Article publié *in* Sagyngaliy AIDERBAYEV, Pierre CHABAL & Zhuldyz SAIRAMBAEVA (dir.), *Mutations de société et réponses du droit. Perspectives franco-asiatiques comparées*, Bruxelles, Peter Lang, 2017, pp. 71-82.

Organisations régionales et cybersécurité : divergences euro-asiatiques à l'ère du numérique

Philippe Ch.-A. GUILLOT
École de l'Air

[Les propos de l'auteur demeurent son expression personnelle et ne reflètent pas nécessairement la position officielle de l'Armée de l'Air ou du Gouvernement français]

Le cyberespace n'appartient à personne mais n'est pas non plus une *res communis*, car « il existe un mouvement de territorialisation du cyberespace matérialisé par la politique chinoise d'isolement de son réseau ou par une segmentation du droit applicable en raison de l'absence d'instruments internationaux universels à même de réglementer l'ensemble du cyberespace de manière uniforme »[1]. Cette territorialisation est au centre des divergences entre les organisations internationales et arrangements régionaux (pan)européens et asiatiques en matière de sécurité cybernétique ou cybersécurité. Cette notion comprend :

- la lutte contre la cybercriminalité, sachant que l'alinéa 9 du Préambule de la *Convention de lutte contre la cybercriminalité* signée à Budapest le 23 novembre 2001 définit la cybercriminalité comme les *« actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données »*[2] ;
- la lutte contre le cyberterrorisme, lequel « consiste essentiellement à détruire ou à corrompre des systèmes informatiques dans le but de faire pression sur un gouvernement ou une entreprise »[3] ;

[1] Anne-Thida Norodom, « Internet et le droit international : défi ou opportunité ? », *in* S.F.D.I., *Internet & le droit international – Colloque de Rouen 2013*, Paris, Pédone, 2014, p. 19-20 ; la Chine exporte également sa technologie de contrôle du cyberesâce vers l'Iran et d'autres régimes autoritaires, cf. Andrew J. Nathan, « The Authoritarian Resurgence : China's Challenge », *Journal of Democracy*, vol. XXVI, n° 1, 2015, p. 163.

[2] Pour d'autres définitions et des typologies cybercriminelles, cf. Mohamed Chawki, *Étude approfondie sur le phénomène de la cybercriminalité et sur les mesures de lutte mises en place par la communauté internationale*, Le Caire, Dar El-Nadha El-Arabia, 2015, p. 5 et s.

[3] Frédéric-Jérôme Pansier & Emmanuel Jez, *La criminalité sur l'Internet*, Paris, PUF, 2000, p. 110 ; sur ce phénomène dont « beaucoup en vivent et très peu en meurent » cf. Olivier Kempf, « Le cyberterrorisme : un discours plus qu'une réalité », *Hérodote*, n° 152-153, 2014, p. 82 et s.

- et les mesures défensives – voire offensives – en matière de « guerre de l'information »[4], en d'autres termes, la « cyberdéfense », qui ne relève pas de la science-fiction puisqu'au forum de Davos de 2010, Le secrétaire général de l'Union internationale des télécommunications (U.I.T.) Hamadoum TOURE avertissait de la possibilité d'une « cyberguerre [qui] serait pire qu'un tsunami ».[5]

Il apparaît que l'Occident – si tant est que l'expression est un sens compte tenu des différences de conception de la liberté d'expression ou de la protection des données personnelles entre les États-Unis et l'Europe – et l'Orient divergent quant au traitement de cette notion, à tel point qu'on a pu parler de « guerre froide numérique »[6]. Au-delà des divergences quant à la substance d'un régime de cybersécurité, s'opère une sorte de « division du travail » entre institutions occidentales spécialisées par secteurs [I] tandis que l'Organisation de coopération de Shanghai (O.C.S.) privilégie une approche globale de la cybersécurité ou de la « sécurité de l'information internationale » pour utiliser l'expression par elle usitée depuis 2009 [II]. Réunissant la majeure partie de l'hémisphère nord, l'Organisation pour la sécurité et la coopération en Europe (O.S.C.E.) pourrait faire émerger une synthèse en développant non seulement une vision unifiée de la cybersécurité mais aussi grâce au rapprochement possible des positions antinomiques par des mesures de confiance, d'autant plus que le forum de coopération économique Asie-Pacifique (APEC) et le Forum régional de l'Association des Nations du Sud-Est Asiatique (A.R.F.) semblent lui emboîter le pas [III].

