com versus Dot.gov: States, International Businesses and an International Regime for Information Assurance*, London, King's College, 2002

B) ARTICLES

ADLER Emanuel, "The Emergence of Cooperation: National Epistemic Communities and The International Evolution of the Idea of Nuclear Arms Control", *International Organization*, no.46, winter 1992

ADLER Emanuel and HAAS Peter M., "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program", *International Organization*, no.46, winter 1992

BADIE Bertrand and SMOUTS Marie.-Claude, "L'International Sans Territoire : Introduction", *Culture et Conflits*, No.21-22

COWHEY Peter F., "The International Telecommunications Regime", *International Organization*, no.44, spring 1990

DRAKE William J. and NICOLAÏDAS Kalypso, "Ideas, Interests, and Institutionalization: 'Trade in Services' and the Uruguay Round", *International Organization*, no.46, winter 1992

HAAS Peter, "Intoduction to Epistemic Communities", *International Organization*, no.46, Winter 1992

HAAS Peter M., "Banning Chlorofluorocarbons: Epistemic Community Efforts to Protect Stratospheric Ozone", *International Organization*, no.46, winter 1992

HOPKINS Raymond F., "Reform in the International Food Aid Regime: the Role of Consensual Knowledge", *International Organization*, no.46, winter 1992

IKENBERRY G.John, "A World Economy Restored: Expert Consensus and the Anglo-American Postwar Settlement", *International Organization*, no.46, winter 1992

KAPSTEIN Ethan Barnaby, "Between Power and Purpose: Central Bankers and the Politics of Regulatory Convergence", *International Organization*, no.46, winter 1992

KRASNER Stephen, "Structural Causes and Regime Consequences: Regimes as Intervening Variables" in KRASNER Stephen (ed.), *International Regimes*, Ithaca, USA: Cornell University Press, 1983

PETERSON M.J., "Whalers, Cetologists, Environmentalists, and the International Management of Whaling", *International Organization*, no.46, winter 1992

RADAELLI C.M., "The Public Policy of the EU: Whither politics of expertise?", *Journal of European Public Policy*, 1999, 6(5)

RESTIER-MELLERAY C., « Experts et expertise scientifique, le cas de la France », *Revue Française de Science Politique*, 1990, 40(4)

SEBENIUS James K., "Challenging Conventional Explanations of International Cooperation: Negotiation Analysis and the Case of Epistemic Communities", *International Organization*, no.46, winter 1992

C) SITES INTERNET

BIAC, http://www.biac.org/

Conseil de l'Europe, http://www.coe.int

Digital Europe, http://www.digital-eu.org

Information Security Forum, http://www.securityforum.org

OECD, http://www.oecd.org

OECD Observer, http://www.oecdobserver.org/

SIGNATURES

Yrd. Doç. Dr. Nazlı Ilgaz

YRD. DOÇ. DR. FÜSUN TÜRKMEN

Yard. Doç. Dr. F. Selcan Serdengeçti

Doç Dr. İdil KAYA
Galatasaray Üniversitesi
Sosyal Bilimler Enstitüsü
Müdürü