La société de l'information et les problèmes de sécurité

J. Archibald
Université McGill

« Votre sécurité est entre vos mains. »
Oussama ben Laden[1]

1. Les objectifs généraux du Sommet mondial sur la société de l'information (Smsi)

Dans sa volonté et détermination commune d'édifier une société de l'information, la famille des Nations Unies a prouvé qu'elle a compris le rôle des technologies de l'information et de la communication (TIC) dans le processus de mondialisation et l'effet profond que celles-ci auront sûrement sur le développement social, économique, intellectuel et culturel de tous les pays tant développés qu'en voie de développement. Dans ce sens, le milieu international en général et les pays développés en particulier auront certes intérêt à collaborer dans le but de « réduire la fracture numérique »[2], car celle-ci divise le nord et le sud ainsi que les pays riches[3] et les moins bien nantis. Cet effort collaboratif de « réduction » consiste en un grand projet à multiples facettes qu'on

[1] *Al-Jazira*. 31 octobre 2004.
[2] Il s'agit de la traduction officielle de l'expression anglaise : « *to bridge the digital divide* ».
[3] Ignacio Ramonet appelle les pays les plus riches de la planète « le club des nantis » (G7 et avec la Russie G8). Ramonet, Ignacio. *Guerres du XXI^e siècle*. PARIS : Galiliée, 2002, p. 110.

pourrait qualifier de cyberculturel. Celui-ci est culturel, car il met en question notre situation sociétale, nos attitudes collectives et individuelles – cognitives, affectives et comportementales - nos valeurs et nos croyances actuelles par rapport à une nouvelle culture à inventer.

Tous les intervenants dans le processus du Sommet mondial sur la société de l'information (Smsi) reconnaissent l'impérieuse nécessité de « réduire la fracture numérique », mais les moyens pour y parvenir ne font pas toujours l'unité.

Le terme « fracture numérique » revient comme un leitmotiv dans tous les textes du Smsi et cette « fracture » prend toute l'ampleur de la cause première qui empêche l'essor socioéconomique des pays en développement. Plusieurs analystes critiquent ce qui paraît être une prise de position techniciste comme si la « réduction » de cette « fracture » ne relevait que de l'accès à l'information par le truchement des TIC. Dans sa critique de la position avancée par les auteurs du concept même de la « société de l'information », Samir Aïta explique que les racines de la problématique actuelle sont d'ordre plutôt communicationnel que technique et que cette fracture préoccupante « est avant tout une notion sociale ». Il note qu'il y a deux aspects de cette fracture dont on doit tenir compte dans l'action commune entreprise par le milieu international pour la réduire :

1. « l'accès proprement dit à l'information et son organisation » (le réseau de diffusion) ;
2. « l'extraction et l'exploitation du savoir tiré de cette information » (le contenu).[4]

[4] Aïta, Samir. « Internet en langue arabe : espace de liberté ou fracture sociale ? » *Maghreb-Machrek* 178 (hiver 2003-2004) : 36.

C'est ainsi que les représentants de la société civile au Smsi ont tant insisté sur l'emploi éventuel dans les textes officiels de termes distincts : *société de l'information*, *sociétés de communication*, *sociétés du savoir*. D'ailleurs, le comité de la société civile chargée de la rédaction de la déclaration de la société civile s'appelle bien « le comité sur les thèmes et le contenu ».

Malgré tout cela, le vrai point rassembleur qui permet de comprendre plus à fond les enjeux consiste en la reconnaissance de la diversité culturelle et linguistique en tant que facteur qui finira par colorer toutes les décisions à prendre allant de la création ou du transfert du savoir jusqu'à la protection des biens matériels et culturels et au bien-être des citoyens du cybermonde. Le respect de cette diversité permettra aux États et aux citoyens d'éviter de « basculer tous les pays du monde dans une société unique »[5] sous l'emprise d'une seule superpuissance économique et d'une langue et culture hypercentrales.[6]

Vu la nature foncièrement politique de la diversité, la logique à l'appui de cette démarche est d'autant plus complexe que la sécurité relève d'un ensemble de réflexions interreliées sur les TIC, la gestion des affaires et les programmes, quelle que soit la perspective des intervenants. Nous nous trouvons dans l'obligation d'analyser les prises de position de tous les intervenants en fonction de cette même diversité. Les questions de sécurité n'échappent pas à cette réflexion sur les programmes d'intervention sociale, culturelle et économique, leur cadre juridique tant national qu'international, et les règles qui

[5] Ramonet, Ignacio. *Guerres du XXI^e siècle*. PARIS : Galilée, 2002, p. 32.
[6] Voir Calvet, Louis-Jean. *Pour une écologie des langues du monde*. PARIS : Plon, 1999.

toucheront notre vie commune dans une cybersociété qui reste à définir en très grande partie.

2. Le processus et les intervenants

Le processus suivi par le Smsi a pu mener à un consensus que les membres de la famille de Nations unies ont accepté. Brièvement, il s'agissait et s'agit encore de préparer, par le truchement d'une série de conférences préparatoires, deux sommets mondiaux, le premier ayant eu lieu à Genève à la fin de 2003[7] et le deuxième devant se tenir à Tunis en 2005. Dans un premier temps, il fallait, d'une part, définir les grands principes de base qui devaient servir de cadre et, d'autre part, ébaucher un plan d'action pour chacun des domaines d'intervention éventuelle, y compris la sécurité. Une fois la base jetée, les intervenants devaient s'atteler à la tâche de préciser les modes d'intervention et les enjeux d'une telle intervention après l'adoption du plan à Tunis en 2005.

