Union Africaine

POSITION AFRICAINE COMMUNE

SUR L'APPLICATION DU DROIT INTERNATIONAL A L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION DANS LE CYBERESPACE

I. PREAMBULE

1. Rappelant l'Acte constitutif de l'Union africaine adopté en 2002, en particulier ses articles 3 et 4 et la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo) adoptée en 2014.

2. Notant que les technologies de l'information et de la communication (TIC) dans le cyberespace sont un élément indispensable dans la vie des êtres humains du monde entier et, qu'elles sont un instrument d'interaction humaine, un vecteur de développement social ainsi qu'un moteur de croissance économique, d'éradication de la pauvreté et de développement durable.

3. Notant en outre qu'il est dans l'intérêt de tous les États, sociétés et générations présentes et futures, d'élaborer une architecture juridique mondiale qui garantisse que les TIC sont utilisées à des fins pacifiques, qui empêche l'utilisation malveillante et criminelle de ces technologies, qui favorise une plus grande coopération entre les États, qui garantisse que le cyberespace reste ouvert, sûr, stable, accessible et pacifique, qui protège les droits humains et les libertés fondamentales des individus et des peuples, et qui promeut les intérêts communs de l'humanité.

4. Réaffirmant que le droit international s'applique au cyberespace et régit l'utilisation des TIC dans le cyberespace. Il est toutefois nécessaire, compte tenu des caractéristiques techniques uniques du cyberespace et de la nature particulière des menaces que représentent les comportements illégaux dans ce domaine, par des États et acteurs non étatiques, d'élargir davantage le dialogue entre les États et les organisations régionales et d'autres acteurs concernés, le cas échéant et dans le cadre de leurs rôles et responsabilités respectifs, par le biais de processus transparents, inclusifs et multilatéraux sur la manière dont le droit international devrait se développer davantage dans ce domaine.

5. Soulignant l'engagement, conformément à leurs obligations en vertu du droit international et conformément à la diligence raisonnable, de lutter contre les cyber opérations malveillantes et criminelles menées par des acteurs non étatiques et souligne que les acteurs non étatiques, en particulier les acteurs non étatiques dont les agissements sont attribuables aux États, devraient s'abstenir de se livrer à toute utilisation malveillante et/ou criminelle des TIC dans le cyberespace.

6. Soulignant que le processus visant à clarifier davantage la manière dont le droit international s'applique à l'utilisation des TIC dans le cyberespace et, le cas échéant, à développer davantage les règles du droit international qui sont applicables dans ce domaine est une question d'intérêt commun pour tous les États. Tous les États ont un droit égal de participer à l'élaboration de règles de droit international applicables au cyberespace et les opinions de tous les États ont le même poids et la même valeur dans ce processus.

7. Notant que le processus d'articulation des règles de droit international applicables à l'utilisation des TIC dans le cyberespace bénéficiera de l'adoption d'une déclaration des Nations Unies sur ce sujet, qui serait négociée avec la participation d'autres parties prenantes, le cas échéant dans le cadre de leur rôles et responsabilités respectifs, y compris d'autres organisations internationales et régionales.

8. Prenant note des réunions en cours du Comité spécial des Nations Unies chargé d'élaborer une convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. L'Union africaine encourage ses États membres qui ne l'ont pas encore fait à envisager de signer et de ratifier la Convention de l'UA sur la cyber sécurité et la protection des données à caractère personnel (Convention de Malabo).

9. Saluant les efforts entrepris par les Nations Unies pour aborder les questions relatives à la cyber sécurité, en particulier le Sommet mondial sur la société de l'information organisé en Afrique par un État membre de l'Union africaine, la Tunisie, et rappelant, à cet égard, l'engagement de Tunis et le plan d'action de Tunis figurant dans le document de l'ONU A/60/687.

10. Soulignant que cette position africaine commune a été adoptée dans l'esprit de contribuer aux débats mondiaux sur l'application du droit international au cyberespace. À cet égard, étant donné le développement continu et rapide de la technologie dans ce domaine, cette position africaine commune devrait être considérée comme une contribution non exhaustive aux discussions en cours dans ce domaine. Les positions exprimées dans le présent document pourraient évoluer à la lumière des progrès technologiques et de la poursuite des discussions avec la communauté internationale. Les États membres de l'Union africaine sont également encouragés à publier des déclarations nationales sur l'application du droit international à l'utilisation des technologies de l'information et de la communication dans le cyberespace. En outre, certains aspects des règles de droit international qui s'appliquent dans le cyberespace ne sont pas abordés dans la présente déclaration, comme les immunités des missions diplomatiques et des organisations internationales, l'inviolabilité des communications officielles de l'État et des correspondances diplomatiques, la légalité des contre-mesures et les restrictions à l'invocation de la nécessité comme circonstance empêchant l'illégalité, sur lesquelles l'Union africaine se réserve sa position .