I) La division du travail parmi les organisations occidentales

Le Conseil de l'Europe s'est spécialisé dans la lutte contre la cybercriminalité avec la Convention de Budapest et coopère en ce domaine avec l'Union européenne (U.E.) [A], tandis

[4] Cf. Christopher C. Joyner & Catherine Lotrionte, « Information Warfare as International Coercion : Elements of a Legal Framework », *European Journal of International Law*, vol. XII, 2001, p. 825 et s. ; Jean-Marie Bockel, *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense*, Paris, Sénat, 18 juillet 2012, p. 11 et s. ; le dossier « Guerre de l'information », *Revue Défense Nationale*, n° 770, mai 2014, p. 17 et s.

[5] Xavier Leonetti, *Guide de cybersécurité. Droits, méthodes et bonnes pratiques*, Paris, L'Harmattan, 2015, p. 90 ; cf. Andrew Nagorski (dir.), *Global Cyber Deterrence. Views from China, the U.S., Russia, India, and Norway*, New York, East-West Institute, 2010 ; Nazli Choucri & Daniel Goldsmith, « Lost in cyberspace : Harnessing the Internet, International Relations, and Global Security », *Bulletin of the Atomic Scientists*, vol. LXVIII, n° 2, 2012, p. 70 et s. ; Coline Ferro & Oriane Barat-Ginies, « Le cyberspace, un nouveau champ de conflictualité », *Géostratégiques*, n° 38, 2013, p. 105 et s. ; James A. Lewis, *Asia : The Cybersecurity Battleground. Statement before the House Foreign Affairs Commitee*, Washington, Center for Strategic and International Studies, 23 juillet 2013, 7 p.

[6] Cf. Philippe Achilléas, « Guerre froide numérique. Autour de la révision du Règlement des télécommunications internationales », *Revue générale de droit international public*, 2013/2, p. 300 et s.

que l'Organisation du Traité de l'Atlantique Nord (OTAN) se concentre sur la cyberdéfense [B].

A) La lutte contre la cybercriminalité par le Conseil de l'Europe et l'Union européenne

1) Le Conseil de l'Europe

La Convention de Budapest réunit une cinquantaine d'États qui sont des membres du Conseil de l'Europe[7] mais aussi des pays tiers[8]. Le *Protocole additionnel* à la Convention de Budapest *relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, ouvert à la signature le 28 janvier 2003 et entré en vigueur le 1er mars 2006, est aussi un texte débordant le simple cadre européen.[9] Ces deux instruments donnent aux Hautes Parties des directives quant à l'adoption, dans leur droit interne, de normes anti-cybercriminalité.

2) L'Union européenne

La stratégie de cybersécurité de l'Union prévoit certes de « développer une politique et des moyens de cyberdéfense liée à la politique de sécurité et de défense commune » mais en conjugaison avec l'OTAN pour « éviter les doublons »[10]. Son action reste donc limitée aux aspects civils de la cybersécurité avec la création de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), « véritable plateforme européenne permettant l'échange et le partage d'informations relatives à la cybersécurité »[11] et la lutte contre la cybercriminalité, grâce notamment à EUROPOL. La stratégie du Conseil de l'U.E. contre la cybercriminalité intègre une série de mesures opérationnelles – cyberpatrouilles, équipes d'enquêtes communes, recherches à distance – et un renforcement de la coopération et de l'échange d'informations entre les autorités répressives et le secteur privé.[12] Depuis 2013, une

[7] La Russie et Saint-Marin n'ont pas signé la Convention ; Andorre, la Grèce, l'Irlande, le Liechtenstein, le Luxembourg, Monaco et la Suède ne l'ont pas ratifié.

[8] Australie, Canada, États-Unis d'Amérique, Israël, Japon, Maurice, Panama, République dominicaine et Sri Lanka.

[9] Parmi les États tiers au Conseil de l'Europe, seuls le Canada et l'Afrique du Sud l'ont signé ; compte tenu de la valeur constitutionnelle du *freedom of speech*, les États-Unis refusent de le signer ; c'est d'ailleurs à cause de cette conception états-unienne de la liberté d'expression que la Convention de Budapest ne contient pas les dispositions restrictives qui ont justifié l'adoption du Protocole.

[10] Commission européenne, *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, JOIN(2013) 1 final. Cf. Alix Desforges, « Les stratégies européennes dans le cyberespace », *in* Annie Blandin-Obernesser (dir.), *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, 2016, p.81 et s.; Piret Pernik, « Improving Cyber Security : NATO and the E.U. », *eo. loco*, p. 143 et s.

