Nations Unies A/76/151

# Assemblée générale

Distr. générale
15 juillet 2021
Français
Original : anglais

**Soixante-seizième session**
Point 74 de l'ordre du jour provisoire*
**Droit des peuples à l'autodétermination**

## Utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes

### Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre à l'Assemblée générale, conformément à la résolution 75/171 de l'Assemblée et à la résolution 42/9 du Conseil des droits de l'homme, le rapport du Groupe de travail sur l'utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes.

* A/76/150.

21-09837X (F)

# Rapport du Groupe de travail sur l'utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes

## Les incidences sur les droits humains des cyberactivités des mercenaires, des acteurs apparentés et des entreprises de services de sécurité et de défense

*Résumé*

Dans le présent rapport, le Groupe de travail sur l'utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes examine la fourniture de services et de produits militaires et de sécurité dans le cyberespace par les mercenaires, les acteurs apparentés et les entreprises de services de sécurité et de défense ainsi que son incidence sur les droits humains.

Ces services militaires et de sécurité fournis dans le cyberespace peuvent prendre des formes très diverses : de la collecte de données à l'espionnage, en passant par le renseignement. Il arrive que les États ou les acteurs non étatiques engagent des acteurs privés, grâce à divers intermédiaires, pour mener des opérations offensives ou défensives et pour protéger leurs réseaux et leur infrastructure, ainsi que pour lancer des cyberopérations afin d'affaiblir les capacités et les moyens militaires des forces armées ennemies, ou pour compromettre l'intégrité territoriale d'autres États. Les personnes qui commettent ces cyberattaques peuvent provoquer des dégâts à distance dans plusieurs juridictions. C'est pourquoi elles peuvent être considérées comme exerçant une activité liée au mercenariat, voire une véritable activité de mercenaire, si elles remplissent tous les critères requis.

La présente étude thématique examine les formes et les manifestations des activités de ces acteurs, qui développent, gèrent et utilisent des cybercapacités pouvant servir à lancer des hostilités dans des situations conflictuelles ou non. Elle analyse les incidences possibles de ces activités sur les droits humains, y compris le droit des peuples à l'autodétermination, et se penche sur la question de la réglementation de la fourniture des services et des produits militaires et de sécurité dans le cyberespace.

Aux fins de l'établissement du présent rapport, le Groupe de travail était composé de Jelena Aparac (Présidente), Lilian Bobea, Ravindran Daniel, Chris Kwaja et Sorcha MacLeod.

# Table des matières

# I. Introduction et contexte

1. Le présent rapport est présenté à l'Assemblée générale par le Groupe de travail sur l'utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes, conformément à la résolution 75/171 de l'Assemblée et à la résolution 42/9 du Conseil des droits de l'homme.

2. Dans le cadre de son mandat, le Groupe de travail surveille, dans différentes régions du monde, les mercenaires et les activités liées au mercenariat, quelles qu'en soient les formes et les manifestations, ainsi que les entreprises de services de sécurité et de défense. En outre, il étudie leurs activités et les conséquences qu'elles peuvent avoir pour les droits humains, en particulier le droit à l'autodétermination.

3. Le présent rapport s'appuie sur des recherches documentaires approfondies ainsi que sur les informations communiquées par les parties prenantes en réponse à un appel à contributions lancé, en janvier 2021, par le Groupe de travail [1]. Le 7 décembre 2020, le Groupe de travail a organisé une consultation virtuelle d'experts sur les mercenaires et les acteurs apparentés dans le contexte de la cybersécurité et des nouvelles technologies afin d'intégrer ses conclusions au présent rapport. Le Groupe de travail souhaite remercier tous ceux qui ont pris part à la préparation du présent rapport en y apportant leur contribution et en participant à la consultation d'experts.

4. Les activités des mercenaires ont, pendant des années, été abordées sous l'angle des opérations militaires traditionnelles auxquelles prennent part les mercenaires pour le compte d'États ou d'autres clients. Plus récemment, les mercenaires, les acteurs apparentés et les entreprises de services de sécurité et de défense ont commencé à mener des activités dans le cyberespace. Dans son rapport intitulé « Mercenaires et activités liées au mercenariat : évolution des formes, des tendances et des manifestations » (voir A/75/259), le Groupe de travail désigne les « cybermercenaires » comme une catégorie d'acteurs susceptibles de mener des activités liées au mercenariat. De plus, les rapports annuels du Groupe de travail soulèvent régulièrement la question de l'utilisation des technologies et des transferts de connaissances en lien avec divers sujets[2]. Le présent rapport examine, quant à lui, la fourniture de services et de produits militaires et de sécurité dans le cyberespace par les mercenaires, les acteurs apparentés et les entreprises de services de sécurité et de défense ainsi que leurs incidences sur les droits humains.