Le processus est essentiellement de nature gouvernementale et intergouvernementale. Malgré les quelques heurts du début, des intervenants non gouvernementaux ont fini par avoir leur mot à dire sans toutefois participer directement au processus décisionnel. Il s'agit des organismes faisant partie de la société civile[8] et des intérêts commerciaux représentés notamment par la Chambre de commerce internationale. Nonobstant un

---

[7] Voir à cet effet notre analyse de la première phase préparatoire : Archibald, J. **«** Pour une réduction de la fracture numérique ». *Chroniques* (août 2002). http://www.orbicom.uqam.ca/index_fr.html

[8] Pour une analyse détaillée de la participation de la société civile à la première phase du Smsi voir : Raboy, Marc et Normand Landry. *La communication au cœur de la gouvernance globale, Enjeux et perspectives de la société civile au Sommet mondial sur la société de l'information.* MONTRÉAL : Département de communication, Université de Montréal, 2004. Voir aussi l'analyse de la « conscience collective » et des mouvements de la société civile dans le monde arabo-musulman dans Aïta, Samir. « Internet en langue arabe : espace de liberté ou fracture sociale ? ». Magreb-Machrek 178 (hiver 2003-2004) : 34-37.

processus long et laborieux, les intéressés se sont finalement mis d'accord dans un premier temps sur les grands principes et les actions souhaitables à envisager. Un numéro complet de la revue américaine *Information Technologies and International Development* fut consacré à l'analyse de la première phase du Smsi.[9] Les auteurs reconnaissent que le processus n'est guère parfait, mais que le Smsi nous conduit néanmoins vers un monde où les TIC seront mises au service de l'humanité. Mais quels sont les enjeux sur le plan de la sécurité ?

[9] *Information Technologies and International Development* 1 (3-4), Spring-Summer 2004. Voir dans ce numéro : Archibald, J. 'Recognizing Cultural Diversity as a Dynamic Force in Cyberspace', pp 83-84.

3. Les objectifs spécifiques en termes de sécurité

« Établir et accroître la confiance et la sécurité dans l'utilisation des TIC »[10] figurent parmi les principes fondamentaux de la société de l'information et relèvent de la conception commune à l'effet que la société de l'information doit « accroître la confiance et la sécurité dans l'utilisation des TIC ».

Aux yeux de l'analyste externe, on pourrait conclure qu'il s'agit d'une question essentiellement technique, mais il n'en est pas entièrement ainsi.

Plus précisément, les gouvernements prétendent vouloir promouvoir un « climat de confiance » dans le contexte des échanges d'informations et le réseautage des utilisateurs des TIC. Pour atteindre l'objectif, il faudra en principe favoriser l'émergence d'une « culture globale de la cybersécurité » et tous les intervenants devront encourager, développer et mettre en œuvre cette nouvelle culture collective dans un environnement de coopération internationale. La déclaration de principes essaie de nous faire comprendre en termes généraux les enjeux.

> Dans cette culture mondiale de la cybersécurité, il importe d'accroître la sécurité et d'assurer la protection des données de la vie privée, tout en améliorant l'accès et les échanges commerciaux. Cette culture mondiale de la cybersécurité doit en outre tenir compte du niveau de développement socio-économique des pays et respecter les aspects de la société de l'information qui sont orientés vers le développement. (Smis. 4F - B5.35)

[10] Smsi. *Déclaration de principes, Construire la société de l'information : un défi mondial pour le nouveau millénaire* (WSIS-03/GENEVA/DOC/4-F). GENÈVE : UIT, 12 mai 2004. Voir le site multilingue du sommet : www.itu.int/wsis

Il est clair que l'accès accru à l'information, aux communications et au savoir constitue un objectif souhaitable dans une perspective mondiale de réduction de la fracture numérique. Ceci est d'autant plus vrai que « [l]a nouvelle richesse des nations reposera de plus en plus, au cours du XXI^{e} siècle, sur […] le savoir [… et] la capacité à innover ».[11] Toutefois, les gouvernements reconnaissent les dangers inhérents à cette orientation. C'est ainsi que les gouvernements ont appuyé un deuxième principe de sécurité dans ce contexte afin de garantir le « maintien de la stabilité et de la sécurité internationales » (Smsi. 4F - B5.36), si bien que chaque État membre de l'ONU devrait pouvoir protéger ses infrastructures nationales et sa propre sécurité. Plus précisément, tout en respectant les droits de l'homme, les États devront veiller à ce que les TIC ne soient mises au service ni de la criminalité ni du terrorisme. C'est une politique d'ouverture et de développement mitigés. En effet, il ne s'agit pas d'une recommandation menant à une liberté sauvage, mais plutôt d'une liberté qui sera traitée « aux niveaux national et international appropriés » dans le respect double de la cybersécurité et de la liberté d'expression et de communication. On pourrait certes conclure que tous les États ne traduiront pas ces principes en action de la même manière si bien que les grandes démocraties veilleront à protéger leurs institutions et leurs citoyens tandis que certains régimes autoritaires ne s'ouvriront que peu à peu à une culture d'information et de communication plus libre car, dans les deux types d'État, le nouveau savoir accessible pourrait bien avoir des effets positifs ou nuisibles selon les perspectives adoptées.

[11] Ramonet, Ignacio. *Guerres du XXI^{e} siècle*. PARIS : Galilée, 2002, p. 16.

Les principes adoptés donnent lieu à un plan d'action.[12] Ce plan est de nature « évolutive ». Toutefois, il définit en termes relativement clairs les moyens dont chaque État peut disposer pour établir une ambiance de sécurité dans la société de l'information.

À la base de cette nouvelle société à bâtir, nous retrouvons le désir commun de promouvoir la confiance parmi les cybercitoyens et au sein même des institutions et des gouvernements dans un climat de sécurité. C'est là un des « principaux piliers de la société de l'information ». (Smsi. 5-F C5 12). En partant des dix plans proposés dans ce contexte, nous reviendrons ici sur quatre d'entre eux, qui sont primordiaux pour bien saisir les enjeux de la sécurité.

