ORGANISATION MONDIALE DU COMMERCE

G/TBT/GEN/357

20 juillet 2023

(23-4958) Page: 1/7

Comité des obstacles techniques au commerce

SÉANCE THÉMATIQUE SUR LA COOPÉRATION ENTRE LES MEMBRES DANS LE DOMAINE DE LA RÉGLEMENTATION DE LA CYBERSÉCURITÉ

20 JUIN 2023, 15 HEURES-18 HEURES

Rapport du modérateur[1]

Lors du neuvième examen triennal, les Membres sont convenus de poursuivre la tenue de séances thématiques en conjonction avec les réunions ordinaires qui auraient lieu entre 2022 et 2024, en vue d'approfondir davantage les échanges de données d'expérience du Comité sur des thèmes spécifiques. De ce fait, le Comité est convenu de tenir une séance thématique sur la coopération dans le domaine de la réglementation de la cybersécurité.[2] Cette séance thématique a donné l'occasion d'examiner la contribution des règlements techniques, des normes et des procédures d'évaluation de la conformité aux politiques des Membres visant à faire face aux menaces pour la cybersécurité. Les Membres ont discuté des approches existantes en matière de gestion des risques de cybersécurité et des possibilités de coopération en matière de réglementation. Des renseignements sur les intervenants, les exposés et les documents qui s'y rapportent peuvent être consultés sur le site Web de l'OMC.[3]

1 OBSERVATIONS LIMINAIRES DU MODÉRATEUR

1.1. Cette séance arrivait à point nommé, en particulier dans un contexte où les Membres discutaient de plus en plus des politiques et réglementations relatives à la cybersécurité au sein du Comité OTC.

1.2. À titre d'exemples, premièrement, les Membres avaient notifié aux alentours de 80 mesures liées à la cybersécurité au Comité OTC (au 31 mai 2023). Il s'agissait clairement d'une nouvelle tendance, car la vaste majorité de ces notifications (plus de 60%) n'avaient été présentées qu'à partir de 2020. Ces notifications portaient sur un vaste éventail de produits et de situations, par exemple: la cybersécurité liée à l'Internet des objets (IdO), la technologie 5G, les télécommunications, les véhicules et les équipements radio, ainsi que les produits reposant sur des logiciels et/ou connectés à un réseau. Pour la moitié de ces mesures environ, il était indiqué qu'elles avaient été proposées ou adoptées aux fins de la protection des intérêts de sécurité nationale.

1.3. Deuxièmement, ces dernières années, le Comité OTC avait de plus en plus été utilisé par les Membres comme enceinte pour soulever et examiner les préoccupations commerciales spécifiques (PCS) concernant diverses mesures liées à la cybersécurité. Les mesures visées par ces PCS réglementaient, par exemple: les produits des TIC et les équipements de réseau, les véhicules, l'aviation civile, les banques et les assurances. À ce jour, les Membres avaient soulevé au moins 26 PCS de ce type, dont la majorité (60%) au cours des 6 dernières années (2017-mai 2023). Ces discussions étaient importantes compte tenu de la nature du sujet ainsi que de la valeur chiffrée que représentaient les PCS en question: d'après des estimations du Secrétariat de l'OMC, la valeur moyenne des importations concernées par PCS liée à la cybersécurité était de près de 160 milliards d'USD. De fait, par rapport au reste des PCS relevant des autres "questions", celles

[1] M. Wei Guo Tang (Singapour). Le présent rapport est distribué sous la propre responsabilité du modérateur.

[2] G/TBT/46, paragraphe 2.11.

[3] OMC | Séance thématique sur la coopération entre les Membres dans le domaine de la réglementation de la cybersécurité.

portant sur les mesures liées à la cybersécurité correspondaient à la catégorie la plus importante s'agissant de la valeur.