5. Dans ses précédentes analyses, le Groupe de travail a montré du doigt les différents mercenaires et acteurs apparentés qui continuent d'influencer le déroulement des conflits armés contemporains, de se rendre coupables d'atteinte aux droits humains et de violer le droit à l'autodétermination, y compris au moyen de cyberactivités. Aujourd'hui, le cyberespace constitue un lieu géostratégique essentiel pour les acteurs étatiques et non étatiques, et diverses entités privées leur proposent des cybercapacités défensives et offensives pour servir leurs programmes ou leurs intérêts, ce qui a des conséquences dévastatrices sur la jouissance des droits humains et sur le droit des peuples à l'autodétermination.

6. Le Groupe de travail a notamment fait remarquer la nature de plus en plus asymétrique des conflits armés modernes ainsi que la participation croissante des acteurs privés (A/75/259). La guerre cinétique classique continue de jouer un grand rôle dans les conflits contemporains ; toutefois, l'utilisation de cyberattaques et

[1] Voir https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx.

[2] Voir A/75/259, par. 50 ; A/HRC/45/9, par. 39 et suivants ; A/HRC/42/42.

d'autres cyberactivités devient, parallèlement au développement des nouvelles technologies, de plus en plus fréquente et continue d'évoluer, même en dehors des conflits armés traditionnels. De même, les mercenaires contemporains et les autres acteurs se sont adaptés et ont commencé à mener des activités dans le cyberespace et sont devenus, dans certains cas, une composante essentielle des cyberopérations.

# II. Observations définitionnelles

7. Le terme « mercenaire » est défini à l'article 47 du Protocole additionnel I aux Conventions de Genève de 1949, dans la Convention internationale contre le recrutement, l'utilisation, le financement et l'instruction de mercenaires, et dans la Convention de l'Organisation de l'Union Africaine sur l'élimination du mercenariat en Afrique. Toutefois, la nature trop restrictive de la définition de ce terme en droit international a fait l'objet de nombreuses analyses et réflexions. Le Groupe de travail convient que la portée de cette définition pose problème et qu'il est difficile d'en trouver une qui réunit tous les critères, notamment pour ce qui est des formes contemporaines d'activités liées au mercenariat, dont celles qui sont menées dans le cyberespace par des acteurs non étatiques.

8. Par ailleurs, en l'absence de définition juridique faisant consensus au niveau international, le Groupe de travail a précédemment défini une entreprise de services de sécurité et de défense comme une société commerciale qui fournit contre rémunération des services militaires ou de sécurité par l'intermédiaire de personnes physiques ou morales[3]. Ces dernières peuvent opérer en situations conflictuelles ou en temps de paix, et sont d'importants fournisseurs de services et de produits militaires et de sécurité dans le cyberespace.

9. Même si aucune des définitions susmentionnées ne fait expressément référence aux cyberactivités ou aux acteurs opérant dans le cyberespace, il n'en reste pas moins que certaines actions menées en ligne peuvent être assimilées à du mercenariat ou considérées comme des activités apparentées à celui-ci, et qu'elles portent, de la même façon, atteinte aux droits humains, en situation de conflit armé ou en temps de paix. Ces actions peuvent prendre la forme d'opérations de cybermalveillance menées par des cyberintermédiaires, qui peuvent être de nationalités diverses et opérer de n'importe quel lieu, mener ces actions en ligne ou hors ligne, ou provoquer directement ou indirectement des dommages[4]. D'aucuns définissent ces actes de malveillance comme le recours à des actions ou opérations visant délibérément à modifier, perturber, induire en erreur, détériorer ou détruire des systèmes et réseaux informatiques, ou à compromettre de toute autre façon la confidentialité, l'intégrité et la disponibilité de ces systèmes et réseaux lors de leur utilisation par des personnes et des populations[5]. Cette définition ne tient pas compte des technologies émergentes, telles que les drones, qui ont un effet cinétique en dehors des réseaux informatiques.

