Réponse de la France au projet de rapport de la Présidence de l'OEWG

Alors que la communauté internationale fait face à une crise sanitaire majeure, le caractère critique des infrastructures de santé, l'importance des technologies de l'information pour maintenir du lien social et poursuivre certaines activités économiques essentielles apparaissent sous une lumière nouvelle. Le constat de notre dépendance à ces outils souligne également toute l'actualité et l'importance des débats menés à l'OEWG afin de protéger nos sociétés.

La France salue le travail de synthèse et de mise en cohérence réalisé par la présidence et les équipes qui l'appuient. La France souhaite faire valoir les considérations ci-après en vue d'établir la deuxième version du projet de rapport.

I. Éléments généraux

La France salue l'économie générale du rapport et l'équilibre dans la présentation des différentes positions. Comme cela est actuellement le cas dans le pré-rapport, il semble particulièrement important d'inscrire le rapport de l'OEWG dans la lignée des travaux précédemment menés et agréés à l'ONU, notamment des résultats des **cinq précédents GGE et de réaffirmer la complémentarité de l'OEWG et du GGE en cours. La France estime nécessaire que la reconnaissance des acquis issus des travaux précédents figure au rapport**.

La France souhaite qu'une plus grande place soit faite à une valorisation de l'ambition finale des travaux menés à l'ONU et notamment à l'OEWG **: le maintien de la paix et de la sécurité internationale et la prévention des conflits**. Ces éléments mériteraient d'apparaître de manière plus claire et plus systématique dès l'introduction et dans l'ensemble du texte, y compris l'engagement des États à vivre en paix les uns avec les autres dans un esprit de bon voisinage, comme les y engage la Charte des Nations Unies.

De même, les éléments figurants dans le paragraphe 10, qui visent à souligner la manière dont la question des technologies de l'information est liée et influe sur les axes du travail des Nations Unies – paix et sécurité, droit de l'homme et développement durable - pourraient intervenir plus tôt dans le texte.

Enfin, le rapport **pourrait de manière plus explicite préciser le lien entre l'évaluation de la menace, le droit international, les normes, le renforcement capacitaire et les mesures de confiance.** Chaque partie du rapport, prise individuellement, ne devrait pas permettre des écarts d'interprétation concernant les engagements des États ou la valeur des principes agréés. La valeur des normes est appréhendée à travers le texte de différentes manières, ce qui mériterait d'être harmonisé, notamment pour réaffirmer que les normes agréées au sein des Nations Unies, particulièrement lors du GGE de 2015, ont une valeur d'engagement des États et non uniquement de lignes directrices *(« guidelines »).*

II. Menaces potentielles et existantes

Plusieurs points retiennent notre attention au sein de la section « Menaces potentielles et existantes ».

Concernant le paragraphe 15, la France souhaite nuancer le pré-rapport sur la question de la militarisation du cyberespace. L'acquisition et le développement de capacités cybernétiques contribuent à garantir la souveraineté des États et ne sauraient contrevenir à l'utilisation pacifique du cyberespace dès lors que leur usage est conditionné par le respect du droit international, en particulier de la Charte des Nations Unies. Par ailleurs, les interférences dans les processus politiques internes et les opérations de désinformation évoquées dans ce même paragraphe, bien que n'étant pas directement liées au mandat du groupe, sont une menace particulièrement préoccupante. Si le sujet devait être néanmoins évoqué dans le rapport, il pourrait être fait référence aux formats pertinents pour le traitement de ces questions, afin de valoriser et d'encourager les travaux actuellement menés sur ces sujets aux Nations Unies. Il conviendrait également de ne pas considérer toute campagne d'influence et de désinformation menée par un État à l'encontre d'un autre comme une atteinte au principe de non-intervention, celui-ci reposant sur deux conditions cumulatives : une atteinte au domaine réservé de l'État victime et l'usage de moyens de contrainte.

Dans le paragraphe 18, le caractère neutre par nature des technologies, souligné en séance, est bien mentionné dans le rapport. Il semble essentiel que cela soit maintenu dans le rapport final. Cela pourrait éventuellement être évoqué dès l'introduction.