2 DISCUSSION

2.1 Questions d'orientation

- Quelles sont les difficultés et les possibilités liées au commerce et à la réglementation de la cybersécurité?
- Comment les disciplines et principes de l'Accord OTC de l'OMC contribuent-ils à l'élaboration de politiques commerciales efficaces permettant de garantir la cybersécurité? Quel rôle le Comité OTC peut-il jouer?
- Quelles meilleures pratiques devraient guider l'élaboration et la mise en œuvre de la réglementation dans ce domaine? Quel rôle les normes internationales peuvent-elles jouer à cet égard?

3 INTERVENTIONS

3.1. **M. Mike Mullane** (Commission électrotechnique internationale, CEI)[4] a présenté les travaux de la CEI sur les normes de cybersécurité, en mettant l'accent sur l'approche écosystémique adoptée par l'organisation pour ce qui est de l'élaboration des normes dans ce domaine. La CEI élabore des normes de cybersécurité horizontales qui traitent de la sécurité de l'information et des opérations, ainsi que des normes verticales sectorielles (par exemple, CEI 63154 ou ISO/CEI 29128-1). M. Mullane a également abordé certains des principaux avantages conférés par l'utilisation de normes et d'évaluations de la conformité dans le domaine de la cybersécurité, comme l'instauration d'une confiance avec les partenaires commerciaux, la garantie d'une cohérence grâce à l'harmonisation, l'amélioration de l'accès aux marchés et une reconnaissance accrue au niveau mondial. Il a également donné des précisions sur l'approche fondée sur les risques des normes de la CEI, qui encourage les entreprises à classer leurs actifs selon le niveau de sécurité requis. M. Mullane a conclu en soulignant qu'il était important de collaborer à l'échelle mondiale pour faire face aux menaces en matière de cybersécurité, et il a encouragé les Membres à adopter le cadre commun de normes de la CEI.

3.2. **Mme Nandini Jolly** (Canada)[5] a expliqué qu'au lendemain de la pandémie de COVID-19 et dans le contexte géopolitique actuel, la sécurité axée sur les données (par opposition à celle uniquement axée sur les réseaux) revêtait une importance croissante. Elle a présenté l'approche "confiance zéro" adoptée par CryptoMill en matière de cybersécurité, qui vise à passer à une sécurité axée sur les données, et elle a souligné qu'il était important d'avoir conscience de l'existence des risques au sein et en dehors des réseaux.

3.3. CryptoMill propose des services spécialisés dans la résolution de problèmes liés aux piratages externes, aux fuites de données internes, aux rançongiciels, aux vulnérabilités dans les chaînes d'approvisionnement, aux courriers électroniques mal acheminés, aux données résiduelles et aux appareils volés. Mme Jolly a également présenté la suite logicielle "Circles of Trust" de l'entreprise, une plate-forme de sécurité qui donne aux entreprises, aux forces armées et aux autorités gouvernementales un contrôle sur l'accès à toutes les données sensibles et leur utilisation, par exemple pour que les données échangées avec les partenaires commerciaux restent aussi protégées. Elle a conclu en évoquant des préoccupations concernant les risques de cybersécurité associés à la popularité croissante du "travail hybride". Mme Jolly a réaffirmé qu'il était important de collaborer et de coopérer, y compris dans le domaine des normes, afin de détecter et d'éliminer ces risques. La collaboration peut contribuer à améliorer le partage de renseignements afin d'accélérer les avancées technologiques nécessaires pour faire face à ces menaces.

3.4. **M. Jonathan McHale** (États-Unis)[6] a présenté un exposé axé sur la nécessité de coopérer et de trouver des solutions au niveau mondial pour faire face aux menaces liées à la cybersécurité. Il a expliqué que les mesures nationales relatives à l'environnement numérique, comme les prescriptions nationales en matière de cryptage ou de sécurité wifi, avaient manifestement des effets

[4] Responsable des activités de sensibilisation, CEI.
[5] Directrice exécutive, Crypto Mill Cybersecurity Solutions (Canada).
[6] Vice-Président chargé du commerce numérique, Computer & Communications Industry Association (États-Unis).