[11] Vincent Joubert & Jean-Loup Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et l'U.E. », *Hérodote*, n° 152-153, 2014, p. 269.

[12] Cf. Céline Castets-Renard, *Droit de l'internet : droit français et européen*, Paris, Montchrestien/ Lextenso, 2e éd., 2012, p. 469-470.

unité d'EUROPOL, le Centre européen de lutte contre la cybercriminalité *(European Cybercrime Centre – E.C.3)* concentre son action sur la fraude en ligne, l'exploitation sexuelle des mineurs et les attaques des infrastructures critiques et des systèmes d'information de l'Union européenne. Il apporte son soutien aux enquêtes opérationnelles et de police scientifique par la mise en place d'un système d'assistance et peut mobiliser « toutes les ressources pertinentes dans les États membres, afin d'atténuer et de réduire la menace cybercriminelle. »[13] L'entraide judiciaire se manifeste au sein de l'Union avec le parquet européen EUROJUST qui a notamment réalisé l'opération *Koala* en 2007 contre les réseaux pédophiles présents dans 19 pays[14].

3) La coopération pan-européenne

Il s'agit de projets que l'Union européenne mène avec le Conseil de l'Europe pour accroître la coopération, y compris judiciaire, en matière de lutte contre la cybercriminalité : les projets *CyberCrime@IPA* élaboré dans le cadre de l'Instrument de Pré-Accession au profit de l'Albanie, de la Bosnie-Herzégovine, du Kosovo, de l'Ancienne République Yougoslave de Macédoine, du Monténégro, de la Serbie et de la Turquie[15] et *CyberCrime@EaP* conçu dans le cadre du Partenariat oriental pour l'Arménie, l'Azerbaïdjan, le Belarus, la Géorgie, la Moldavie et l'Ukraine.[16] Il convient d'ajouter le *Projet joint sur l'Action globale sur la cybercriminalité* (*GLACY*) du Conseil de l'Europe et de l'U.E., signé le 18 octobre 2013, auquel les États-Unis pourraient adhérer[17].

B) La cyberdéfense, chasse gardée de l'OTAN

Après avoir subi des attaques en déni de services lors de son intervention au Kosovo, l'OTAN a lancé son programme de cyberdéfense *NATO Computer Incident Response Capability* en 2002, lequel repose sur un Centre de coordination à Bruxelles et sur un Centre technique à Mons. En 2008, l'OTAN a créé à Tallinn le *Cooperative Cyber Defence Centre of Excellence* (C.C.D.C.O.E.), lequel a commandité une étude de droit prospectif sur la cyberguerre connu sous le nom de *Manuel de Tallinn*[18]. Le dispositif est complété par le *Cyber*

[13] M. Troels Oerting, (directeur de l'E.C. 3), cité par A. Beky, « Le Centre européen anti-cybercriminalité (EC3) ouvre ses portes », 11 janvier 2003, <http://www.silicon.fr/le-centre-europeen-cybercriminalite-ec3-europol-82588.html>.
[14] Cf. Christiane Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'Internet*, Paris, Dalloz, 6e éd., 2010, p. 1015.
[15]<http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp>.
[16] <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/Default-EaP_en.asp>.
[17] <http://www.coe.int/fr/web/portal/-/glacy-en->
[18] L'intitulé exact est *Tallinn Manual on the International Law applicable to Cyber Warfare*. Cf. Mireille Couston, *Droit de la sécurité internationale*, Bruxelles, Larcier, 2016, p. 247 et s.

Defence Management Authority chargé de coordonner et d'initier des actions de cyberdéfense immédiates et effectives grâce à des équipes de réaction rapide. Enfin, le 8 juin 2011, les ministres de la défense des pays de l'Alliance atlantique ont approuvé une politique de cyberdéfense (document confidentiel).[19]

Cependant, il semblerait que l'OTAN ait des difficultés à développer une vision globale de la cybersécurité et à spécifier des normes ou des aspirations partagées y afférentes. Une des conséquences de ce manque de vision est le refus d'indiquer quel type de cyber-attaques contre un membre serait susceptible d'entrainer une réponse de défense mutuelle. La préférence est plutôt donnée aux consultations au cas par cas, et pour les membres de choisir s'ils soutiennent l'État ciblé.