Chaque État est appelé à « améliorer la sécurité » (Smsi. 5-F C5 12a) dans la façon de gérer l'information et les réseaux des communications informatisées. Cela veut dire que chaque État aura la responsabilité renouvelée

- de renforcer la confiance des utilisateurs,
- de protéger l'intégrité des données et des réseaux, et
- d'envisager les menaces existantes et potentielles.

On peut bien « envisager » ces questions, mais que faire et dans quel contexte ?

Renforcer le cadre de sécurité et de confiance exige l'adoption par les États et les organismes intergouvernementaux d'initiatives complémentaires dont la synergie reflète un certain de niveau de collaboration entre États et organismes intergouvernementaux ainsi que la promulgation d'une nouvelle façon d'agir cyberculturelle. Cette attitude

[12] Smsi. *Plan d'action* (WSIS-03/GENEVA/DOC/5-F). GENÈVE : UIT, 12 mai 2004.

éventuelle s'interprète de plusieurs manières. L'État totalitaire et l'État démocratique ne voient pas le processus d'un même œil, car les uns se rallieront du côté de la liberté d'expression et de communication tandis que d'autres se pencheront plutôt vers des mesures coercitives pour protéger la sécurité de l'État et des pouvoirs publics. Par contre, il ne faut pas non plus tomber dans le piège de l'angélisme, car même les régimes constitutionnellement « démocratiques » ou « républicains » se retrouvent dans l'obligation de protéger leurs citoyens et leurs institutions par le truchement de mesures qui frôlent l'autocratie. Par exemple, le droit à la confidentialité des systèmes et des données n'est pas sans bornes même dans les pays les plus « libres ». Vu la troisième responsabilité de l'État mentionnée ci-dessus, l'existence réelle de menaces contre l'ordre public met les États et les organismes intergouvernementaux dans l'obligation de moduler leur interprétation des droits de l'homme, surtout en ce qui concerne certaines libertés sacro-saintes dans les régimes de tradition démocratique : l'expression, la religion, la communication, la presse, etc. C'est pour ces raisons que la protection et la prévention peuvent paraître aux yeux de certains comme une forme d'intervention étatique proche du totalitarisme.

Vu l'impact escompté de la mondialisation sur la société de l'information à l'échelle planétaire, il est également recommandé que les États et les organismes de veille internationaux « échangent les meilleures pratiques dans les domaines de la sécurité de l'information et de la sécurité des réseaux ». (Smsi. 5-F C512g) En principe, tous les États et tous les organismes internationaux devront, dans leurs pratiques réelles, épouser cette orientation, car l'un des objectifs du Smsi consiste en l'amélioration de ces mêmes

pratiques de façon à accroître la confiance des citoyens du cybermonde, à protéger l'intégrité des données et des réseaux, - et à lutter contre les ennemis d'une société mondiale en émergence qui soit respectueuse des libertés. Ceci est d'autant plus important que le crime international et le terrorisme suivent aussi un élan d'internationalisation et cherchent souvent, pour des raisons tout autres, à miner la confiance des peuples dans les structures démocratiques, à infiltrer des systèmes ostensiblement sécuritaires et à mettre en danger des peuples par des actions qui s'inspirent des mêmes stratégies envisagées par le Smsi tout en les appliquant à des fins qui menacent la stabilité de l'ordre régional, national et international. Les TIC n'ont pas de valeur éthique intrinsèque ; ce sont des outils - ou des armes tactiques selon certains – qu'on peut mettre au service d'objectifs contraires : protéger ou menacer. La technologie peut très bien faciliter ces stratégies compossibles, d'où l'importance pour les États d'améliorer la sécurité des données et des systèmes et de mettre les TIC au service de la stabilité démocratique du monde.

Compte tenu du manque de pouvoir réel de la famille des Nations unies, le Smsi veut encourager les États ayant adopté les principes et accepté l'orientation du plan d'action à « contribuer activement aux activités » (Smsi. 5-F C512j) de l'ONU pour qu'ils s'intègrent bien dans un monde qui respecte de fait la Charte des Nations unies et la Déclaration universelle des droits de l'homme.

Il est à espérer que cet appel à l'action se traduira par la mise en place d'un certain nombre de mesures à être prises par les États membres, notamment :

1. la détection de la cybercriminalité ;
2. la veille à l'endroit des organisations visant à déstabiliser l'ordre public ;
3. l'adoption de dispositions législatives, judiciaires et administratives pour combattre une utilisation illicite des TIC ;
4. l'organisation de programmes d'éducation et de sensibilisation aux avantages et aux menaces des TIC ;
5. la protection de la vie privée ;
6. l'évaluation interne de la législation nationale ;
7. l'adoption de mécanismes de coordination pour la gestion et le traitement d'incidents qui vont à l'encontre de l'orientation internationale consentie ;
8. la création et le maintien de réseaux efficaces de coopération pour le développement et la sécurité.

Dans l'ensemble, ces objectifs sont extrêmement ambitieux et risquent de n'être atteints que partiellement. Le vrai engagement des États et des organismes internationaux ne pourra se mesurer qu'à l'issue du Sommet de Tunis. D'ici là, les pays ayant accepté et les principes et le plan d'action proposé devront commencer à planifier leurs stratégies d'alignement pour atteindre le but ultime de réduction de la fracture numérique dans un climat de confiance et de sécurité. Dans ce contexte, il est à craindre toutefois que « la société civile des pays arabes ne soit pas à même de jouer pleinement son rôle, à la différence de ce qu'on peut observer dans d'autres parties du monde ».[13] Par conséquent, nous pourrions bien témoigner de certaines défaillances dans ce partenariat prometteur entre États et société civile.