de distorsion des échanges et n'apportaient pas d'avantages flagrants, et que les mesures comme la localisation des données pouvaient parfois compromettre la cybersécurité mondiale en limitant la visibilité des menaces existantes à l'échelle mondiale. Selon lui, une réponse mondiale fondée sur la normalisation était nécessaire pour faire face aux menaces en matière de cybersécurité dans un environnement numérique dont la conception même était à visée mondiale. M. McHale a souligné que la coopération était nécessaire pour parvenir à un consensus au niveau mondial sur la définition des menaces les plus importantes en matière de cybersécurité, afin de résoudre ces problèmes en utilisant les ressources de manière efficace. Il a conclu en rappelant aux participants les principaux facteurs à prendre en compte lors de l'élaboration de normes de cybersécurité, tels que les exigences de conformité connexes, la participation des parties prenantes au processus d'élaboration et les effets sur le commerce.

3.5. **Mme Jacqueline Fick** (Afrique du Sud)[7] a souligné l'importance de la coopération et de l'harmonisation au niveau international afin d'établir une législation en matière de cybersécurité, dans le but de renforcer les dispositifs de cybersécurité et la confidentialité des données. Elle a expliqué que la cybersécurité et la cybercriminalité étaient des questions interdépendantes, qui devaient donc être traitées conjointement. Pour ce faire, elle a proposé une approche transfrontières et collaborative visant à traiter la nature sans frontières de la cybercriminalité, sur la base de mécanismes efficaces et efficients pour résoudre des problèmes qui apparaissaient très rapidement. La législation en matière de cybersécurité est essentielle, car elle permet de soutenir un commerce électronique efficace, d'accroître la confiance entre les pays, d'améliorer les interventions en cas d'incident, ainsi que de renforcer la capacité, si nécessaire, de traduire les cybercriminels en justice. Ainsi, Mme Fich a souligné que l'harmonisation, la coopération internationale et la normalisation étaient nécessaires non seulement pour créer des instruments internationaux efficaces, mais aussi pour renforcer la certitude relative aux pratiques de cybersécurité acceptées au niveau mondial, intensifier les mesures de lutte contre la cybercriminalité et faciliter l'échange, entre les pays, d'éléments de preuve électroniques recevables devant un tribunal. Il n'était pas nécessaire de "réinventer la roue". Aucune de ces démarches ne devait être considérée comme une tentative d'empiéter sur la souveraineté des pays; il s'agissait plutôt d'y voir le renforcement d'un environnement mondial cybersécurisé. Mme Fick a indiqué que le gouvernement sud-africain avait défini le traitement de la cybersécurité comme l'une de ses priorités et elle a présenté l'approche législative à cet égard. Elle a également appelé à intensifier les activités de formation et de sensibilisation relatives à la cybersécurité, ainsi que l'entraide judiciaire et le partage de renseignements.

3.6. **M. Jiefu Gan** (Chine)[8] a présenté un exposé soutenant la nécessité d'une coopération multilatérale plus inclusive dans le domaine de la normalisation et des évaluations de la conformité relatives à la cybersécurité. À cet égard, il a énuméré plusieurs des possibilités et difficultés. Selon M. Gan, il existait des possibilités dans les domaines de l'économie numérique, des données et des produits numériques, ainsi que de la cybersécurité et de la sécurité des données. Parmi les difficultés notables figuraient le déficit de gouvernance numérique au niveau mondial et, par conséquent, le risque de division et de fragmentation de cette gouvernance.

3.7. M. Gan a formulé plusieurs propositions, à savoir: garder les marchés ouverts et exempts de discrimination, renforcer l'unité et la coopération au niveau mondial en créant des règles interopérables et communes, trouver un équilibre entre développement et sécurité, s'engager en faveur de l'équité et de la justice, et rendre la coopération plus inclusive dans le domaine des normes et des évaluations de la conformité relatives à la cybersécurité. Enfin, il a donné des exemples de pratiques adoptées en Chine. Plusieurs mesures avaient été prises, y compris le recours à des procédures d'évaluation de la conformité en tant que moyen technique pour appuyer la gestion de la cybersécurité, et la mise en œuvre de textes législatifs pour promouvoir la certification et les normes.