La prédominance états-unienne exercée au sein de l'OTAN et, indirectement, sur l'U.E., s'étend encore plus largement puisque le traité ANZUS a été amendé pour inclure la coopération en matière de cybersécurité et que les États-Unis ont signé un mémorandum d'entente sur les cyberattaques avec l'Inde.[20] Ce qui explique que, dans sa défense d'un monde multipolaire, l'O.C.S., adopte une autre position.

II) L'approche globale et alternative de l'O.C.S.

Par rapport aux politiques euro-atlantiques sectorielles, l'O.C.S. développe une approche globale [A'] et insiste sur la souveraineté numérique[21] des États [B'].

A') Une conception globale de la cybersécurité

Au contraire de leurs homologues otaniens, les membres de l'O.C.S. ont été capables de se mettre d'accord sur des règles de collaboration en matière de cybersécurité du fait de l'insistance de l'organisation sur la coopération sécuritaire au nom de la souveraineté nationale et de l'intégrité territoriale et contre les « trois fléaux » du terrorisme, du séparatisme et de l'extrémisme. Alors même que les motifs de coopération sont moins prisés par les membres de

[19] Cf. UNIDIR, *The Cyber Index: International Security Trends and Realities*, Genève, ONU, 2013, p. 108-109; pour une présentation beaucoup plus détaillée, cf. Olivier Kempf, *L'OTAN au XXI e siècle. La transformation d'un héritage*, Perpignan / Paris, Artège / Éditions du Rocher, 2e éd., 2014, p.515 et s..

[20] Cf. Cassandra M. Kirsch, « Science Fiction No More: Cyber Warfare and the United States », *Denver journal of International Law & Policy*, vol. XL, n° 4, p. 641.

[21] Cette notion n'est toutefois pas incompatible avec la conception européenne du cyberespace, cf. Pierre Bellanger, *La souveraineté numérique*, Paris, Stock, 2014 ; Pierre Trudel, « Ouverture – La souveraineté en réseaux », *in* Anne Blandin-Obernesser (dir.), *op. cit.*, p. 5 et s.

l'O.C.S. que l'intérêt de l'État ou la préservation du régime politique, la compréhension commune que chacun d'eux est confronté à des menaces similaires leur permet de coopérer.[22]

Cette coopération prend notamment la forme de plateformes de partage de renseignement et de bases de données communes. En septembre 2014, la Structure régionale anti-terroriste a créé un groupe d'experts avant d'identifier et prévenir les utilisations de l'internet au profit des trois fléaux.

La conception extensive des cyberattaques de l'O.C.S. comprend l'utilisation des TIC pour déstabiliser les régimes politiques ce qui permet aussi de lutter contre toute contestation politique[23]. Sur ce point, l'O.C.S. diverge des organisations occidentales en promouvant un étroit contrôle national non seulement sur les systèmes informatiques mais aussi sur les contenus[24].

Sans surprise, une coopération similaire existe au sein de l'Organisation du traité de sécurité collective (O.T.S.C.) en matière de surveillance des TIC et des réseaux sociaux aux fins de lutte contre d'éventuelles entreprises de déstabilisation des États membres avec le *Règlement sur la coopération dans le domaine de la sécurité de l'information* adopté en 2010.[25] Lors d'un sommet informel de l'O.T.S.C. en 2011, S.E. Nursultan NAZARBAEV a plaidé pour le développement d'une « muraille inexpugnable » afin de contrer toute menace provenance de l'utilisation des TIC[26]. Par ailleurs, le traité russo-chinois du 8 mai 2015 se situe bien évidemment dans la même perspective[27].

B') La politique alternative militante de l'O.C.S.

L'*Accord sur la coopération dans le domaine de la sécurité de l'information internationale*[28] de l'O.C.S. reprend les concepts d'« utilisation de l'information pour fragiliser le système politique, économique et social d'autres États de même que leur environnement spirituel et culturel », de « domination de l'aire informationnelle au détriment des intérêts et de

[22] Belfer Center for Science and International Affairs/ CSAIL-MIT/Canada Centre for Global Security Studies/ Amercian Bar Association, *A Call to Cyber Norms. Discussions at the Harvard – MIT – University of Toronto Cyber Norms Workshops, 2011 and 2012*, mars 2015, p. 35.
[23] Cf. Oona A. Hattaway *et alii*, « The Law of Cyber-Attack », *California Law Review*, vol. C, 2012, p. 53.
[24] Cf. Abraham D. Sofaer, David Clark & Whitfiled Diffie, « Cyber Security and International Agreements », *Proceedings of a Workshop on Dettering Cyber Attacks : Informing Strategies and Developing Options for U.S. Policy*, National Academy of Sciences, p. 186, <http://www.nap.edu/catalog/12997.html>.
[25] Nuria Kutnaeva, « The Complexities of Central Asian Cyber Security », *Per Concordiam*, vol. V, n° 2, 2014, p. 18.
[26] Cité *in* Privacy International, *Private Interests : Monitoring Central Asia. Special Report*, novembre 2014, p.25.
[27] Cf. Elaine Korzak, « The Next Level For Russia-China Cooperation? », 20 août 2015, <http://blogs.cfr.org/cyber>.
[28] Signé le 16 juin 2009 à Iekaterinbourg, <http://www.sectsco/EN/show.asp?id=95>.