11. Réaffirmant que l'adoption de la présente Position africaine commune confirme l'engagement exprimé par l'UA dans la Stratégie de transformation numérique de l'Afrique, qui vise à exploiter les technologies numériques et l'innovation pour transformer les sociétés et les économies africaines afin de promouvoir l'intégration de l'Afrique, de générer une croissance économique inclusive, de stimuler la création d'emplois, de réduire la fracture numérique et d'éradiquer la pauvreté pour le développement socio-économique du continent, et d'assurer l'appropriation par l'Afrique d'outils modernes de gestion numérique.

II. <u>LA SOUVERAINETE DANS LE CYBERESPACE</u>

12. La souveraineté est un attribut des États. À ce titre, les États jouissent de l'indépendance en vertu du droit international ainsi que de la suprématie personnelle et territoriale dans leurs affaires intérieures et extérieures, en addition d'être obligés de ne pas porter atteinte à l'indépendance d'autres États ou de ne pas violer leur souveraineté territoriale ou personnelle, en plus d'être obligés de respecter les droits humains fondamentaux et les libertés fondamentales des individus qui se trouvent sur leurs territoires ou qui relèvent de leur juridiction.

13. La souveraineté territoriale est un corollaire de la souveraineté de l'État. En vertu de cette souveraineté, les États ont le droit, dans les limites établies par les règles applicables du droit international, d'exercer un contrôle exclusif sur leur territoire terrestre et ses dépendances, y compris l'espace aérien et les zones maritimes qui sont soumis à la souveraineté de l'État. L'obligation de respecter la souveraineté territoriale des États est une règle primaire solidement établie en droit international, qui s'applique au comportement des États dans le cyberespace. [Cette règle se reflète dans plusieurs décisions judiciaires, notamment l'arrêt de la Cour internationale de Justice dans *l'Affaire du Détroit de Corfou*, qui affirme qu'*« entre États indépendants, le respect de la souveraineté territoriale est un fondement essentiel des relations internationales »* et] l'arrêt de la Cour internationale de Justice dans l'*Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci*, qui affirmait que *« [l]e concept juridique fondamental de souveraineté de l'État dans le droit international coutumier, exprimé, entre autres, dans le paragraphe de l'article 2 1, de la Charte des Nations Unies, s'étend aux eaux intérieures et à la mer territoriale de chaque État ainsi qu'à l'espace aérien au-dessus de son territoire. »*

14. En vertu de la souveraineté territoriale, les États ont le droit d'exercer une juridiction, y compris un pouvoir législatif, juridictionnel et d'exécution, sur les composantes du cyberespace situées sur leur territoire. Cette juridiction des États s'applique également de manière extraterritoriale aux TIC situées à bord d'aéronefs et de navires battant le pavillon de l'État et autres engins spatiaux dans l'espace extra-atmosphérique enregistrés par l'État.

15. L'Union africaine affirme que le droit international, tel qu'il s'applique à l'utilisation des TIC dans le cyberespace, ne permet pas à un État d'exercer des pouvoirs d'exécution sur le territoire d'un État étranger en réponse à des cyber activités illégales émanant du territoire de cet État étranger. Cette règle s'applique même si l'exercice de ce pouvoir d'exécution par un État n'a pas d'effets préjudiciables, virtuels ou physiques, sur le territoire d'un État étranger.

16. L'Union africaine affirme qu'en vertu de la souveraineté territoriale, tout accès non autorisé d'un État dans l'infrastructure des TIC située sur le territoire d'un État étranger est illégale. Par conséquent, l'UA souligne que l'obligation de respecter la souveraineté territoriale des États, telle qu'elle s'applique dans le cyberespace, ne comporte pas de seuil minimal d'effets dommageables en deçà duquel l'intrusion d'un État dans l'infrastructure des TIC située le territoire d'un État étranger ne serait pas illicite. L'Union africaine affirme en outre que les cyber opérations imputables à un État contre une infrastructure TIC située sur le territoire d'un État étranger et qui provoquent des effets, tels qu'une perte ou une altération de fonctionnalité, sur le territoire d'un État tiers, peuvent constituer une violation de la souveraineté territoriale de ce dernier.

17. L'UA souligne que la codification des règles de droit international s'appliquant au cyberespace et visant à permettre aux États d'exercer des pouvoirs d'exécution sur le territoire d'un État étranger ou établissant un seuil de préjudice qui réduit la portée protectrice de la règle de l'inviolabilité de la souveraineté territoriale des États, présente des risques importants d'un point de vue politique. Compte tenu des grandes disparités de capacités techniques entre les États, de telles règles seraient, comme l'a noté la Cour internationale de justice (CIJ) dans l'*affaire du détroit de Corfou*, « par la nature des choses, réservées aux États les plus puissants », ce qui pourrait donner lieu à de graves abus susceptibles de porter atteinte aux principes de l'indépendance et de l'égalité souveraine des États.

18. Corollaire de la souveraineté territoriale, les États doivent protéger, conformément aux règles applicables du droit international, notamment du droit international des droits de l'homme et, le cas échéant, du droit international humanitaire, les personnes physiques et morales se trouvant sur leur territoire contre les utilisations illégales des TIC dans le cyberespace qui sont imputables à des États étrangers ou à des acteurs privés.