[13] Aïta, Samir. « Internet en langue arabe : espace de liberté ou fracture sociale ? » *Maghreb-Machrek* 178 (hiver 2003-2004) : 40.

4. Étude comparée des principes et des plans : gouvernements – société civile

Le Smsi a associé dans son entreprise deux partenaires ayant des objectifs parfois complémentaires et parfois contradictoires.

Pour sa part, la société civile a réussi à attirer l'attention sur les conséquences socioculturelles des principes et plans d'action proposés et sur la nécessité de justifier démocratiquement les options stratégiques préconisées par les gouvernements. La grande diversité de la société civile et sa façon souvent pragmatique d'aborder différentes questions en font un acteur clé dans ce nouveau partenariat international. Créé à l'occasion de la deuxième réunion de la conférence préparatoire, le Bureau international de la société civile se charge de mettre en place des mécanismes qui facilitent le dialogue avec les gouvernements, tout en assurant une participation efficace de la société civile. Ce Bureau est composé des grandes « familles » de la société civile : syndicats, média, créateurs et acteurs culturels, pouvoirs publics locaux et municipaux, ONG, représentants des jeunes, des femmes, des peuples autochtones, des personnes handicapées, etc. Il comprend également des points de contact régionaux, l'objectif étant d'établir un réseau interactif partout dans le monde.

Hormis cette ouverture, il faut rappeler que la vision que nous avons présentée plus tôt reflète l'orientation gouvernementale du Smsi dans la mesure où les documents officiels adoptés au Sommet de Genève le furent uniquement par les gouvernements membres de l'ONU. Nous avons évoqué ailleurs les différends fondamentaux entre la partie

gouvernementale et la société civile qui ont failli constituer un obstacle infranchissable dès les premières réunions préparatoires. Les membres de la société civile ne disposant que d'un statut d'observateur n'avaient pas de droit de parole aux conférences préparatoires, et leurs travaux se tenaient littéralement en marge du Smsi lui-même. Par contre, les groupes d'intérêts commerciaux étaient présents et leur leadership a pris la parole devant l'assemblée plénière des représentants des États membres. Or cette alliance était mal vue par une majorité des ONG qui perdaient confiance en la bonne volonté des organisateurs du Smsi. À nous en tenir à la question de sécurité, la société civile avait l'impression que le milieu des affaires et les gouvernements étaient de connivence dans le but de contrôler l'information[14] et de créer des occasions commerciales sous prétexte de « réduire la fracture numérique ». Par ailleurs, plusieurs membres de la société civile estimaient qu'il fallait faire éclater la notion restrictive et passive de « société de l'information » pour réorienter le processus en fonction d'une « société de la communication » dont l'un des principes de base devrait consister en la promotion du savoir et le respect des libertés. La confiance ne régnait certes pas.

Ce malaise s'explique par ce que le *Cato Institute* a appelé un « conflict of visions », car il n'y a pas de congruence parfaite entre les valeurs et croyances promulguées par les gouvernements et les membres de la société civile.

[14] Cette méfiance ne s'est pas encore entièrement dissipée. À la réunion du Forum européen sur les droits de la communication qui s'est tenue le 24 octobre 2004 à Londres, les participants étaient d'avis que les questions de sécurité servaient de prétexte pour la mise en place d'une société de contrôle par le truchement d'une « vague de législations antiterroristes répressives » et l'adoption de « nouveaux moyens de contrôle et de surveillance » dont les premières victimes seraient les « libertés publiques » et « les Droits humains fondamentaux ».

> The tilt toward government intervention can be excessive. In an earlier time the unruly Internet was thought to be a virtual Wild West, an unregulated province of libertarians and cyber-anarchists. However, it appears now to be well on the way to becoming a heavily regulated network increasingly encumbered by conflicting demands from federal, state, and international governments, along with assorted special interests.[15]

Dans un rapport de la Fondation Heinrich-Böll publié en 2003, nous trouvons la même tension entre les gouvernements et la société civile. Les différends s'articulent autour de la sécurité et de l'e-gouvernement et le lien indissociable entre ces deux questions.[16] Selon ce rapport, la préoccupation de la société civile se focalise surtout sur les dispositifs de « sécurité militaire » que les pays moins démocratiques pourraient mettre en place pour garantir la stabilité intérieure et lutter contre les menaces du terrorisme. Quelle « stabilité » et quelles « menaces » peut-on se demander.

Heureusement, les parties ont fini par trouver moyen d'ouvrir le dialogue et de se consulter dans un esprit d'ouverture par rapport à leurs positions respectives. Et malgré la grande diversité des prises de position, les deux parties ont fini par pouvoir travailler ensemble en vue de promouvoir un agenda commun si bien que la déclaration finale au Sommet de Genève représentait dans ses grandes lignes un consensus relativement acceptable par les gouvernements et la société civile.

---

[15] Crews, Clyde Wayne et Adam Thierer. « Introduction : Who Rules the Net? ». In Thierer, Adam, dir. *Who Rules the Net?*, p. xvii. WASHINGTON : Cato Institute, 2004.
[16] Heinrich-Böll Foundation. *Major conflicts still unresolved*. 12 novembre 2003. http://www.worldsummit2003.de/en/web/517.htm (3 novembre 2004)

Toutefois, la société civile continue d'axer ses positions sur les valeurs d'une communication plus ouverte, le respect de la liberté d'expression et le besoin de favoriser l'émergence de sociétés de savoir respectueuses de la diversité culturelle et linguistique. Par contre, la société civile ne nie pas les menaces de la criminalité et du terrorisme.