10. Le Groupe de travail souhaite néanmoins souligner que les services militaires et de sécurité fournis dans le cyberespace ne sont pas systématiquement des opérations menées par des acteurs liés au mercenariat, mais qu'il faut plutôt envisager chaque cas de figure à la lumière de son contexte et de ses circonstances spécifiques (voir A/75/259, par. 54).

---

[3] Pour la définition complète, voir A/HRC/15/25, annexe, article 2.

[4] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge, 2018, p. 31.

[5] Herb Lin, « Offensive cyber operations and the use of force », *Journal of National Security Law and Policy*, vol. 4, nº 1, 13 août 2010, p. 4–63 ; et ISO/IEC 27000:2009.

11. Le Groupe de travail a admis, en 2020, que la cyberguerre permettait non seulement de s'infiltrer parmi des objectifs militaires ou civils, de les perturber, de les endommager, voire de les détruire, mais aussi de nuire gravement aux êtres humains. Le Comité international de la Croix-Rouge a conclu qu'elle doit être menée, comme c'est le cas pour la guerre conventionnelle, conformément au droit international humanitaire[6]. Cet impératif est d'autant plus pertinent que les capacités stratégiques dépendent de plus en plus des infrastructures et de la technologie (voir A/75/259, par. 42).

12. La transformation des conflits contemporains et l'évolution rapide des nouvelles formes d'opérations militaires, associées à l'absence de réglementation, de suivi et de contrôle ainsi qu'aux difficultés que présentent les enquêtes sur des infractions commises à partir d'un autre pays figurent parmi les raisons qui ont poussé le Groupe de travail à se pencher sur ce phénomène. Celui-ci s'inquiète aussi de l'accès inégal de certains pays développés et d'autres acteurs fortunés aux technologies et au savoir-faire y afférent.

13. Le Groupe de travail est conscient que les situations dans lesquelles opèrent les mercenaires ont des conséquences différentes et disproportionnées sur les femmes, les enfants et d'autres groupes (voir A/75/259, par. 5). Il observe les difficultés liées au manque de consensus international sur la définition de « cyberattaque » (ou « hostilités en ligne ») dans le droit international humanitaire, ce qui empêche actuellement de déterminer la position du concept dans ce droit ainsi que les manquements et les violations en la matière.

14. Un point qui revient souvent dans les discussions actuelles sur les conditions, présentes et futures, de réglementation de ces cyberactivités est le rôle que jouent les acteurs non étatiques dans les cyberactivités et la cyberguerre, en particulier les mercenaires, les acteurs apparentés et les entreprises de services de sécurité et de défense, mais aussi les autres entités commerciales et privées. Dans le présent rapport, le Groupe de travail s'est donc employé à passer en revue divers services militaires et de sécurité fournis dans le cyberespace et susceptibles de donner lieu à des activités liées au mercenariat. Il espère ainsi alimenter un débat sur la meilleure façon de définir ces activités et de lutter contre elles (voir A/75/259, par. 52). Des dispositions réglementaires sont certes nécessaires, mais il faut également mettre en place une coopération efficace, aux niveaux national et international, entre les parties concernées pour lutter contre ce phénomène.

# III. Services militaires et de sécurité dans le cyberespace : activités, catégories d'acteurs, et relations entre acteurs étatiques et non étatiques

15. Les services militaires et de sécurité comprennent une grande variété de services, dont la collecte de données et l'espionnage. Il arrive que les États ou les acteurs non étatiques engagent des acteurs privés, grâce à divers intermédiaires, pour mener des opérations offensives ou défensives de protection de leurs réseaux et de leur infrastructure, pour lancer des cyberopérations visant à affaiblir les capacités et les moyens militaires des forces armées ennemies, ou pour compromettre l'intégrité du territoire d'un autre État. En utilisant leur cyberpuissance de feu, tant offensive que défensive, ces acteurs participent à des tentatives ou à des actions visant à

[6] Comité international de la Croix-Rouge, « Le droit international humanitaire et les cyberopérations pendant les conflits armés », document de position du CICR, novembre 2019.

découvrir, pirater ou perturber des installations militaires ou civiles critiques en vue de les détruire.