la sécurité des autres États » et d'« influence transfrontière non autorisée par l'information » que la Russie avait formulés dès 1999.[29]

La Chine, l'Ouzbékistan, la Russie et le Tadjikistan ont présenté en septembre 2011 à l'Assemblée générale des Nations Unies un projet de Code de conduite internationale pour la sécurité de l'information[30]. Prenant en compte différents commentaires et suggestions provenant de divers États ou du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (G.G.E.)[31], ainsi que les travaux de la Conférence mondiale des télécommunications internationales (C.M.T.I.) de décembre 2012 à Dubaï mais aussi les révélations de M. Edward SNOWDEN[32] de juin 2013, l'O.C.S. a déposé à l'Assemblée générale une nouvelle version de ce Code en janvier 2015 afin de faire avancer le débat international sur les normes universelles relatives à la sécurité de l'information et d'aider à dégager un consensus en la matière.[33] Le Code insiste avant tout sur la souveraineté de l'État et sur la territorialité dans l'espace numérique et est pétri de considérations afférentes aux impératifs du renseignement, de la sécurité nationale et de la stabilité des régimes politiques. Il reprend les recommandations du G.G.E. sur la mise en place de mesures de confiance (M.D.C.) afin de prévenir les conflits entre États. S'appuyant sur les résultats du Sommet mondial de la Société de l'Information[34] et de la C.M.T.I., le Code insiste sur les droits souverains des États à régir les questions d'intérêt public relatives à l'Internet et sur l'égale responsabilité que les États devraient avoir en matière de la gouvernance de l'Internet, de sa sécurité, de sa continuité, de sa stabilité et de son développement.[35] Il est parcouru de références à la « stabilité sociale » ou la « sécurité de la société ». En revanche, il est notable que le Code ne fasse pas la moindre référence à la protection des données personnelles ou de la vie privée.

Lors de la Conférence de l'U.I.T. de 2012 au sujet de la révision du Règlement sur les télécommunications internationales, dont l'applicabilité à l'Internet a opposé les États membres, certains pays dont la Chine et la Russie ont milité pour l'accroissement des

[29] Doc. ONU A/54/213.
[30] Doc ONU A/66/359.
[31] Doc. ONU A/68/98.
[32] Cf. James A. Lewis, « Étude préliminaire sur les analyses en cybersécurité: l'affaire Snowden comme étude de cas », *Hérodote*, n° 152-153, 2014, p. 26 et s. et le dossier « After Snowden : Rethinking the Impact of Surveillance », *International Political Sociology*, vol. VIII, 2014, p. 121 et s.
[33] Doc ONU A/69/273.
[34] Cf. Guillaume Le Floch, « Le sommet mondial de Tunis sur la société de l'information », *Annuaire français de droit international*, vol. LI, 2005, p. 464 et s.
[35] Cf. Sarah McKune, « An Analysis of the International Code of Conduct for Information Security », 28 septembre 2015, <https://citizenlab.org/2015/09/international-code-of-conduct>.

compétences de l'U.I.T. dans le cyberespace, « moins pour en réguler l'épanouissement que pour mieux contrôler le réseau puisqu'ils voulaient que le Règlement consacre le droit souverain de chaque État de réglementer l'internet sur son territoire. »[36] Pour l'O.C.S., la souveraineté numérique signifie que les États ont juridiction sur les infrastructures et les activités des TIC sur leur territoire, que les gouvernements ont le droit d'élaborer et conduire des politiques publiques pour le cyberespace fondées sur des conditions nationales particulières et qu'aucun pays ne doit utiliser l'Internet pour s'ingérer dans les affaires intérieures d'autres pays ou pour nuire aux intérêts d'autres pays. Alors que l'Organisation de coopération et de développement économiques (O.C.D.E.) et ses États membres – principalement occidentaux mais aussi asiatiques – tiennent à préserver la liberté de l'Internet, ainsi que son unicité : « une fragmentation suivant les frontières nationales remettrait en question beaucoup de ses avantages pour l'avenir »[37]. Pourtant, force est de constater une « volonté de réappropriation par les États du cyberespace [dont l]a gouvernance connaît ainsi actuellement un mouvement d'interétatisation plus que d'internationalisation »[38].

