**Appels à contributions : rapport sur la fourniture de produits et services militaires et de sécurité dans le cyberespace par les cyber-mercenaires et son impact sur les droits humains**

|  |  |
| --- | --- |
| **Echéance:** | 12 février 2021 |
| **Issu par:** | Groupe de travail sur l’utilisation des mercenaires |
| **Objectif:** | Informer le rapport du Groupe de travail qui sera présenté à la 76ème session de l’Assemblée générale en octobre 2021 |

**Contexte**

Deux fois par an, le Groupe de travail sur l’utilisation des mercenaires sollicite des contributions pour informer l’élaboration de ses études thématiques qui seront présentées au Conseil des droits de l’homme à sa session de septembre et à l'Assemblée générale en octobre.

**Objectifs du rapport**

Le Groupe de travail sur l’utilisation des mercenaires a identifié les « cyber mercenaires » comme une catégorie d’acteurs susceptibles de générer des activités liées aux mercenariat. Cela implique une large gamme de services militaires et de sécurité fournis dans le cyberespace, y compris la collecte de données et l’espionnage. Il arrive que des acteurs privés soient engagés par des États ou par des acteurs non étatiques pour mener des opérations offensives ou défensives, pour protéger les réseaux et l’infrastructure de ces instances, ainsi que pour mener des cyberopérations visant à affaiblir les capacités et moyens militaires des forces armées ennemies, ou à porter atteinte à l’intégrité du territoire d’un autre État. Les individus qui commettent des cyberattaques peuvent causer des dommages à distance, dans diverses juridictions. Partant, ils peuvent être considérés comme exerçant une activité liée au mercenariat, voire une activité de mercenaire en propre si tous les critères requis pour ce faire sont remplis.

Cette étude sur les *la fourniture de produits et services militaires et de sécurité dans le cyberespace par les cyber-mercenaires et d’autres acteurs concernés, et son impact sur les droits humains* vise à évaluer comment les mercenaires et les acteurs privés tirent profit du développement, du maintien et de l’exploitation des cyber-capacités, qui peuvent être utilisés dans la conduite des hostilités et dans des contextes non conflictuels pour violer les droits humains, y compris le droit des peuples à disposer d’eux-mêmes.

**Portée de l'étude et questions clés**

Le Groupe de travail accueille favorablement les contributions d'États, d’organisations de la société civile, d'universitaires, d’organisations internationales et intergouvernementales, d’institutions nationales des droits de l’homme, d'entreprises privées, de particuliers et de tout autre acteur concerné.

Bien que le Groupe de travail accueille favorablement toute information jugée pertinente à la question, il s’intéresse particulièrement aux domaines mentionnés ci-dessous. Tout en répondant aux questions suivantes, veuillez fournir, dans la mesure du possible, des **exemples, des bonnes pratiques et des recommandations** que vous jugez importantes dans le contexte de ce questionnaire, ainsi que toute analyse sur les développements futurs dans ce domaine

Tendances et développements actuels

1. Qui sont les clients et/ou bénéficiaires des cyber-capacités et opérations ?

*Par exemple, cela peut inclure des acteurs étatiques et non étatiques qui engagent des « cyber-mercenaires » et d’autres acteurs opérant seuls ou à travers des entreprises militaires et de sécurité privées (EMSP) pour acquérir des cyber-capacités, y compris des services et produits militaires et de sécurité.*

1. Quel est le rôle des acteurs opérant seuls ou à travers des EMPS, dans a) le développement, b) le maintien, c) la vente, d) la fourniture de cybercapacités (y compris des produits ou services militaires ou de sécurité) à des tiers, ou e) mener du cyber espionnage ?
2. Quelles sont les facteurs de motivation et les intentions stratégiques : a) des clients qui recrutent des « cyber-mercenaires » ainsi que le type de relation qu’ils peuvent entretenir avec eux ; et b) des « cyber-mercenaires » et d’autres acteurs opérant seuls ou à travers des EMPS dans le cyberespace ?

*Les facteurs de motivation peuvent inclure, par exemple, un gain privé, une compensation matérielle, des raisons idéologiques et autres.*

1. Quels types de services et produits sont-ils disponibles dans le cyberespace (par exemple, les logiciels espions ou malveillants, l’intelligence artificielle), et quel est leur objectif tant dans les situations de conflit que de non-conflit ?
2. Quel est le rôle des nouvelles technologies pour causer des dommages à distance dans le contexte des cyberopérations, et quels sont les risques encourus ? Comment définiriez-vous « participer directement aux cyberopérations » ?

Cadres réglementaires et leur mise en œuvre

1. Veuillez fournir des informations sur les cadres législatifs, politiques et réglementaires nationaux, régionaux ou internationaux existants, ou d’autres initiatives, concernant la conduite dans le cyberespace et leur mise en œuvre (par exemple, transparence, comportement responsable, prévention des comportements interdits).
2. Veuillez fournir des informations sur les normes et/ou réglementations spécifiques nationales ou régionales régissant la fourniture de produits et services de sécurité dans le cyberespace par des acteurs opérant seuls ou à travers des EMPS et d’autres acteurs concernés.
3. Veuillez fournir des informations sur les cadres et mécanismes nationaux, régionaux ou internationaux visant à enquêter, et tenir les individus, groupes, États ou entreprises responsables des abus dans le cyberespace, y compris pour l’espionnage, les cyberopérations, les produits et les services illégaux, ainsi que leur efficacité.

Impacts sur les droits humains et le DIH des cyber-capacités et opérations offensives menée par des acteurs opérant seuls ou à travers des EMPS

1. Veuillez décrire comment le développement et l'utilisation des cybercapacités, des opérations et des services (par exemple, les attaques contre les infrastructures et les données numériques/physiques, la surveillance d'individus) par des acteurs opérant seuls ou à travers des EMPS peuvent provoquer et contribuer à des abus et violations des droits humains dans des contextes hors conflits.

*Cela inclut par exemple le droit à la vie, à l’intégrité physique et mentale, à la vie privée, à la santé, au vote, au droit des peuples à disposer d’eux-mêmes, ainsi que la liberté de mouvement, de réunion et d’association, qui pourraient affecter des individus ou des groupes, tels que des défenseurs des droits humains, des leaders de l’opposition ou des journalistes*.

1. Veuillez décrire comment le développement et l’utilisation de cybercapacités, d’opérations et de services dans le cyberespace par des acteurs opérant seuls ou à travers des EMPS peuvent provoquer et contribuer à des violations du droit international humanitaire dans le cadre de conflits armés.

**Comment et où soumettre les contributions**

Les contributions peuvent être envoyées par courrier électronique dans un format accessible (document Word) à [mercenaries@ohchr.org](mailto:mercenaries@ohchr.org). Les contributions doivent être reçues avant le **12 février 2021 à 18h00 CEST**.

Lorsque vous soumettez votre réponse, veuillez indiquer si vous avez des objections concernant la publication de votre réponse sur ce site.

**Comment les réponses seront utilisées**

Toutes les soumissions reçues en format accessible Word seront publiées sur cette page Web, à moins que l’auteur n’indique clairement qu'elle/il ne souhaite pas que ses commentaires soient rendus publics lors de la soumission de sa réponse.

Les soumissions reçues en format PDF ne seront pas publiées, mais seront disponibles sur demande.