19. L'obligation de respecter la souveraineté territoriale des États est une règle qui s'applique dans les relations interétatiques, par conséquent uniquement un fait international illicite imputable à un État conformément aux règles applicables du droit international, comme indiqué dans la section 9 de la présente, pourrait constituer une violation de la souveraineté territoriale d'un État.

III. LA DILIGENCE RAISONNABLE DANS LE CYBERESPACE

20. La diligence raisonnable joue un rôle important dans le domaine du cyberespace. Compte tenu des difficultés techniques liées à l'attribution de responsabilité pour les actes internationalement illicites commis au moyen des TIC dans le cyberespace et le fait que de tels actes sont souvent commis par des acteurs non étatiques, la diligence raisonnable prévoit un outil important pour promouvoir l'ouverture, l'accessibilité, la sûreté et la sécurité du cyberespace.

21. Les États membres de l'UA reconnaissent que la diligence raisonnable est une obligation qui opère dans le contexte d'autres règles primaires du droit international. En cet égard, L'UA affirme qu'en vertu de la souveraineté territoriale, tout État a l'obligation, comme l'a déclaré la Cour internationale de justice (CIJ) dans l'affaire du détroit de Corfou, « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres Etats ». Ce principe qui est un corollaire de la souveraineté est aussi confirmé par des précédents judiciaires, notamment dans l'affaire de l'usine de pâte à papier et la décision arbitrale de l'Ile de Palmas.

22. L'UA considère que la diligence raisonnable établit une obligation de comportement, et non une obligation de résultat. Par conséquent, la diligence raisonnable n'exige pas d'un État qu'il garantisse que son territoire ou le territoire sous son contrôle ou sa juridiction n'est pas utilisé pour commettre un fait internationalement illicite. Elle établit plutôt l'obligation de prendre des mesures nécessaires, réalisables dans la mesure des capacités de l'État et des ressources disponibles, pour prévenir ou faire cesser un fait internationalement illicite dont l'État sait ou aurait dû savoir qu'il est commis à l'aide des TIC sur son territoire ou le territoire sous son contrôle ou sa juridiction.

23. L'obligation de diligence raisonnable consistant à prendre des mesures, dans les limites des capacités disponibles de l'État, pour prévenir ou faire cesser un fait internationalement illicite n'est déclenchée que si un État a connaissance du fait qu'un tel acte provient ou transite par des TIC situées sur son territoire ou le territoire sous son contrôle ou sa juridiction. Cette connaissance n'est toutefois pas présumée du seul fait de la souveraineté territoriale ou du contrôle. En effet, dans l'affaire du détroit de Corfou, la CIJ a déclaré qu'« on ne saurait conclure du seul contrôle exercé par un État sur son territoire terrestre ou sur ses eaux territoriales que cet État a nécessairement connu ou dû connaître tout fait illicite international qui y a été perpétré non plus qu'il a nécessairement connu ou dû connaitre ses auteurs ». La question de savoir si un État a connaissance d'un fait internationalement illicite provenant ou transitant par les TIC situées sur son territoire ou le territoire sous son contrôle ou sa juridiction doit donc être déterminée au cas par cas, au vu des informations dont dispose l'État et de ses capacités techniques et institutionnelles ainsi que des ressources financières qui lui sont disponibles.

24. La diligence raisonnable renforce également l'obligation des États de ne pas permettre à un autre État [ou aux acteurs non étatiques] d'utiliser des TIC situées sur son territoire ou sous sa juridiction ou son contrôle pour commettre des actes internationalement illicites à l'encontre d'un autre État.

25. L'Union africaine reconnaît également les défis uniques auxquels sont confrontés les pays en développement dans la mise en œuvre des mesures de diligence raisonnable en raison des contraintes de ressources et des défis liés à l'expertise technique]. Les États membres de l'Union africaine soulignent l'importance de la coopération internationale et du partage d'informations, notamment par le biais des équipes d'intervention en cas d'urgence informatique (CERT)/équipes de réponse aux incidents de sécurité informatique (CSIRT), pour permettre aux États de respecter pleinement leur obligation de diligence raisonnable. À cet égard, l'Union africaine souligne l'importance d'accroître la coopération internationale et le renforcement des capacités, et permettant aux pays en développement de participer pleinement aux forums d'élaboration des politiques relatifs à la gouvernance du cyberespace.

IV. INTERDICTION D'INTERVENIR DANS LES AFFAIRES INTÉRIEURES ET EXTÉRIEURES DES ÉTATS DANS LE CYBERESPACE

26. L'interdiction d'intervenir dans les affaires intérieures et extérieures des États est un principe général de droit international qui est aussi reflété dans plusieurs traités multilatéraux, notamment

dans les instruments fondateurs des organisations régionales, tels que l'Acte constitutif de l'Union africaine, la Charte de l'Organisation des États américains, la Charte de l'Organisation de la coopération islamique et la Charte de l'Association des nations de l'Asie du Sud-Est, ainsi que dans d'autres instruments, tels que l'Acte final d'Helsinki de 1975, et dans les résolutions de l'Assemblée générale des Nations Unies, telles que la Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États, adoptée en 1970.

