MISSION PERMANENTE DU NIGER
AUPRES DES NATIONS UNIES
417 EAST 50TH STREET, NEW YORK, NY 10022
Tél : (212)421-3260/61/86 Fax : (212)753-6931
E-mail : nigermission@ymail.com

Onzième Session de fonds sur le Groupe de travail à composition non limitée sur la sécurité et l'utilisation des technologies de l'information et de la communication (2021-2025)

New York, du 07 au 11 juillet 2025

Explication de position pour le « Recueil des déclarations sur le rapport final du Groupe de travail à composition non limitée sur la sécurité et l'utilisation des technologies de l'information et de la communication (2021-2025) »

Par Monsieur Tila Boulama Mamadou Ari Koutale, Premier Secrétaire à la Mission Permanente du Niger auprès des Nations Unies.

1. Tout d'abord j'adresse mes félicitations au Président du Groupe de travail, avec son équipe, pour leur professionnalisme et leur disponibilité qui ont

d'emblée rendu possible la réussite du processus jusqu'à l'adoption du rapport final.

2. Sur l'application du droit international dans le cyberespace, il est clair que le rapport réaffirme à juste titre l'applicabilité du droit international, en particulier de la Charte des Nations Unies, au cyberespace notamment aux paragraphes 39-43.
3. Nous saluons entièrement cette position consensuelle qui vise à garantir à notre avis, le développement des discussions, des normes et des règles sures et claires pour la stabilité et la prévisibilité des interactions entre États dans ce domaine. Cependant, nous proposons des clarifications supplémentaires sur quelques concepts clefs, notamment sur :

-La diligence raisonnable : Bien que mentionnée au paragraphe 40, une définition opérationnelle et assez développée de ce concept dans le contexte cybernétique renforcerait sa mise en œuvre pratique.

-Le droit international humanitaire (DIH) : Au paragraphe 40 (b) (ii), le rapport note son applicabilité en cas de conflit armé mais nous proposons une analyse plus approfondie des principes de distinction et de proportionnalité appliqués aux cyberopérations pour permettre aux États de connaître les implications pratiques.

-La Responsabilité des États : Le mécanisme d'attribution des cyberattaques et les voies de recours pour les États victimes mériteraient des lignes directrices plus concrètes, avec des cas pratiques clairs pour mettre en lumière le mécanisme d'attribution.

4. Sur le futur mécanisme permanent, nous proposons l'élaboration d'un guide pratique sur l'application du droit international, incluant des études de cas et des avis d'experts neutres, avec l'approbation des États membres.
5. Sur le renforcement des capacité, le rapport souligne la pertinence et l'importance du renforcement des capacités comme pilier transversal. Les propositions telles que le portail mondial (GSCCP) et le fonds volontaire

sont des avancées considérables. Nous proposons plus encore, une approche inclusive dans le programme de parrainage des délégués et la bourse pour les femmes, qui doivent être élargis pour couvrir davantage de pays en développement. Par ailleurs, on pourra instituer une évaluation des besoins dans le catalogue proposé, qui devrait intégrer un mécanisme de feedback des États bénéficiaires pour éviter les doublons.

6. Le futur mécanisme devrait adopter un plan quinquennal de renforcement des capacités, avec des indicateurs de succès mesurables et un budget dédié pour une question d'efficacité.
7. Sur l'annuaire des points de contact nationaux, nous saluons amplement cette initiative, qui doit au moins caque année, être révisé et mis à jour. Son opérationnalisation nécessite a notre avis, des exercices et des simulations pratiques réguliers au moins chaque deux années.
8. Sur la participation du secteur privé dans le processus, il faut souligner le rôle des entreprises dans la sécurité des chaînes d'approvisionnement, qui devrait s'accompagner de cadres incitatifs et des facilitations afin d'accompagner leur action.