Bien que la société civile n'ait pas formulé de désaccord irréconciliable vis-à-vis des gouvernements, elle a toutefois estimé que les gouvernements et organismes internationaux devaient promouvoir le « développement durable » par des projets visant la promotion de la paix et de l'égalité ainsi que la résolution de conflits dans un contexte de diversité linguistique et culturelle.[17]

Les chercheurs universitaires et institutionnels – comme membres de la société civile au Smsi – ont identifié le rapport entre la diversité, la sécurité et l'émergence d'une cyberculture comme un champ de recherche particulièrement porteur.

La Commission européenne, l'un des organismes intergouvernementaux intéressés aux conclusions du Smsi et à la mise en application du plan d'action est du même avis. C'est ainsi que Philippe Busquin, responsable de la recherche à la CE, a

[17] Archibald, J. « Vers une politique internationale de la diversité sur la Toile ». Communication présentée dans le cadre du colloque « La localisation sur la Toile : politiques, stratégies et pratiques ». MONTRÉAL : Université McGill, octobre 2004.
http://upload.mcgill.ca/conted-translation/La-localisation-sur-la-toile.pdf

identifié la sécurité comme étant une « question clé » dans le processus de réduction de la fracture numérique, car une garantie internationale de sécurité et de stabilité est une excellente façon d'investir collectivement dans le bien-être des générations montantes. La CE reconnaît qu'aucun État membre ne pourra le faire seul et atteindre le même niveau d'efficacité collective.[18] Voilà donc un exemple du potentiel de collaboration entre la société civile et les États où les objectifs de diversité, de sécurité et de développement cyberculturel s'ouvrent sur une collaboration mutuellement bénéfique.

Cette opinion fut formulée à la suite des attentats de Madrid et reflète aussi une attitude de plus en plus fréquente en Europe : la peur de l'autre dans une Europe de plus en plus pluriculturelle. En effet, dans son rapport sur la sécurité européenne, Burkard Schmitt établit clairement le lien entre la diversité porteuse de danger, la vulnérabilité de la société européenne et l'expansion rapide des TIC dans une société de l'information mondialisée. Il reconnaît néanmoins les avantages de cette cyberculture.

> The spread of ideas and information across the Internet and via other global media broadens cultural horizons and becomes a powerful tool to advance the cause of human rights and democracy.[19]

Par contre, il est entièrement conscient des dangers que cette nouvelle culture peut nous amener parce que « conflicts in remote regions can destabilize the international order and directly affect Europe's security and interests ».[20] Nous nous acheminons vers des sociétés marquées par un sens de vulnérabilité, et les citoyens vivent un niveau d'anxiété en rapide croissance vu leur incapacité à saisir toute la portée des nouvelles menaces qui

---

[18] Commission européenne. « Security research a "key topic" in next Framework Programme », 19 juillet 2004. http://europa.eu.int/comm/research/security/news/article_1282_en.html (14 Sept 2004). Voir aussi CE. 'Preparatory Action for Security Research' (PASR2004).

pèsent sur les États, les institutions et les personnes. En effet, dans un sondage récent, on apprend que 60 % des Européens ont peur des conflits interethniques et culturels sur leur propre territoire en raison de la diversité accrue des populations.[21] C'est dire que les ennemis potentiels ne se trouvent plus à l'étranger ; ils sont d'ici maintenant. Dans l'immédiat, l'élargissement de l'Europe n'y portera pas remède.[22]

Voilà la raison pour laquelle il faudra accentuer des recherches sur cet ensemble de questions. Les quelques exemples cités ci-dessus illustrent le potentiel de collaboration et de conflit entre la société civile et les gouvernements.

---

[19] Schmitt, Burkard, rapporteur. *Research for a Secure Europe*, p. 8. LUXEMBOURG : Office for Official Publications of the European Communities, 2004.
[20] *Ibid.*
[21] Les autres sources d'anxiété collective sont par ordre d'importance : le terrorisme international (80 %), le crime organisé (78 %), la prolifération des ADM (70 %) et la sécurité nucléaire (65 %).
[22] *Ibid*., p. 9.

5. Favoriser une culture de cybersécurité dans la cyberculture

Promouvoir une culture de cybersécurité est un objectif spécifique qui devrait faciliter l'atteinte des objectifs du Smsi. Mais ce type de culture est subsidiaire à une cyberculture plus générale qui ne s'est pas encore implantée à grande échelle sur la planète. C'est justement pour cela que la communauté internationale essaie d'élaborer des politiques et des plans d'action conçus dans le but de réduire la fracture numérique, fracture qui existe souvent pour des raisons culturelles. Dans le contexte des politiques de sécurité, il faut voir dans cette promotion de la cyberculture et des TIC une arme à double tranchant. Certes, elle peut sécuriser et stabiliser ; toutefois, en de mauvaises mains elle peut aussi facilement insécuriser et déstabiliser.

En effet, dans le monde arabe cette situation est jugée « préoccupante », car les TIC recèlent à la fois des « potentialités déstabilisatrices [et] libératrices ».[23] Par conséquent, la communauté internationale et les États directement concernés se trouvent confrontés à la nécessité de gérer ces deux tendances. Celles-ci feront l'objet d'une attention particulière dans l'espace social et juridique du monde arabo-musulman, car cet espace est « d'ores et déjà transnational »[24] et favorise l'émergence de communautés virtuelles qui vivent à l'heure actuelle dans une sorte de no man's land juridique que les milieux intergouvernementaux et nationaux essaient tant bien que mal de gérer, d'où l'intérêt des propositions du Smsi par rapport au développement de la société de l'information.

---

[23] Gonzalez-Quijano, Yves. « L'Internet arabe ». *Maghreb-Machrek* 178 (hiver 2003-2004) : 7-8.
[24] Anderson, Jon W. « Des communautés virtuelles ? ». *Maghreb-Machrek* 178 (hiver 2003-2004) : 47.

C’est pour cette raison que tous les intervenants étatiques de bonne volonté sont dans l’obligation d’analyser de manière critique les tenants et les aboutissants de la cyberculture et, plus particulièrement, ceux de la culture de cybersécurité.