3.8. **Mme Huirong Tian** (Chine)[9] a présenté un exposé sur les activités normatives relatives à la cybersécurité et à la protection des données menées en Chine dans le domaine des TIC. Elle a présenté les quatre types de normes existant dans ces domaines, ainsi que leurs différentes portées:

[7] Directrice générale, VizStrat Solutions (Afrique du Sud).

[8] Directeur adjoint de département, Centre chinois de l'examen de la cybersécurité, des technologies et de la certification (Chine).

[9] Ingénieur en chef de l'Institut de recherche en sécurité, Académie chinoise des technologies de l'information et de la communication (CAICT) (Chine).

i) les normes nationales; ii) les normes industrielles; iii) les normes d'association; et iv) les normes d'entreprise. Plusieurs comités techniques de la normalisation (TC) existent dans chaque domaine. Par exemple, les normes nationales de sécurité relèvent principalement du TC260. Plus spécifiquement, l'organisation des normes de sécurité industrielles relève de l'Association chinoise de normalisation des communications, et le principal TC chargé des aspects liés à la sécurité est le TC8 (un comité technique chargé de la sécurité des réseaux et des données). Les travaux sur les questions de sécurité menés dans le cadre de l'Association chinoise de normalisation des communications portent par exemple sur les normes relatives à la sécurité des réseaux, des données, des nouvelles technologies et des applications intégrées. La coopération internationale et les organisations internationales de normalisation sont également importantes pour les travaux de l'Association chinoise de normalisation des communications, comme la coopération avec l'Internet Engineering Task Force (IETF) et l'Open Mobile Alliance (OMA), et les partenariats avec la Global Standards Collaboration (GSC) et le projet de partenariat de troisième génération (3GPP).

3.9. **Mme Amy Mahn** (États-Unis)[10] a présenté son organisation et le rôle de longue date que joue celle-ci dans le domaine de la cybersécurité, depuis l'élaboration par la NIST de la norme relative au cryptage des données dans les années 1970. Elle a également présenté le Cadre de la cybersécurité de la NIST, qui aide les organisations à réduire les risques de cybersécurité et a déjà été adopté par de nombreux gouvernements dans le monde, en plus de celui des États-Unis, comme ceux de l'Uruguay, du Japon et de l'Italie, pour n'en citer que quelques-uns. Le Cadre de la cybersécurité s'inspire de nombreux points de vue, issus du secteur privé, des milieux universitaires ou du secteur public, et il fait actuellement l'objet d'un réexamen sur la base des observations transmises par les parties prenantes. Mme Mahn a également réaffirmé certains points antérieurement soulevés par d'autres intervenants concernant le rôle essentiel que pouvaient jouer des normes largement acceptées afin de créer des marchés concurrentiels et sûrs et de faciliter les échanges internationaux.

3.10. **M. Hideyasu Tamura** (Japon)[11] a commencé par évoquer des préoccupations concernant les orientations des mesures relatives à la cybersécurité, qui pouvaient avoir des effets restrictifs pour le commerce. Il s'agissait, par exemple, de prescriptions relatives à l'utilisation de composants ou de logiciels d'origine nationale pour les infrastructures essentielles, fondées sur des raisons de sécurité. Il a rappelé aux participants l'importance qu'il y avait à élaborer des mesures de cybersécurité qui soient conformes à l'Accord OTC et aussi peu restrictives que possible pour le commerce. Comme d'autres intervenants, M. Tamura a souligné la nécessité d'intégrer une approche collaborative au traitement de la cybersécurité, et il a notamment souligné l'approche ambitieuse qui avait été adoptée en matière de normalisation dans le cadre de l'Accord de partenariat transpacifique global et progressiste (PTPGP). Il a conclu en parlant de la nécessité d'établir des systèmes d'étiquetage des produits relatifs à la cybersécurité, qui soient harmonisés et interopérables.