27. L'interdiction d'intervention est une règle qui s'applique aux relations interétatiques. En conséquence, seul un fait qui est imputable à un État conformément aux règles applicables du droit international pourrait constituer une violation de l'interdiction d'intervention.

28. L'interdiction d'intervention protège contre les actes qui empiètent sur des questions relevant de la compétence nationale des États sur lesquelles chaque État est autorisé, en vertu du principe de souveraineté de l'État, à décider librement. Il est également établi qu'en vertu de leur souveraineté, les États ont le droit inaliénable de choisir leurs systèmes politiques, économiques, sociaux et culturels, sans l'intervention d'aucun autre État.

29. L'interdiction d'intervention s'applique à l'utilisation de tout instrument, tels que les moyens armés, politiques, économiques ou tout autre moyen, y compris l'instrument d'information, qui peut être utilisé par un État dans le but d'intervenir dans les affaires intérieures ou extérieures d'un État étranger. L'interdiction d'intervenir est particulièrement pertinente dans le contexte du cyberespace, vu la connectivité croissante entre les États et les sociétés, qui offre à des acteurs malveillants, y compris des acteurs étatiques et non étatiques dons les actes sont attribuables aux États, des possibilités accrues d'utiliser les TIC à des fins d'intervention dans les affaires intérieures et extérieures des États. Diverses codifications de l'interdiction d'intervention ont également affirmé que cette règle proscrit à la fois l'intervention directe par des organes de droit et de fait d'un État et l'intervention indirecte par des personnes ou des groupes agissant sous la direction, l'instruction ou le contrôle d'un État. Cette règle interdit également l'organisation, le financement ou la fourniture de toute forme d'assistance aux acteurs non étatiques engagés dans des actes d'intervention contre un autre État.

30. Pour constituer une violation de l'interdiction d'intervention, ces instruments doivent être utilisés d'une manière qui équivaut à la coercition, que la CIJ a décrite, dans l'*affaire relative aux activités militaires et paramilitaires au Nicaragua et contre celui-ci*, comme l'élément *« constitutif de l'intervention prohibée et formant son essence même »*.

31. UA est de d'avis que la coercition, dans le contexte de l'interdiction de l'intervention, devrait être définie comme une politique visant à imposer des contraintes à la volonté d'un État étranger. Comme pour la prohibition de la menace ou de l'usage de la force, qui est examinée ci-dessous, déterminer si l'utilisation par un ou plusieurs États des TIC dans le cyberespace pour influencer le comportement d'un État étranger équivaut à de la coercition est une décision qui doit être prise au cas par cas.

32. Bien que la définition de la coercition dans ce contexte doive faire l'objet d'une étude et de délibérations plus approfondies entre les États, les États membres de l'UA n'acceptent pas l'opinion selon laquelle, pour constituer une coercition, le comportement d'un État doit aller jusqu'à priver un État étranger de sa liberté de choix ou forcer cet État à agir ou à s'abstenir d'agir de manière involontaire. Cette conception de la coercition, que plusieurs États ont adoptée, impose un seuil de coercition excessivement élevé qui réduit inutilement la portée de la prohibition d'intervenir. En outre, rien n'exige que, pour constituer une violation de l'interdiction d'intervenir, un acte de coercition parvienne effectivement à contraindre l'État soumis à de tels actes à modifier son comportement. Une tentative d'intervention infructueuse est illégale au regard du droit international.

Les États membres de l'UA soulignent que les offres ou les appels au règlement pacifique des différends à travers la négociation, les enquêtes, la médiation, la conciliation, l'arbitrage, et le règlement judiciaire, les bons offices et les discussions et communications diplomatiques sont présumés ne pas constituer des actes de coercition.

33. L'UA rappelle qu'en vertu de leur souveraineté territoriale, tous les États sont tenus de faire preuve de la diligence raisonnable pour empêcher que leur territoire soit utilisé par d'autres États ou des acteurs non étatiques pour s'engager dans des actes qui constituent une violation de la prohibition de l'intervention dans les affaires internes et externes des États.

V. LE REGLEMENT PACIFIQUE DES DIFFERENDS DANS LE CYBERESPACE

34. L'obligation d'utiliser des moyens pacifiques pour résoudre les différends internationaux est une règle de droit international coutumier, qui est aussi codifié dans les traités internationaux et régionaux, incluant la Charte des Nations Unies, et les instruments juridiques fondateurs des organisations régionales tel que l'Acte constitutif de l'Union africaine.

35. Les États membres de l'UA rappellent l'article 4(e) sur le règlement pacifique des différends et 4(f) sur l'interdiction du recours à la force, ou la menace d'utiliser la force de l'Acte constitutif de l'Union africaine, et réaffirme, que, conformément à aux articles 2(3) et 33 de la Charte des Nations Unies, l'obligation de régler pacifiquement les différends internationaux s'applique à tout différend pouvant survenir entre États relatif à des actes, omissions , ou désaccord su un point de droit ou de fait, liés à l'utilisation des TIC dans le cyberespace, ou qui a trait à l'application ou à l'interprétation du droit international dans ce domaine. Cette obligation n'est pas seulement limitée aux différends dont la continuation serait susceptible de compromettre le maintien de la paix et la sécurité internationales.