6. Des modèles de développement cyberculturel

La bibliographie sur la culture organisationnelle est extrêmement vaste et nous n'aurons pas l'occasion, dans le cadre de ce travail, d'en explorer tous les méandres.

Vu le rapport entre diversité et sécurité, nous avons choisi d'explorer le modèle d'analyse à la fois souple et rigoureux conçu par Renaud Sainsaulieu et expliqué dans son ouvrage *Sociologie de l'organisation et de l'entreprise.* Bien que le modèle soit un précurseur des réflexions actuelles sur la société de l'information, Internet représente néanmoins une organisation, et chaque organisme qui « habite » le cybermonde présente des caractéristiques organisationnelles que nous devons comprendre si nous voulons vraiment faire preuve de solidarité dans la promotion des principes et des plans du Smsi.

Le modèle en question réunit plusieurs aspects qu'on retrouve dans la problématique présentée par le projet du Smsi :

- la culture est un facteur de développement à une époque de contingences, menaces et crises ;
- la dynamique culturelle consiste en un processus d'action au cœur des interactions stratégiques ;
- la culture a toujours une histoire héritée ;
- la culture a une portée diachronique et synchronique de nature systémique.[25]

À la lumière de ce cadre d'analyse, on comprend l'action des gouvernements et des organismes inter ou supragouvernementaux. Les pouvoirs publics dans leurs plans

[25] Sainsaulieu, Renaud. *Sociologie de l'organisation et de l'entreprise*. PARIS : Presses de la Fondation nationale des sciences politiques & Dalloz, 1987, p. 214.

d'action prennent en compte les contingences et retiennent les mesures nécessaires pour se protéger contre les menaces, prévenir les crises et gérer les effets de celles-ci. Ils adoptent des stratégies de développement qui sont à l'image de la dynamique culturelle (et linguistique) du pays ou de l'organisme intergouvernemental. Culturellement, ils sont les héritiers de leur propre passé et les auteurs de leur avenir, tantôt seuls tantôt en collaboration.

Le premier constat, c'est qu'il n'existe pas de culture unique. Selon Sainsaulieu, il y a un certain nombre de modèles de base. Comme point de départ, il en propose neuf :

1. la culture paternaliste,
2. la culture des communautés professionnelles,
3. les cultures antagonistes,
4. les cultures bureaucratiques et statutaires,
5. les cultures rationnelles ou tayloristes,
6. les cultures relationnelles,
7. les cultures de marché,
8. les cultures de fonctionnement collectif,
9. les cultures du développement social.

Sous l'effet d'une dynamique combinatoire, on constate également la présence de cultures hybrides. Par exemple, il peut exister une organisation ayant à la fois les traits d'une culture paternaliste et ceux d'une culture de développement social. Une telle culture hybride reconnaît la pluralité des identités culturelles et linguistiques en son sein, mais se préoccupe davantage de l'élaboration collective de projets ainsi que de l'évaluation collective des résultats. Le tout se fait sous l'œil vigilant d'un leader patriarcal qui protège ses proches ou ses semblables et exclut des groupes ou personnes

ne faisant pas partie du groupe sous protection.[26] Le leader exige une loyauté sans faille, et les membres de l'organisation partagent un même système de valeurs et de croyances. Pour comprendre les valeurs communes d'une telle organisation, il faut étudier l'identité ethnique des membres, les strates, les âges, les sexes, les langues pratiquées, le niveau d'éducation et les régions ou zones d'origine ou d'exercice entre autres. Il faut aussi avoir une idée précise de l'histoire passée, actuelle et prévisible du groupe dans un contexte bien défini.

Or, on peut très bien comprendre les enjeux de cette analyse dans un projet de promotion de la cyberculture.

L'établissement d'une culture de cybersécurité dans un tel groupe exige une connaissance approfondie de la culture organisationnelle. Voici, à titre de suggestion, quelques questions de recherche.

- Comment le leader a-t-il réussi a garantir sa position et comment protège-t-il la pérennité de son leadership ?
- Comment le leader s'assure-t-il de la loyauté des membres de son organisation ?
- Quelle est la composition ethnoculturelle de l'organisation ?
- Quelle est la langue véhiculaire utilisée par l'organisation ?
- D'autres langues sont-elles connues ou utilisées, et à quel degré et dans quel but ?[27]
- Y a-t-il une vision commune et partagée de leurs origines et de leur avenir par rapport à l'existence actuelle ?

---

[26] Ignacio Ramonet signale l'apparition ce qu'il appelle « l'État-individu » où le leader se voit « reconnaître les attributs et les prérogatives qu'avaient jusqu'à présent les États ». Il prétend que cette institutionnalisation de l'individu a pu se réaliser grâce aux nouvelles technologies de la communication et de l'information. Telle est l'explication de l' « État-réseau » d'Oussama ben Laden. Ramonet, Ignacio. *Guerres du XXI^e siècle*. PARIS : Galilée, 2002, p. 143.

[27] D'après Jens Allwood, on peut mesurer l'utilité d'une langue en étudiant le rapport entre celle-ci et le pouvoir politique, économique et militaire de ses locuteurs collectivement et individuellement. A cela, nous ajoutons le pouvoir (cyber)culturel de la langue.

Ce type de questionnement met en relief la valeur de l'information dans le processus de planification stratégique. En termes de cybersécurité dans un contexte de diversité, ces questions revêtent une importance capitale, car l'information peut servir de base à la prise de décision pour sécuriser ou stabiliser une organisation, d'une part ; ou pour l'insécuriser ou la déstabiliser, d'autre part.

Nous avons choisi cet exemple parce qu'il nous permet de voir les deux côtés de la médaille dans un contexte de développement et de gestion d'une culture de cybersécurité face à des éléments criminels ou terroristes.