Dans le paragraphe 19, les éléments portant sur l'importance et la nature spécifique des menaces visant les infrastructures critiques régionales ou transnationales sont particulièrement pertinents et pourraient faire l'objet de développements supplémentaires dans la mesure où ces infrastructures présentent des défis particuliers. **Une part plus grande pourrait être accordée à des secteurs d'activités d'importance vitale tels que la santé, le secteur financier, le transport ou les infrastructures électorales. Une attention particulière pourrait notamment être portée aux infrastructures de santé, dont la pandémie en cours souligne, une fois encore, le caractère central pour nos sociétés.**

III. Droit international

La France souhaite réaffirmer la pleine applicabilité du droit international, notamment de la Charte des Nations Unies ainsi que du droit international humanitaire au cyberespace. Alors que l'applicabilité du droit international a été affirmée dans les rapports de 2013 et 2015 adoptés par voie de consensus par l'Assemblée générale des Nations Unies, il conviendrait de s'interroger en priorité sur les modalités d'application de ce droit au cyberespace.

La France n'estime pas à ce stade nécessaire la création d'un outil juridiquement contraignant. Bien qu'il n'existe pas de normes de droit international spécifiquement dédiées au cyberespace, une interprétation évolutive du droit international existant, notamment en

prenant en compte les effets des activités menées dans le cyberespace sur les États, permet déjà d'assurer le respect du droit international.

La France continue à promouvoir la transparence sur les doctrines et se félicite que le pré-rapport encourage la poursuite des échanges en la matière. Chaque État devrait faire preuve de transparence dans son interprétation de l'application du droit international dans le cyberespace en temps de paix ou plus spécifiquement en contexte de conflit armé, notamment pour ce qui est de l'application du droit international humanitaire. **Affirmer l'applicabilité du droit international humanitaire et interpréter ses dispositions à la lumière des évolutions techniques en contexte de conflit armé ne revient pas à légitimer l'usage de la force, celui-ci étant strictement encadré par la Charte, mais à garantir que les populations et les biens civils sont protégés contre les effets d'opérations cyber qui seraient mises en œuvre par les parties en présence dans un conflit armé déjà en cours.** La transparence permet en revanche d'accroître la prédictibilité des comportements dans le cyberespace.

Par ailleurs, la France estime que les principes issus du droit international sont trop peu évoqués dans cette section du document alors qu'ils ont été mentionnés en filigrane lors des discussions. Il est souhaitable qu'ils soient réaffirmés. Des développements pourraient être apportés, notamment sur **le principe de diligence requise (*due diligence)***. La France considère comme essentiel de parvenir à une compréhension partagée, au niveau international, des obligations qui pèsent sur un État dont les infrastructures seraient utilisées à des fins malveillantes, contre les intérêts d'un autre État. En vertu du principe de *diligence requise*, un État a l'obligation de ne pas permettre que son territoire soit utilisé sciemment pour commettre des faits internationalement illicites à l'encontre d'un État tiers à l'aide de moyens cybernétiques. Cette obligation s'applique notamment à l'égard des activités menées dans le cyberespace par des acteurs non-étatiques se trouvant sur le territoire ou sous la juridiction de cet État. Il conviendrait également de rappeler que **les États ne doivent pas utiliser d'intermédiaires non-étatiques** (proxies) pour commettre des violations du droit international. Une meilleure compréhension de l'application de ces principes aux enjeux de cybersécurité permettrait de renforcer la coopération entre les États et de contribuer à éviter les conflits, en vue de protéger certaines infrastructures critiques, mais aussi pour faire cesser des cyberattaques majeures qui transiteraient *via* un État tiers. **Enfin, le droit international des droits de l'homme n'est considéré qu'à travers la simple mention de son applicabilité,** alors que les questions de la protection des données personnelles et de l'usage du cyberespace comme espace de manifestation de libertés fondamentales sont, à l'heure actuelle, primordiales.

La question de la création d'un cadre politiquement contraignant, envisagée au paragraphe 29, pourrait être accompagnée d'éléments permettant d'expliciter ce que pourrait être une telle initiative, notamment si un programme d'action (PoA – Programme of Action) est envisagé.