36. Conformément à la Charte des Nations Unies, les États ont l'obligation de régler leurs différends internationaux par des moyens pacifiques tels que la négociation, les enquêtes, la médiation, la conciliation, les bons offices, l'arbitrage, le règlement judiciaire, les recours aux organismes ou accords régionaux ou par d'autres moyens pacifiques de leur choix.

37. L'Union africaine reconnait le potentiel des TIC pour améliorer le règlement pacifique des différends et encouragent leur utilisation dans le contexte du règlement des différends. L'UA soutient aussi le développement d'outils et de plateformes basés sur les TIC pour le règlement pacifique des différends, tels que les plateformes de médiation en ligne et les logiciels de règlement des différends, exhorte les États à investir dans la recherche et le développement des TIC pour le règlement pacifique des différends dans le cyberespace.

VI. INTERDICTION DE LA MENACE OU DE L'USAGE DE LA FORCE DANS LE CYBERESPACE

38. L'interdiction de la menace ou du recours à la force est une règle de jus cogens[1] reconnue comme une norme fondamentale et cardinale du droit international général qui est également un élément essentiel de la Charte des Nations Unies. Cette règle est également codifiée dans divers traités et instruments fondateurs des organisations régionales, comme l'Acte constitutif de l'Union

[1] Le Royaume du Maroc a émis une réserve concernant la référence au concept de « jus cogens ». Le Royaume du Maroc est d'avis que dans le cadre du développement progressif du droit international, l'interdiction du recours à la force pourrait éventuellement être qualifiée de norme impérative par les organes compétents des Nations Unies chargés de la codification et du développement progressif du droit international.

africaine, et dans des accords bilatéraux. Il s'agit de règles de droit international qui s'appliquent dans le cyberespace et qui régissent la conduite des États en ce qui concerne les TIC dans le cyberespace.

39. L'interdiction du recours à la force n'admet que deux exceptions : le recours à la force en cas d'attaque armée et le recours à la force autorisé par le Conseil de sécurité des Nations Unies en vertu du chapitre VII de la Charte des Nations Unies. L'Union africaine affirme que l'interdiction de la menace ou de l'usage de la force s'applique au recours à la force armée par les États. L'Union africaine est d'avis que les cyberopérations relèveraient de l'interdiction du recours à la force lorsque l'ampleur et les effets de l'opération sont comparables à ceux d'un acte de violence conventionnel couvert par l'interdiction. En particulier, une cyberopération, selon son ampleur et son effet, équivaudrait à un recours à la force si elle est censée causer des dommages, des blessures ou la mort, ce qui est comparable à un recours à la force par un acte conventionnel visé par l'interdiction.

40. Par exemple, une cyber opération qui détruit, inflige des dommages, ou désactive de manière permanente des infrastructures critiques au sein d'un État peut être considérée comme équivalant à un recours à la force en vertu du droit international. De même, une cyber opération visant un actif militaire en détruisant, endommageant ou désactivant un système de défense antimissile pourrait constituer une violation de l'interdiction du recours à la force. Il convient de déterminer au cas par cas.

41. L'UA souligne qu'il faut faire une distinction entre les formes les plus graves de recours à la force qui constituent une attaque armée qui autorisent l'État lésé à invoquer le droit à la légitime défense individuelle ou collective conformément à l'article 51 de la Charte des Nations Unies et les formes moins graves de recours à la force. La question de savoir si un cas particulier de recours à la force équivaut à une attaque armée doit être déterminée au cas par cas. Cette détermination devrait être entreprise sur la base d'une évaluation de l'ampleur et des effets du cas particulier de recours à la force. En général, le critère de l'échelle nécessite un examen d'éléments tels que la durée de l'attaque, la nature des cibles attaquées, les lieux où elles se trouvent et les types d'armes utilisées, tandis que le critère des effets mesure l'étendue des dommages causés par l'attaque.

42. L'UA prend note des points de vue selon lesquels les États ont le droit de se défendre contre des menaces imminentes de recours à la force. Il s'agit là d'une question controversée sur laquelle il n'existe que peu de précédents judiciaires et qui ne fait pas l'unanimité parmi les éminents publicistes. Les États membres de l'UA estiment que cette question doit faire l'objet d'une étude et de délibérations plus approfondies entre les États, en tenant compte à la fois des caractéristiques uniques du cyberespace et des cyber opérations et des implications que toute règle pouvant émerger en relation avec cette question pourrait avoir pour l'intégrité des interdictions de la menace ou de l'usage de la force. À cet égard, les États membres de l'UA soulignent que, d'un point de vue juridique, la Charte des Nations Unies autorise les États à recourir à la force en cas de légitime défense individuelle ou collective en cas « d'agression armée » contre un État. En outre, les États membres de l'UA soulignent que, d'un point de vue politique, le maintien de la paix et de la sécurité internationales favorise le maintien d'une interprétation restrictive des exceptions à l'interdiction du recours à la force.