Tandis qu'une coopération interrégionale serait souhaitable pour la cybersécurité, les réponses divergentes des organisations régionales « balkanisent » le régime du cyberespace[39]. Une solution pourrait être trouvée grâce aux arrangements inter-régionaux ou transrégionaux.[40]

III) Vers une vision commune de la cybersécurité grâce à l'approche des organisations inter-régionales ?

L'O.S.C.E. et, dans une moindre mesure, l'APEC et l'A.R.F. développent une approche globale de la cybersécurité dans laquelle sont déployées des M.D.C. pouvant être à même de concilier la sauvegarde d'un cyberespace ouvert et le respect de la souveraineté des États [A"]. La souveraineté numérique doit elle-même être compatible avec un autre domaine de compétence de l'institution viennoise que sont les droits de l'Homme [B"].

A") Les organisations intercontinentales

1) L'approche pragmatique de l'O.S.C.E.

[36] Frank Latty, « La diversité des sources du droit de l'Internet », *in* S.F.D.I.., *op. cit*., p. 52-53, notes omises.
[37] Réunion à Haut Niveau de l'O.C.D.E., *L'économie Internet : un moteur d'innovation et de croissance*, synthèse du Président, 28-29 juin 2011, p. 6.
[38] Anne-Thida Norodom, *op. cit.*, p. 20.
[39] Cf. Amaël Cattaruzza, « La "balkanisation" du cyberespace », *in* Annie Blandin-Obernesser, *op. cit.*, p.109 et s.
[40] Sur ces notions, cf. Sun-Hee Park, « L'interrégionalisme comme forme de coopération régionale », *in* Pierre Chabal (dir.), *Régions, institutions, politiques. Perspectives euro-asiatiques institutionnelles et fonctionnelles*, Paris, Apopsix, 2010, p. 62 et s.

L'O.S.C.E. a commencé à s'intéresser à la cybersécurité en 2008 en organisant plusieurs réunions à haut niveau sur ce thème. En 2011, elle organisa une conférence sur une *Approche globale de la cybersécurité.* Habituée à travailler sur des sujets civils comme sur des sujets militaires, l'O.S.C.E. n'a eu évidemment aucun problème à concevoir de manière holistique la cybersécurité puis, forte de son expérience en M.D.C. acquise dans le domaine du désarmement et de la maîtrise des armements, elle en est venue à transposer différentes procédures d'échange d'informations et de surveillance mutuelle au cyberespace. Le 26 avril 2012, le Conseil permanent adopta la décision n° 1039 *Mesures de confiance de l'O.S.C.E. visant à réduire les risques de conflit découlant de l'utilisation des technologies d'information et de communication.* Le 10 mars 2016, le Conseil permanent a adopté la décision n° 1202 éponyme qui complète la précédente en renforçant les échanges d'informations entre États membres.et les invite à mener « des activités sur une base volontaire pour aider les autorités et les experts à faciliter l'accès aux voies de communication autorisées et protégées en vue de prévenir et de réduire les risques de perception erronée, d'escalade ou de conflit mais aussi de clarifier les mécanismes techniques, juridiques et diplomatiques pour pouvoir traiter les demandes en rapport avec les TIC », ainsi qu'à nouer « une collaboration régionale et sous-régionale entre les autorités compétentes sur le plan juridique pour sécuriser les infrastructures critiques en vue d'examiner les opportunités et de relever les défis posés aux réseaux TIC nationaux et transnationaux sur lesquels repose cette infrastructure critique. »

2) Le régime de cybersécurité en construction de l'APEC

L'APEC s'intéressant essentiellement au commerce et à l'économie – ses membres sont appelés « économies » et comportent une région chinoise (Hong Kong) et un État non reconnu comme tel par certains autres membres (Taïwan) – ses premières réalisations dans l'établissement d'un régime de cybersécurité ont concerné des normes de droit souple relatives au commerce électronique dès 1999 – fondées en grande partie sur les lignes directrices de l'O.C.D.E. – et aux données personnelles à partir de 2003 et, en février 2014, l'APEC a adopté un *Référentiel* élaboré par un groupe de travail conjoint APEC/Union européenne afin de renforcer la compatibilité des normes APEC avec le droit européen des données personnelles.[41] Lors du sommet de Shanghai en mai 2002, l'APEC a adopté une *Stratégie de cybersécurité* concentrée sur les aspects de cybercriminalité. Le *Plan d'action stratégique 2010-2015* du