Cette question est d'autant plus importante que plusieurs groupes militants profitant d'un mouvement vers la mondialisation des communications et des techniques de la localisation peuvent facilement rejoindre une diaspora communautaire de fidèles et de nouveaux adhérents pour faire avancer une cause ou une idée. Il s'agit de ce que Jon Anderson a appelé le « paradigme islamique de la localisation » mis au service des « nouveaux oulémas » dans un but de médiation psychosociologique.[28]

[28] Anderson, Jon W. « Des communautés virtuelles ? » *Magreb-Machrek*. 178 (hiver 2003-2004) : 54. Voir aussi l'analyse de *l'oumma virtuelle d'Internet* dans Roy, Olivier. *L'Islam mondialisé*, nouvelle édition. PARIS : Le Seuil, 2004, pp 179-199.

7. Un défi à relever par les gouvernements, le milieu des affaires, les organismes de la société civile et la société en général

À notre avis, le défi à relever par les gouvernements, le milieu des affaires et la société civile consiste en un défi informationnel et communicationnel, car on n'atteindra ni les objectifs de développement ni les objectifs de sécurité à moins de disposer des renseignements nécessaires et de pouvoir les communiquer à qui de droit afin de pouvoir prendre des décisions stratégiques en temps voulu.[29] Il importe alors de posséder une connaissance ethnographique de l'autre et de ses instabilités internes afin de prévoir de manière précise ses prédispositions.[30] Cette stratégie s'applique tant aux cas de développement ou d'entraide qu'aux cas de conflit.

Tenons-nous-en à l'exemple d'une organisation de culture hybride telle que décrite sommairement ci-dessus.

Si un gouvernement ou une institution intergouvernementale voulait, dans l'esprit du Smsi, intervenir pour aider une telle organisation à adopter une culture de cybersécurité, il ne suffirait pas de fournir les TIC, car ces outils ne pourraient servir à protéger ladite

[29] Le renseignement prend en effet quatre formes différentes mais complémentaires : le *comint* (*communications intelligence*), le *elint* (*electronic intelligence*), le *humint* (*human intelligence*) et le *sigint* (*signals intelligence*). D'après John Keegan, malgré l'utilisation de plus en plus pointue des moyens technologiques dans la cueillette du renseignement, le rôle de l'être humain prime, car c'est lui qui peut le mieux comprendre la culture de l'ennemi et, par voie de conséquence, sa cyberculture et sa compréhension de la culture de cybersécurité. Keegan, John. *Intelligence in War*. NEW YORK : Random House, 2004, pp 296-7.

[30] Voir à cet effet la discussion du renseignement stratégique dans Keegan, John. *Intelligence in War*. NEW YORK : Random House, 2004, pp 7-25. Le principe de base évoqué consiste en la valeur du

organisation ni à prévenir les menaces qui risqueraient de peser sur elle à moins de les cadrer dans une cyberculture réceptive. Le renseignement stratégique permettra de cibler les interventions nécessaires pour atteindre l'objectif.

Une étude ethnographique préalable de l'organisation s'impose de rigueur. Une telle étude peut fournir des éléments de réponse quant aux situations éventuelles nécessitant la mise en place de *mesures habilitantes*.[31] Voici quelques réflexions à être envisagées par le chercheur.

- Comment l'adoption d'une cyberculture permettra-t-elle au leader de maintenir et prolonger sa position de leadership, de se protéger et de prévoir sa succession ?
- Comment le leader peut-il s'assurer de la loyauté des membres de son organisation tout en donnant accès aux informations, en encourageant la communication libre et en garantissant la liberté d'expression chez les membres de l'organisation ?
- Comment les TIC peuvent-elles servir de support pour l'organisation ethnoculturelle ?
- Comment les TIC peuvent-elles faciliter l'usage de la langue véhiculaire utilisée par l'organisation ?
- Comment peuvent-elles servir à faciliter l'apprentissage d'autres langues utiles au développement de l'organisation ?
- Quels programmes cyberculturels faut-il mettre en place afin de promouvoir et faire accepter une vision commune et partagée des origines du groupe et de son avenir par rapport à l'existence actuelle ?

Nous pouvons nous pencher sur le même modèle et le tourner autrement. Prenez l'exemple de l'organisation terroriste qui met les TIC à sa propre disposition pour déstabiliser ou insécuriser un adversaire dans un but purement politique.

---

renseignement qui permet de connaître l'ennemi car, pour remporter la victoire dans une guerre, il faut connaître l'adversaire de l'intérieur.

[31] Selon le représentant du Canada au Smsi, les TIC consistent en une « technologie habiltante » ; d'après lui, elles faciliteront la réduction de la fracture numérique, et les pays développés ont le devoir de porter secours aux pays en développement pour atteindre les objectifs du Smsi. Marchi, Sergio. « Canadian Statement to the World Summit on the Information Society ». GENÈVE : Smsi, 2003.

Pour comprendre le fonctionnement interne d'un groupe terroriste comme Al-Qaeda, par exemple, il faut pénétrer le système de communication interne et externe puisque c'est ce système qui permet de découvrir la culture du groupe et la façon dont il envisage son rôle dans une cyberculture mondialisée et dont il adopte une contre-culture de cybersécurité à son avantage.

Le monde développé réussira d'autant mieux à instaurer une culture de cybersécurité qu'il appréhende les cultures organisationnelles, les cybercultures et les contre-cultures de la cybersécurité, car les objectifs de ces groupes se retournent souvent contre certains pouvoirs publics, gouvernements, institutions, civilisations et individus. Le savoir acquis pour le développement peut tout aussi bien s'appliquer aux groupes qui visent à affaiblir ou éliminer leurs adversaires.