43. L'interdiction de la menace ou du recours à la force s'adresse aux États dans leurs relations internationales. Par conséquent, cette règle et ses exceptions ne s'appliquent pas au comportement d'acteurs non étatiques qui n'est pas imputable à des États. En conséquence, les États membres de l'UA affirment que le droit de légitime défense n'est déclenché que si une attaque armée est attribuable à un État conformément aux règles applicables du droit international coutumier en matière de responsabilité des États.

44. L'Union africaine note que l'armement et la formation des acteurs non étatiques pourraient constituer une violation de l'interdiction de menacer ou d'utiliser la force. Cela s'applique à la fourniture d'une assistance technique ou d'une formation aux acteurs non étatiques qui se livrent à des actes équivalant à la menace ou à l'utilisation de la force par les TIC contre un autre État

45. Dans ce contexte, les États membres de l'UA réaffirment qu'en vertu de leur souveraineté territoriale, tous les États sont tenus de faire preuve de diligence raisonnable tel que reflété en Section III pour veiller à ce que leur territoire ne soit pas intentionnellement utilisé pour violer les droits d'autres États par des actes qui constituent une menace ou l'usage de la force, que de tels actes aient été entrepris par des organes de l'État ou par des acteurs non étatiques agissant sous la direction, le contrôle ou les instructions de l'État.

46. Un comportement qui ne constitue pas une violation de l'interdiction de la menace ou du recours à la force peut, selon les circonstances, constituer une violation d'autres règles du droit international, notamment de l'obligation de respecter la souveraineté territoriale des États et de l'interdiction d'intervention dans les affaires intérieures ou extérieures des États.

VII. LE DROIT INTERNATIONAL HUMANITAIRE DANS LE CYBERESPACE

47. Les États membres de l'UA affirment que le droit international humanitaire (DIH) s'applique au cyberespace. Bien que la plupart des règles du DIH soient apparues avant l'apparition du cyberespace, le DIH s'applique, parallèlement à toute autre règle du droit international, aux cyber opérations susceptibles d'être entreprises dans le cadre d'un conflit armé. Comme cela a été relevé par la CIJ, dans son avis consultatif sur la Licéité de la menace ou de l'emploi d'armes nucléaires en vertu de *sa « nature intrinsèquement humanitaire »*, le DIH s'applique à *« à toutes les formes de guerre et à toutes les armes, celles du passé, comme celles du présent et de l'avenir »*.

48. Afin de déclencher l'application du DIH, une situation doit constituer un conflit armé. Le DIH reconnaît deux catégories de conflits armés : les conflits armés internationaux, dans lesquels les parties sont des États engagés dans des hostilités avec la force armée, et les conflits armés non internationaux, dans lesquels les parties sont des forces armées d'un État engagées dans des hostilités contre des groupes armés organisés ou une situation dans laquelle des groupes armés sont engagés dans des hostilités entre eux sur le territoire d'un État.

49. Dans un conflit armé international, le DIH s'applique dès qu'il y a recours à la force armée entre des États, quelle que soit l'intensité de ces activités. L'application du DIH à un conflit armé international n'est affectée ni par l'absence d'une déclaration formelle de guerre ni par l'évaluation de la légalité, en vertu des règles applicables de la Charte des Nations Unies, du recours à la force par les États belligérants. En revanche, les États membres de l'Union africaine sont conscients de la possibilité que les cyber opérations, en elles-mêmes, puissent déclencher un conflit armé non international. L'application du DIH commence dans un conflit armé non international lorsque l'intensité du conflit équivaut à une violence armée prolongée, ce qui signifie qu'elle dépasse le niveau de violence relatif aux troubles internes, tels que les émeutes, la violence isolée et sporadique, et dans les situations où les groupes armés engagés dans les hostilités atteignent un certain degré d'organisation.

50. Les États membres de l'UA réaffirment leur attachement aux principes cardinaux du DIH qui régissent tous les moyens et les méthodes de guerre et réaffirment que ces principes s'appliquent à la fois à l'utilisation des TIC dans le cyberespace et à la protection des TIC civiles pendant les conflits armés. En particulier, les États membres de l'UA rappellent le principe selon lequel *« Le droit des belligérants d'adopter des moyens de blesser l'ennemi n'est pas illimité »* et le principe selon lequel les

belligérants ont l'obligation de limiter les souffrances, les blessures et les destructions causées par un conflit armé.

51. Sur la base de ces principes généraux, les États membres de l'UA soulignent l'importance du principe de distinction, qui interdit les attaques dirigées contre des civils ou des biens de caractère civil, y compris les TIC, que ces attaques soient menées utilisant des moyens cinétiques ou cybernétiques. L'UA souligne également l'importance du principe de proportionnalité, qui interdit les attaques dont on peut attendre qu'elles causent incidemment des dommages aux civils qui seraient excessifs par rapport à ce qui est nécessaire pour obtenir un avantage militaire précis.