3.11. **M. Mohamad Endhy Aziz** (Indonésie)[12] a présenté les faits nouveaux survenus en matière de cybersécurité en Asie du Sud-Est au cours des dernières années, en soulignant l'importance croissante de l'économie numérique pour la région. En Indonésie, l'environnement numérique se cristallisait autour du commerce électronique et des services numériques, des secteurs qui devraient contribuer au PIB du pays à hauteur d'au moins 14% d'ici à 2027. M. Endhy Aziz a cependant alerté sur le fait que l'Indonésie était de plus en plus exposée aux cybermenaces, le nombre de cyberattaques ayant été multiplié par sept au cours des quatre dernières années. Pour l'Indonésie et d'autres partenaires de l'ASEAN, il était donc particulièrement important de renforcer la coopération internationale sur les questions liées à la cybersécurité. Selon M. Endhy Aziz, la communauté commerciale pouvait prendre des mesures plus poussées afin d'accroître la coopération en matière de cybersécurité, notamment en définissant une conception commune des cybermenaces et de leur portée, et en convenant d'adopter une approche de la cybersécurité fondée sur les risques. Il a conclu en rappelant aux participants l'importance qu'il y avait aussi à assurer la conformité avec

[10] Spécialiste des politiques internationales, Institut national des normes et de la technologie (NIST) (États-Unis).

[11] Directeur principal du Bureau de la politique de commerce extérieur, Ministère de l'économie, du commerce et de l'industrie (METI) (Japon).

[12] Spécialiste principal de la cybersécurité, Agence nationale de cybersécurité et de cryptage (Indonésie).

les normes communes de cybersécurité, tout en continuant à élaborer celles-ci de la façon la moins restrictive possible pour le commerce.

3.12. **Mme Veena Dholiwar** (Royaume-Uni)[13] a donné un aperçu du régime de sécurité des produits du Royaume-Uni, qui s'inscrit dans le cadre de la stratégie nationale du gouvernement en matière de cybersécurité. À l'origine de cette stratégie se trouve l'engagement pris par les autorités de protéger les intérêts des citoyens et de leur éviter tout dommage. Parmi les éléments essentiels du régime figure la Loi de 2022 sur la sécurité des produits et des infrastructures de télécommunications. Avec cette loi, le régime de sécurité du Royaume-Uni serait le premier au monde à imposer des prescriptions minimales en matière de cybersécurité s'appliquant avant que les produits de consommation de l'Internet des objets ou "intelligents" ne soient vendus aux consommateurs.[14]

3.13. Mme Dholiwar a également résumé les travaux menés par le Royaume-Uni en vue d'élaborer un code de pratiques volontaire, des normes internationales et une voie législative. Elle a mis en avant un exercice de collaboration qui comprenait la participation des parties prenantes, des consultations publiques et des appels à opinions ainsi que des travaux de recherche auprès de l'industrie et des consommateurs. Elle a souligné que le régime concordait avec les principes des obligations de transparence dans le domaine des OTC, de l'ouverture et de la collaboration. Enfin, elle a souligné l'engagement pris par le Royaume-Uni en faveur de la collaboration internationale et du partage de données d'expérience avec d'autres Membres.

3.14. **M. Fabio Polverino** (Union européenne)[15] et **M. Luis Miguel Vega Fidalgo** (Union européenne)[16] ont présenté le rôle précieux que joue la réglementation relative à la cybersécurité pour le commerce. Pour illustrer l'importance de cette réglementation, ils ont donné des détails sur les coûts élevés associés aux cyberincidents. L'Allemagne fournissait un exemple clair à cet égard: en 2020, le coût global des incidents de sécurité visant les entreprises s'était élevé à 220 milliards d'euros. Pour traiter la cybersécurité des produits, l'UE a d'abord commencé par se pencher sur les dispositifs sans fil, au moyen de l'acte délégué au titre de la Directive relative aux équipements radioélectriques, pour ensuite se tourner vers un traitement de tous les produits comportant des éléments numériques et de l'ensemble de leur cycle de vie, dans le cadre de la proposition de législation sur la cyberrésilience. Cette approche législative par étapes a permis de réévaluer, de détecter et de corriger les lacunes constatées dans les textes antérieurs.