[41] Cf. Catherine Valerio Barrad & Alan Charles Raul, « APEC Overview », *Privacy, Data Protection and Cybersecurity Law Review*, vol. I, n° 1, p. 29-30.

groupe de travail sur les télécommunications et l'information (APEC TEL) se situe dans cette lignée tout en préconisant une coopération accrue avec le secteur privé.

3) L'embryonnaire politique de cybersécurité de l'A.R.F.

L'ASEAN n'ayant pour l'instant que des velléités de construction d'un régime régional de coopération en matière de cybersécurité[42], c'est l'A.R.F. qui fournit le cadre de coopération pour l'Asie méridionale élargie au Pacifique. Il ne s'agit que d'un cadre de droit souple mais qui, néanmoins, témoigne d'une certaine montée en puissance depuis la publication en 2006 d'une *déclaration sur la coopération dans la lutte contre les cyberattaques et l'utilisation terroriste du cyberespace*[43] puisque l'A.R.F. a dernièrement hébergé un *Atelier sur les mesures de renforcement de la cyberrsécurité – aspects juridiques et culturels* codirigé par la Chine et la Malaisie, a adopté un *Plan de travail sur la lutte contre le terrorisme et le crime transnational* avec l'Australie, la Malaisie et la Russie comme chefs de file et travaille au développement de mesures de confiance cybernétiques.[44] Début mars 2016, un *Atelier sur l'opérationnalisation des M.D.C. pour la coopération lors des réactions aux cyber-incidents* s'est enu à Kuala Lumpur, co-présidé par la Malaisie et l'Union européenne.

B") Mesures de cybersécurité et droits de l'Homme

Selon le rapport d'un groupe d'experts de l'Office des Nations Unies contre la drogue et le crime (UNODC) sur la cybercriminalité, « [l]e droit international des droits de l'Homme constitue une arme aussi bien offensive que défensive puisqu'il oblige à la fois à incriminer (de façon limitée) les formes d'expression extrêmes et à protéger les autres formes »[45] . Le rapport de l'UNDOC précise que les contenus représentent un important motif de préoccupation pour les gouvernements qui « cherchent à éliminer non seulement les contenus pédopornographiques ou ayant pour but l'incitation à la haine, mais aussi ceux qui sont diffamatoires ou critiques à leur égard, ce qui soulève des problèmes du point de vue des droits de l'Homme dans certains cas. »[46] La cybersurveillance dérive vers la lutte contre les idées subversives (ou considérées comme telles) au mépris de la liberté d'expression, voire vers l'arrestation de cyberdissidents. Or, le filtrage de l'Internet n'est conforme au droit international que s'il obéit au principe de proportionnalité, c'est pourquoi les démocraties libérales restreignent voire interdisent

[42] Cf. Catríona H. Heinl, *Regional Cyber Security : Moving Towards a Resilient ASEAN Cyber Security Regime*, S. Rajaratnam School of International Studies Working Paper, Singapour, n° 263, 9 septembre 2013, p. 5.
[43] <http://www.mofa.go.jp/%5Cregion/asia-paci/asean/conference/arf/state0607-3.html>.
[44] Cf. *Report on the 10th ASEAN Regional Forum Security Policy Conference*, Bandar Seri Begaan, Brunei Darusalam, 23 mai 2013.
[45] UNODC/CCPCJ/EG.4/2013/2, p. 6.
[46] *Ibidem*, p. 3.