52. L'UA souligne que certains objets et biens civils, toute infrastructure TIC qui leur est associée, sont additionnellement protèges spécifiquement sous les règles relatives du DIH. Ces objets qui sont indispensables à la survie de la population civile, et parmi lesquels figurent par exemple les hôpitaux, le personnel et les installations médicales ainsi que les opérations de secours humanitaire, qui doivent être respectées et protégées et ne doivent pas être attaqués, détruits, enlevés ou rendus inutiles.

VIII. LE DROIT INTERNATIONAL DES DROITS DE L'HOMME DANS LE CYBERESPACE

53. Les États membres de l'UA affirment que le droit international des droits de l'homme (DIDH), qu'il soit codifié dans des conventions universelles ou régionales auxquelles les États sont parties ou qu'il soit consacré par le droit international coutumier, s'applique au cyberespace. Ainsi donc, les États ont l'obligation de respecter, de protéger et d'assurer les droits humains des personnes et des peuples se trouvant sur leur territoire ou relevant de leur juridiction qui sont liés à l'utilisation des TIC dans le cyberespace, notamment en protégeant ces droits individuels et collectifs contre les atteintes portées par des tiers et des acteurs non étatiques.

54. L'UA affirme encore que le DIDH exige des États qu'ils protègent la liberté d'expression en ligne, y compris le droit de rechercher, de recevoir et de transmettre des informations et des idées et de diffuser des opinions par le biais des TIC. Toute restriction imposée par les États à ces droits doit être prévue par la loi et se limiter à ce qui est strictement nécessaire dans une société démocratique pour respecter et protéger les droits ou la réputation d'autrui et pour protéger la sécurité nationale, l'ordre public, la santé publique ou les mœurs. Les États membres de l'UA réaffirment également que les États ont l'obligation de veiller à ce que les TIC ne soient pas utilisées à des fins d'incitation à la violence, au terrorisme ou à la discrimination pour quelque motif que ce soit, notamment la race, l'ethnie, la couleur, le sexe, la langue, la religion, l'opinion politique ou toute autre opinion, l'origine nationale et sociale, la fortune, la naissance ou tout autre statut. À cet égard, l'Union africaine rappelle que des égards particuliers devraient être accordés aux personnes en situation de vulnérabilité.

55. L'UA estime qu'un comportement responsable en matière d'utilisation des TIC dans le cyberespace exige des États qu'ils veillent à ce que leur conduite ne porte pas atteinte aux droits humains des individus et des peuples dans d'autres États. En particulier, certaines activités entreprises par les États, telles que l'interception transnationale des communications constituent une violation du droit à la vie privée des personnes qui en font l'objet, en plus d'une violation de la souveraineté territoriale des États sur le territoire desquels une telle interception a lieu. Les États membres de l'UA sont également préoccupés par l'absence de protection adéquate du droit à la vie privée au niveau international, ce qui accroît le risque d'utilisation abusive des données privées par des acteurs malveillants ou leur détournement à des fins lucratives par des acteurs privés.

56. L'UA affirme que les États doivent protéger les individus et les peuples dans leurs territoires ou les zones sous leurs juridictions contre les violations des droits humains individuels et collectifs sur leur territoire ou dans les zones sous leur juridiction qui sont commises par des tiers, y compris les

entreprises qui opèrent dans le secteur des TIC. En outre, les entreprises commerciales qui opèrent dans le secteur des TIC ont la responsabilité de respecter et de protéger les droits humains, en particulier le droit à la vie privée et la liberté d'expression, notamment en faisant preuve de diligence raisonnable pour identifier, prévenir, atténuer et rendre compte de tout impact négatif de leurs activités sur les droits humains.

57. L'UA souligne l'importance de maintenir le cyberespace ouvert, sûr, stable, accessible et pacifique ; cela constituant un élément important pour promouvoir la croissance économique, attirer des opportunités d'investissement et faire progresser le développement durable, en particulier dans les États en développement et les États les moins avancés. À cet égard, les États membres de l'UA relèvent que le droit au développement est un droit établi par la Convention internationale des droits de l'homme qui exige des États qu'ils coopèrent de bonne foi y compris comme indiqué dans la section X sur le renforcement des capacités et la coopération internationale, pour soutenir les pays en développement dans les efforts qu'ils déploient pour développer leurs capacités scientifiques et technologiques, y compris dans le domaine des TIC, afin d'accélérer la réalisation des droits économiques, sociaux et culturels des peuples de ces pays.

58. L'UA souligne l'importance de combler le fossé numérique à assurer la pleine jouissance des droits de l'homme. À cet égard, les États contribuent à renforcer l'autonomisation des femmes et des filles. Les États encouragent également les personnes handicapées à profiter pleinement des avantages des TICs ce qui contribuerait à la conception, le développement et la production des TIC comprenant des technologies d'assistance et d'adaptation accessibles aux personnes handicapées.

59. L'Union africaine appelle au développement et à la gestion responsable des systèmes d'identité numérique d'une manière qui respecte les droits humains de tous les individus.

60. Les États membres de l'UA encouragent les États à envisager la conclusion d'accords d'assistance mutuelle dans le domaine de la lutte contre la cybercriminalité, ce qui contribuerait davantage à la protection et à la pleine réalisation des droits humains individuels.