3.15. Les intervenants ont mis en avant des réglementations existantes et à venir, à savoir: i) l'acte délégué au titre de la Directive relative aux équipements radioélectriques et ii) la législation sur la cyberrésilience. Adopté en 2022, l'acte délégué au titre de la Directive relative aux équipements radioélectriques est un texte législatif axé sur les prescriptions relatives à la cybersécurité dans le cas des dispositifs sans fil. Il vient remédier à une lacune constatée dans un texte législatif antérieur sur les produits et, pour la première fois, impose des obligations en matière de cybersécurité aux fabricants. La législation sur la cyberrésilience, proposée en septembre 2022 et en attente d'adoption définitive, s'appuie sur la législation existante (y compris l'acte délégué au titre de la Directive relative aux équipements radioélectriques) et vient combler un vide juridique en instaurant des prescriptions obligatoires en matière de cybersécurité pour tous les produits comportant des éléments numériques, y compris les produits matériels et logiciels. La législation sur la cyberrésilience a comme objectif principal de veiller à ce que les fabricants garantissent un niveau de cybersécurité adéquat pour les produits comportant des éléments numériques qui sont mis sur le marché de l'UE, dès la phase de conception et de développement et tout au long du cycle de vie du produit. Elle vise aussi à garantir un cadre cohérent en matière de cybersécurité en établissant des exigences horizontales en la matière, et elle renforcera la confiance des consommateurs en améliorant la transparence des propriétés de sécurité. L'acte délégué au titre de la Directive relative aux équipements radioélectriques comme la législation sur la cyberrésilience seront mis en œuvre au moyen de normes applicables aux produits ou aux procédés, en s'appuyant sur les normes

[13] Responsable, respect des règles et preuves, sécurité des produits de l'Internet des objets, Département des sciences, de la technologie et de l'innovation (DSIT) (Royaume-Uni).

[14] Le régime impose trois prescriptions en matière de sécurité que les fabricants doivent respecter avant de vendre leurs produits aux consommateurs du Royaume-Uni.

[15] Chargé de mission, Unité responsable des politiques en matière de cybersécurité et vie privée numérique, Direction générale des réseaux de communication, du contenu et des technologies, Commission européenne.

[16] Chargé de mission, Unité responsable des machines et équipements, Direction générale du marché intérieur, de l'industrie, de l'entrepreneuriat et des PME, Commission européenne.

européennes et internationales existantes. Cette démarche démontre le rôle et les avantages des normes en vue, notamment, d'assurer une sécurité juridique, de réduire les coûts de mise en conformité et d'éviter les obstacles au commerce.

4 DISCUSSION

4.1. La discussion a donné lieu à un dialogue ouvert entre des acteurs du secteur privé, des représentants d'organismes de réglementation et des délégués qui ont fait part de leurs points de vue et approches au sujet de la cybersécurité. Les participants issus du secteur privé ont tous souligné l'importance, pour les autorités de réglementation, de promouvoir l'interopérabilité, l'ouverture aux consultations avec les parties prenantes et la tenue de discussions techniques lors de l'élaboration des normes et réglementations en matière de cybersécurité. Les participants ont également exprimé leur soutien en faveur des mesures et des approches pratiques proposées par les organismes de réglementation représentés au sein du groupe d'experts.

4.2. La question a été posée au groupe d'experts de savoir si la solidité des normes de cybersécurité dépendait du pays d'origine des producteurs ou des fournisseurs des produits numériques. En réponse, plusieurs intervenants ont évoqué des normes internationales existantes qui finiraient par ne plus établir de distinction entre les pays.