Qu'on envisage le problème de la sécurité du point de vue des gouvernements, du milieu des affaires ou de la société civile, les paradigmes d'analyse ne diffèrent guère. Les gouvernements ont des citoyens et des institutions à protéger ; les grandes sociétés multinationales mènent des services de renseignements pour mieux pénétrer des marchés, pour protéger leur personnel et leurs investissements[32] ; la société civile a tout intérêt à protéger ses propres intérêts de la même manière. C'est le défi de développement que le

[32] L'entreprise multinationale se voit dans l'obligation de protéger ses salariés et leurs familles de toute une gamme de « threats to the[ir] safety and health » en se servant de renseignements recueillis par les services gouvernementaux ou trouvés dans la documention accessible au grand public. ____. « Doing business in dangerous places » (p. 11) et « Plots, alarms and arrests » (pp 22-24). *The Economist*. 14-20 août 2004.

Smsi essaie de relever par la proposition de plans d'action qui pourront s'appliquer à la suite du Sommet de Tunis en 2005.

Conclusion

Le Smsi nous propose une série de moyens pour accroître la sécurité dans la cyberculture d'un monde à venir qui rapprochera en principe les pays développés des pays en développement. Une utilisation accrue des TIC devra faciliter ce rapprochement et améliorer les conditions de vie de tous les peuples tout en respectant la diversité culturelle et linguistique ainsi que les libertés fondamentales. Cette orientation reflète fidèlement les bonnes intentions de la famille des Nations unies.

Malheureusement, en dépit des déclarations officielles et de l'entente pragmatique entre gouvernements, milieu des affaires et société civile, de nouvelles menaces contre la stabilité et la paix internationales émergent. Les auteurs de ces menaces ont aussi accès aux TIC et participent d'une manière autre à la cyberculture en mettant les techniques de la cybersécurité à leur propre service.

Nous devons rester vigilants et nous rendre compte du fait que tout un chacun a une responsabilité accrue d'établir en collaboration avec tous les peuples de bonne volonté dans toute leur diversité une culture de cybersécurité qui sera pour nous une force dynamique de développement économique, social, intellectuel et culturel à l'épreuve des contre-cultures qui visent à déstabiliser le monde.

OUVRAGES CITÉS

_____. « Doing business in dangerous places » *The Economist* (14-20 août 2004) : 11.

_____. « Plots, alarms and arrests ». *The Economist* (14-20 août 2004) : 22-24.

Aïta, Samir. « Internet en langue arabe : espace de liberté ou fracture sociale ? » *Maghreb-Machrek* 178 (hiver 2003-2004) : 29-44.

Anderson, Jon W. « Des communautés virtuelles ? ». *Maghreb-Machrek* 178 (hiver 2003-2004) : 45-57.

Archibald, J. **«** Pour une réduction de la fracture numérique ». *Chroniques* (août 2002). http://www.orbicom.uqam.ca/index_fr.html

_____. « Recognizing Cultural Diversity as a Dynamic Force in Cyberspace ». *Information Technologies and International Development* 1 (3-4, Spring-Summer 2004) : 83-84.

_____. « Vers une politique internationale de la diversité sur la Toile ». Communication présentée dans le cadre du colloque « La localisation sur la Toile : politiques, stratégies et pratiques ». MONTRÉAL : Université McGill, octobre 2004. http://upload.mcgill.ca/conted-translation/La-localisation-sur-la-toile.pdf

Allwood, Jens. *Linguistic Diversity and the Digital Divide*. GŐTENBORG : University of Götenborg, Department of Linguistics, Papers in Theoretical Linguistics, 2004.

Calvet, Louis-Jean. *Pour une écologie des langues du monde*. PARIS : Plon, 1999.

Commission européenne. « Security research a "key topic" in next Framework Programme », 19 juillet 2004. http://europa.eu.int/comm/research/security/news/article_1282_en.html (14 Sept 2004).

Crews, Clyde Wayne et Adam Thierer. « Introduction : Who Rules the Net? ». In Thierer, Adam, dir. *Who Rules the Net?* WASHINGTON : Cato Institute, 2004.

Heinrich-Böll Foundation. *Major conflicts still unresolved*. 12 novembre 2003. http://www.worldsummit2003.de/en/web/517.htm (3 novembre 2004).

Gonzalez-Quijano, Yves. « L'Internet arabe ». *Maghreb-Machrek* 178 (hiver 2003-2004) : 7-9.

Keegan, John. *Intelligence in War*. NEW YORK : Random House, 2004.

Marchi, Sergio. « Canadian Statement to the World Summit on the Information Society ». GENÈVE : Smsi, 2003.

Raboy, Marc et Normand Landry. *La communication au cœur de la gouvernance globale, Enjeux et perspectives de la société civile au Sommet mondial sur la société de l'information*. MONTRÉAL : Département de communication, Université de Montréal, 2004.

Ramonet, Ignacio. *Guerres du XXI^e siècle*. PARIS : Galilée, 2002.

Roy, Olivier. *L'Islam mondialisé*, nouvelle édition. PARIS : Le Seuil, 2004.

Sainsaulieu, Renaud. *Sociologie de l'organisation et de l'entreprise*. PARIS : Presses de la Fondation nationale des sciences politiques & Dalloz, 1987.

Schmitt, Burkard, rapporteur. *Research for a Secure Europe*. LUXEMBOURG : Office for Official Publications of the European Communities, 2004.

Sommet mondial sur la société de l'information. *Déclaration de principes, Construire la société de l'information : un défi mondial pour le nouveau millénaire* (WSIS-03/GENEVA/DOC/4-F). GENÈVE : UIT, 12 mai 2004.

_____. *Plan d'action* (WSIS-03/GENEVA/DOC/5-F). GENÈVE : UIT, 12 mai 2004.