IX. LES REGLES RELATIVES A L'ATTRIBUTION D'UN COMPORTEMENT A UN ETAT DANS LE CYBERESPACE

61. Sous réserve de l'émergence de règles spécifiques d'attribution, l'Union africaine affirme que les règles coutumières sur la responsabilité des États, Comme le reflètent les projets d'articles de la CIT sur la responsabilité des États pour les actes internationalement illicites, les règles applicables pour l'attribution aux États de la conduite entreprise par les TIC dans le cyberespace.

62. L'Union africaine est d'avis que, conformément aux règles pertinentes du droit international, c'est à l'État qui fait une telle affirmation qu'il incombe de prouver qu'un État a commis un acte illicite au plan international au moyen des TIC dans le cyberespace. L'Union africaine souligne également l'importance de la coopération, y compris entre les autorités nationales, telles que les équipes d'intervention en cas d'urgence informatique (CERT)/les équipes d'intervention en cas d'incident de sécurité informatique (CSIRT), pour détecter, enquêter, prévenir et mettre fin aux actes répréhensibles internationaux commis au moyen des TIC dans le cyberespace.

63. Les États membres de l'UA soulignent que les réponses aux actes internationalement illicites commis par le biais des TIC dans le cyberespace devraient être conformes aux obligations qui leur incombent en vertu de la Charte des Nations Unies, en particulier les obligations relatives au règlement pacifique des différends, ainsi qu'aux autres règles applicables du droit international.

X. RENFORCEMENT DES CAPACITES ET COOPERATION INTERNATIONALE DANS LE DOMAINE DES TIC ET DU CYBERESPACE

64. L'Union africaine souligne l'importance de la coopération internationale pour faire face aux défis mondiaux de notre époque, notamment dans le domaine du cyberespace. L'Union africaine rappelle également que dans un monde numériquement interdépendant, la coopération internationale, notamment par l'assistance en matière d'expertise technique et de renforcement des capacités, est essentielle pour réduire la fracture numérique et garantir que le cyberespace soit ouvert, sécurisé, stable, accessible et pacifique.

65. L'Union africaine souligne l'importance de la coopération avec les États partenaires, les organisations internationales et le secteur privé en développant les capacités institutionnelles régionales et nationales à travers le renforcement des capacités, l'assistance technique et l'échange d'expertise technique dans le domaine du cyberespace afin d'identifier et remédier aux fractures et inégalités numériques, et améliorer la coordination entre les autorités techniques, politiques, juridiques et réglementaires aux niveaux national et international.

66. L'Union africaine souligne l'importance de renforcer les efforts de renforcement des capacités visant à permettre aux États d'identifier, de protéger et de sauvegarder collectivement les infrastructures nationales critiques, y compris les infrastructures d'information critiques, et de sauvegarder en coopération les infrastructures d'information critiques. L'Union africaine affirme également qu'une attention particulière est nécessaire pour soutenir les capacités des États en développement, tant au niveau politique que technique, dans des domaines tels que le développement de stratégies nationales de cybersécurité et de résilience, l'accès aux technologies pertinentes et le soutien à la réponse aux urgences informatiques. Équipes (CERT)/Équipes de réponse aux incidents de sécurité informatique (CSIRT). L'Union africaine réaffirme qu'une attention particulière est nécessaire pour renforcer la coopération internationale afin de clarifier et de développer davantage les règles du droit international applicables au cyberespace, de manière à intégrer pleinement la dimension du développement dans l'élaboration future de ces règles.

67. L'Union africaine réaffirme que le renforcement des capacités et l'assistance technique doivent respecter la souveraineté des États et doivent également être fondés sur la confiance mutuelle et la reconnaissance de l'appropriation nationale. L'Union africaine souligne que le renforcement des capacités et toute coopération dans ce domaine doivent respecter l'intégrité et la sécurité de l'infrastructure nationale des TIC, correspondre aux besoins et priorités identifiés au niveau national, et respecter et protéger la confidentialité des politiques et plans nationaux.

XI. CONCLUSION

68. Les points de vue exprimés dans la présente position commune africaine sont une articulation non exhaustive des points de vue l'Union africaine concernant certaines des questions importantes relatives à l'application du droit international dans le cyberespace. Ces points de vue sont sans préjudice de l'application éventuelle d'autres règles de droit international relatives à la gouvernance du cyberespace, en particulier de tout instrument régional ou international applicable relatif à la lutte contre la cybercriminalité. Les États membres de l'Union africaine et les États membres de l'Union africaine, agissant individuellement ou collectivement, peuvent développer ces opinions, à la lumière des développements technologiques et des discussions en cours sur ces questions.

69. L'Union africaine reste déterminée à participer de manière positive et constructive aux débats internationaux, inclusifs et multilatéraux sur ces questions, en vue de garantir que le cyberespace reste ouvert, sûr, pacifique, sûr, stable et accessible, et que les TIC continuent de servir de véhicule pour promouvoir l'intégration régionale en Afrique et défendre les intérêts communs de l'humanité.