4.3. Une discussion plus vaste s'est également tenue sur la participation des parties prenantes extérieures, y compris les entreprises, à la collaboration actuellement menée aux niveaux national et régional en matière de cybersécurité. Compte tenu du grand nombre de textes législatifs et de mesures présentés pendant les exposés, il a été demandé aux Membres de l'OMC concernés de notifier officiellement toutes les réglementations, normes et procédures d'évaluation de la conformité nouvelles et proposées, comme l'exigeait l'Accord OTC.

5 OBSERVATIONS DU MODÉRATEUR

5.1. Cette séance, au cours de laquelle 12 intervenants ont apporté des contributions, a été très enrichissante. Les principaux éléments à retenir de cette séance thématique sur la coopération entre les Membres dans le domaine de la réglementation de la cybersécurité sont les suivants:

- Les Membres ont de plus en plus recours à des mesures réglementaires dans le cadre de leurs efforts visant à traiter la cybersécurité. Certains intervenants ont mis en garde contre le fait que ces réglementations avaient parfois l'effet inverse et pouvaient compromettre les efforts mondiaux en matière de cybersécurité lorsqu'elles étaient adoptées de manière unilatérale ou au niveau national. Les intervenants ont également exprimé des préoccupations quant aux possibles obstacles au commerce découlant des mesures nationales relatives à la cybersécurité. À cet égard, plusieurs intervenants ont souligné la nécessité de parvenir à une compréhension commune des risques existants et futurs en matière de cybersécurité, ce qui permettrait également de traiter les problèmes associés de manière plus efficace.

- Comme nous l'avons vu aujourd'hui, les efforts visant à élaborer des normes internationales ambitieuses, équitables et inclusives dans le domaine de la cybersécurité sont en bonne voie. Tous les intervenants se sont accordés sur le fait que les normes internationales sont essentielles afin de contrer les menaces en matière de cybersécurité. Nombre d'entre eux (si ce n'est tous) ont évoqué des initiatives internationales, y compris les travaux menés par des organismes de normalisation comme la CEI et l'ISO.

- La plupart des intervenants (que ce soit les représentants de l'industrie ou ceux des pouvoirs publics) ont souligné la nécessité, pour les autorités publiques et le secteur privé, de travailler de manière plus coordonnée et plus collaborative avec les organismes de réglementation. Ce point est essentiel pour remédier à la fragmentation et aux divergences croissantes en matière de réglementation et traiter les préoccupations relatives à la cybersécurité et la question de la gouvernance numérique. Cette collaboration est également importante pour lutter contre les actes de cybercriminalité et les cyberincidents qui se multiplient. Dans le même ordre d'idées, les intervenants ont indiqué que les organismes de réglementation devraient faire participer les parties prenantes à

l'élaboration et à l'adoption des mesures de cybersécurité. Cela concerne les différentes branches de production et les consommateurs de ces marchés.

- Les pays développés et pays en développement Membres ont échangé des données d'expérience sur la conception, l'adoption et la mise en œuvre de mesures réglementaires et de normes relatives à la cybersécurité visant à protéger leurs citoyens. Les organismes internationaux de normalisation ont également présenté leur approche écosystémique de l'élaboration des normes relatives à la cybersécurité, qui met l'accent sur des normes horizontales traitant de la sécurité de l'information et des opérations ainsi que sur des normes verticales sectorielles.

- Du côté du secteur privé, des exemples nous ont été donnés par des entreprises exerçant dans le domaine de la lutte contre diverses menaces en matière de cybersécurité. Nous avons également eu un aperçu des problèmes liés à la réglementation de la cybersécurité couramment rencontrés par les PME, comme le risque d'être évincé d'un marché en raison de prix trop élevés lorsque les réglementations deviennent trop strictes et fragmentées.

5.2. Dans l'ensemble, les discussions ont été riches et instructives. Le modérateur souhaitait remercier les intervenants pour leurs contributions qui donnaient matière à réflexion. Il a dit espérer que le Comité OTC continuerait également de faire fond sur ces discussions thématiques sur la coopération dans le domaine de la réglementation de la cybersécurité.