Au paragraphe 32, les éléments sur une possible coopération technique en vue d'attribuer des attaques informatiques ne semblent pas pertinents à ce stade. La France considère que

l'attribution est une compétence et une prérogative souveraines. **Il appartient aux États de coopérer entre eux s'ils le souhaitent sur ces questions, sur une base *ad hoc*.**

IV. Normes et principes de comportement responsable pour les États

Dans les éléments « chapeau » de la section « Normes et principes », la notion d' « *additional specific guidance* » utilisée pour décrire les normes semble d'une portée inférieure au niveau d'engagement qui peut être attendu des États. Il conviendrait *a minima* de souligner que les normes permettent d'établir une distinction claire entre les comportements acceptables et ceux qui ne le sont pas. Comme indiqué dans les commentaires généraux, la manière dont est appréhendée la valeur des normes devrait être harmonisée à travers l'ensemble du document.

Le pré-rapport fait référence à plusieurs textes au paragraphe 36 dont les statuts diffèrent, afin d'évoquer la genèse des normes. **Il conviendrait de ne pas mettre sur le même plan des éléments agréés et universalisés et des éléments présentés à la communauté internationale, mais qui n'ont pas fait l'objet d'un accord.**

Plusieurs normes proposées dans le non-papier associé au rapport ont retenu notre attention. La France note la réticence de certains États à adopter de nouvelles normes quand les éléments déjà agréés ne sont pas parfaitement mis en œuvre par tous. **Dans un esprit de consensus, les propositions retenues *in fine* pourraient être celles permettant d'expliciter les normes déjà agréées à la manière de principes ou de recommandations.** Par ailleurs, la France note une inflation de propositions dont la portée, le statut et l'articulation sont parfois difficilement compréhensibles. Le groupe, s'il souhaite intégrer ces éléments, devra travailler à formuler des propositions réalistes en termes de contenu et de portée.

Il est noté au paragraphe 40 que différents acteurs ont une responsabilité en matière de sécurité dans le cyberespace. **Il conviendrait d'appeler les États à prendre les mesures nécessaires de sensibilisation, de coopération et éventuellement, là où cela est nécessaire, de régulation, pour que les différents acteurs - publics, privés et de la société civile - prennent leurs responsabilités.**

La France réaffirme son attachement à la proposition formulée conjointement avec la Croatie, la Finlande et la Slovénie. Les États devraient être encouragés à prendre les mesures destinées à empêcher les acteurs non étatiques, y compris le secteur privé, de conduire des opérations TIC pour leurs propres objectifs ou ceux d'autres acteurs non étatiques au détriment de tiers, notamment quand ceux-ci sont situés sur le territoire d'un autre État. Cet objectif peut être atteint en travaillant avec le secteur privé pour définir les actions autorisées en employant une méthode fondée sur l'analyse des risques, et pour développer des outils concrets – certifications, guide de bonnes pratiques, mécanismes de réponse en cas d'incident et, quand cela est approprié, par la réglementation nationale.

La France soutient également les propositions formulées par les Pays-Bas qui sont cohérentes avec les principes définis par l'Appel de Paris pour la paix et la sécurité dans le cyberespace.

V. Mesures de confiance

Un important travail a été mené au sein de l'OEWG cette année au sujet des mesures de confiance. Ces échanges nous semblent reflétés dans les propositions actuelles, notamment pour rendre compte de l'importance des organisations régionales. Au sein de l'OSCE, les États participent sur une base volontaire à la mise en œuvre des mesures de renforcement de la confiance. S'engager dans ce travail et collaborer est aussi, en soi, une mesure de confiance. **L'élaboration de mesures de confiance est essentielle pour créer des conditions de dialogue apaisé entre les États, prévenir les conflits et limiter l'escalade en cas de crise**.

Plutôt qu'un répertoire recensant les mesures de confiance existantes et mises en œuvre au niveau régional, l'OEWG gagnerait sans doute à travailler avec les instances régionales afin de définir des lignes directrices permettant de rendre efficaces de tels dispositifs. Par exemple, il semble pertinent d'organiser des exercices au niveau opérationnel, comme cité dans le projet de rapport, mais également au niveau stratégique afin de permettre un partage de l'information optimal et d'assurer le lien avec le niveau politique.