l'exportation de techniques de contrôle de l'Internet vers les États autoritaires[47]. Cependant, les États libéraux ne sont pas non plus exempts de critiques comme en attestent plusieurs études[48] et comme l'illustrent les révélations au sujet des écoutes de la *National Security Agency* (N.S.A.) qui ont mis en évidence, d'une part, une « perte de contrôle » de l'U.E. et de ses États membres en matière de souveraineté numérique et, d'autre part, une grande méfiance des institutions européennes ainsi des gouvernements nationaux envers la politique états-unienne de lutte contre le terrorisme.[49] La Commission des libertés civiles, de la justice et des affaires intérieures du P.E. n'hésite pas à fustiger « la mise en place d'un État "ultrapréventif" »[50] et l'Assemblée parlementaire du Conseil de l'Europe dénonce une connivence entre la N.S.A. et les services de renseignement de certains pays alliés.[51] En outre, l'Assemblée générale de l'ONU, dans sa résolution 68/167 du 18 décembre 2013, *Le droit à la vie privée à l'ère du numérique*, rappelle aux États qu'ils doivent « respecter pleinement les obligations que leur impose le droit international des droits de l'Homme »[52], tandis que sa résolution 68/178 du même jour, *Protection des droits de l'Homme et des libertés fondamentales dans la lutte antiterroriste*, les encourage à préserver le droit au respect de la vie privée[53]. Il est vrai que pour de nombreux États, les principales menaces cybernétiques sont états-uniennes[54]. La France n'est pas non plus exemplaire car la loi n° 2015-912 du 24 juillet 2015 relative au renseignement – adoptée alors même que l'*USA Freedom Act* du 2 juin 2015[55] venait de restreindre les

[47] Cf. Philippe Achilléas., « Vers un contrôle des transferts internationaux des biens et des technologies de cybersécurité », *in* S.F.D.I., *op. cit.*, 2013, p. 373 et s. ; pour une vision critique, cf. Innokenty Pyetranker, « An Umbrella in a Hurricane : Cyber Technology and the December 2013 Amendement to the Wassenaar Agreement », *Northwestern Journal of Technology and Intellectual Property*, vol. XIII, n° 2, 2015, p. 153 et s. : le comportement de la Russie est lui évidemment à l'opposé, cf. Peter Bourgelai, *Commonwealth of Surveillance States : On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia*, 29 juin 2013, <http://www.accessnow.org >.

[48] Juli Zeh & Ilija Trojanow, *Atteinte à la liberté : les dérives de l'obsession sécuritaire*, (trad. d'*Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte* par P. Charbonneau), Arles, Actes Sud, 2010 ; Simon Chesterman, *One Nation Under Surveillance. A New Social Contract to Defend Freedom Without Sacrificing Liberty*, Oxford, OUP, 2011; Raf Jespers, *Souriez, vous êtes fichés. « Big Brother » en Europe*, Mons, Couleur livres, 2013.

[49] Cf. Didier Bigo *et alii*, « Open Season for Data Fishing on the Web. The Challenges of the US PRISM Programme for the E.U. », *CEPS Policy Brief*, n° 293, 18 juin 2013, p. 4.

[50] Claude Moraes, *Rapport sur la programme de surveillance de la N.S.A., les organismes de surveillance dans divers États membres et les incidences des droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures*, 21 février 2014, A7-0139/2014, p. 24, § 12.

[51] Pieter Omtzigt, *Les opérations massives de surveillance, Rapport pour la Commission des questions juridiques et des droits de l'Homme de l'Assemblée parlementaire du Conseil de l'Europe*, 26 janvier 2015, § 38.

[52] A/RES/68/167, p. 2 ; le texte pertinent est l'art 17 du Pacte international relatif aux droits civils et politiques du 16 décembre 1966 sur le respect de la vie privée.

[53] A/RES/68/178, p. 4, point 6 g.

[54] Cf. Jack Goldsmith, « Cybersecutity Treaties. A Skeptical View », *in* Peter Berkowitz (dir.), *Future Challenges in National Security and Law*, Hoover Institution / Stanford University, 2011, p. 7-8.

[55] *Uniting and Strenghtening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015*, Public Law 114-23, 129 Stat., p. 268 et s.

pouvoirs en la matière de la N.S.A. – accroît le recours aux moyens de surveillance et d'investigation au profit des services spécialisés.[56] En ce domaine aussi, l'O.S.C.E. peut être une source d'inspiration puisque les *Recommandations d'Amsterdam sur la liberté des médias et l'Internet* adoptées en juin 2003 appellent « à promouvoir la liberté d'expression et à tenter de réduire la censure sur le réseau »[57].

[56] Cf. la communication de Gilles Lebreton dans cet ouvrage ; Philippe Ch.-A. Guillot, « Ombres et lumières sur le droit fondamental à la protection des données personnelles confronté aux services de renseignement en matière de prévention du terrorisme », *Annales de Droit*, n° 10, 2016, p. 165 et s.

[57] Citées par Philippe Lagrange, « Internet et l'évolution normative du droit international : d'un droit international applicable à l'internet à un droit international du cyberespace ? », *in* S.F.D.I., *op. cit.*, p. 71.