VI. Renforcement des capacités

Comme le souligne le rapport, le renforcement capacitaire doit être un élément majeur des réflexions internationales en matière de sécurité et de stabilité du cyberespace. À travers des programmes de renforcement capacitaire, nous pouvons espérer un accroissement de la résilience mondiale.

Il est nécessaire de favoriser des programmes qui, au-delà des opérations de sensibilisation, constituent des offres de long terme et permettent de favoriser le développement de systèmes nationaux résilients et de développer les ressources humaines associées. Un renforcement capacitaire efficace devra s'appuyer sur des programmes créés conjointement avec les récipiendaires. Les programmes de renforcement capacitaire doivent également être développés à l'intention du secteur privé qui opère une part non négligeable des infrastructures critiques. Un travail sur les instances de gouvernance nationale peut également permettre de contribuer à des modèles nationaux plus efficaces et plus performants. Ces points devraient figurer au rapport.

Il existe un réel manque de ressources ainsi que des difficultés à réconcilier les besoins et les offres. La bonne coordination et l'utilisation optimale des ressources constituent une difficulté majeure du renforcement capacitaire. **Il serait utile que le rapport fasse plus explicitement référence aux institutions susceptibles, hors ONU, de jouer ce rôle au niveau international.**

VII. Dialogue institutionnel régulier

La possibilité de « mécanismes dédiés » ou de mise en place de différents formats, notamment une agence intergouvernementale, est évoquée dans la section « Dialogue institutionnel

régulier ». **De nombreux États se sont exprimés pour faire valoir que le fond devrait guider la forme si un format spécifique était créé – ce qui n'a pas, à ce stade, été démontré. La France est favorable à ce que le texte reflète mieux cette préoccupation.**

La nature du dialogue multi-acteurs reflète bien les discussions menées lors des deux premières sessions. En effet, même si les décisions au sein d'un groupe de travail issu de la première commission des Nations Unies ont vocation à être intergouvernementales, les échanges avec les différentes parties prenantes demeurent capitaux. Tout au long du processus, le groupe aurait sans doute bénéficié d'un nombre accru d'échanges sous différents formats, y compris avec des acteurs qui n'ont pas traditionnellement la possibilité de s'exprimer au sein des Nations Unies. La France soutient le maintien de ces éléments dans le rapport final.

VIII. Conclusions et recommandations

La France remercie la présidence et ses équipes pour les éléments de recommandations qui visent à trouver un compromis entre les positions et propositions des États participants.

Cependant, la France note que les recommandations comportent un nombre important de travaux de synthèse et de recensement. Il convient de s'interroger sur le coût, l'utilité et la pérennité de ces travaux. Certains sont, par ailleurs, réalisés par d'autres institutions, parfois au niveau régional ou déjà proposés par l'ONU, notamment via l'UNIDIR. **Il serait sans doute utile de définir quelques priorités, et de recommander un travail sur celles-ci.** Cela permettrait de créer, au-delà d'une cartographie, un document ou une ressource de référence qui pourrait être maintenu à jour dans le temps. Parmi les propositions figurant dans le rapport et comme précisé lors des deux premières sessions de l'OEWG, **la France considère que la priorité choisie devrait être un travail de la communauté internationale portant sur la manière dont les normes sont mises en œuvre,** afin d'affiner la compréhension collective des normes déjà agréées et de permettre la définition de lignes directrices et d'échanges de bonnes pratiques. Ce point fait par ailleurs l'objet d'une proposition spécifique portée par l'Australie, le Mexique, la France, le Canada, le Chili, l'Indonésie, l'Afrique du Sud, l'Organisation des Îles du Pacifique et la Nouvelle-Zélande.

Par ailleurs, le mécanisme proposé en matière de coordination du renforcement capacitaire reflète un besoin réel. Néanmoins, il mériterait de faire l'objet de plus amples discussions, notamment pour aborder le rôle de l'ONU en la matière et la manière dont elle pourrait collaborer avec d'autres structures, traditionnellement spécialisées sur ce sujet.