16. Comme nous l'avons vu, il est important d'observer que les cyberservices sont également fournis aux États dans des situations n'impliquant pas de conflit armé, notamment à des fins de collecte de renseignements et de surveillance, ou pour maintenir l'ordre au niveau national et garantir la sécurité [7]. En outre, les cyberservices comprennent des services d'assistance aux États pour les cybercapacités qu'ils possèdent déjà ainsi que la fourniture de cyberproduits qui peuvent les intéresser. Il convient de noter qu'une vaste gamme de produits et de services sont proposés librement à la commercialisation sur le marché : il faut en tenir compte lorsque l'on envisage de réglementer ce type de services.

17. Parmi les nombreuses cyberactivités et méthodes de cyberopérations actuellement entreprises, on trouve le sabotage au moyen de logiciels malveillants ou rançonneurs, l'espionnage et la subversion par le recours à des informations fausses et à la désinformation. D'un point de vue pratique, ces activités peuvent consister à contraindre à l'arrêt ou à endommager certaines infrastructures essentielles comme les fournisseurs d'électricité et d'eau, les hôpitaux, les services de surveillance et les installations de communication, ou à permettre de cibler ou de neutraliser des systèmes de défense militaires ou autres.

18. Les entreprises de cybersécurité qui travaillent pour des sociétés privées et des États proposent des moyens de défense contre les cyberattaques et la cyberguerre. Les pare-feux, les correctifs et les antivirus sont, par exemple, des moyens purement défensifs, alors que les « pots de miel » et autres pièges à pirates, ainsi que le balisage pour dissuader et piéger les pirates en constituent une variante un peu plus offensive[8]. Qu'ils soient passifs ou actifs, ces moyens de défense tombent sous le coup des dispositions légales réglementant actuellement les opérations de cybersécurité.

19. Cependant, le Groupe de travail s'inquiète notamment du fait que les entreprises de cybersécurité privées et publiques ainsi que les opérateurs criminels disposent, eux aussi, de capacités offensives. Ces capacités des entreprises de cybersécurité peuvent être utilisées contre les États développés, par exemple, dans des attaques contre les infrastructures électorales, qui sont menées, suppose-t-on, par des acteurs étatiques ou par des intermédiaires travaillant pour le compte des États. Les activités de cybermalveillance consistent également à cibler des actifs virtuels et des prestataires de services liés aux actifs virtuels ainsi qu'à attaquer des entreprises du secteur de la défense, notamment pour obtenir illégalement l'accès à des technologies militaires (voir S/2021/211, annexe, par. 125-126). Rien ne permet de trouver des caractéristiques communes claires et évidentes pour les acteurs étatiques et non étatiques qui acquièrent ces technologies. Les États démocratiques comme les États autoritaires, les États qui disposent de cybercapacités nationales tout comme ceux qui en sont dépourvus, font tous l'acquisition de technologies offensives auprès de fournisseurs externes.

20. Le marché des cybercapacités offensives connaît une croissance rapide, est peu réglementé et offre la possibilité de réaliser des bénéfices importants. C'est pourquoi de nombreuses entreprises de services de sécurité et de défense conventionnelles ouvrent des divisions de cybersécurité [9]. Quel que soit leur pays d'origine, les prestataires de services de cybersécurité, comme de plus en plus d'entreprises de

[7] Voir la contribution de la fondation ICT for Peace.

[8] Contribution reçue sous scellés.

[9] W. J. Hennigan, « Defense contractors see opportunity in cybersecurity sector », *Los Angeles Times*, 21 janvier 2015. Consultable à l'adresse suivante : www.latimes.com/business/la-fi-0122-cyber-defense-20150122-story.html.

services de sécurité et de défense traditionnelles, collaborent avec les gouvernements nationaux et deviennent ainsi des extensions du pouvoir étatique, ce qui en fait, aux yeux de certains, des intermédiaires semblables à des mercenaires.

21. Il est possible d'appliquer aux services militaires et de sécurité fournis dans le cyberespace les distinctions entre services offensifs et services défensifs ainsi qu'entre transparence et ambiguïté de leur régime juridique. Les États ou les acteurs non étatiques peuvent engager des acteurs privés non seulement pour protéger leurs réseaux et leur infrastructure, mais aussi pour mener des cyberopérations conçues pour affaiblir les capacités et les moyens militaires des forces armées ennemies ou pour compromettre l'intégrité du territoire d'un autre État. La présence de mercenaires dans le cyberespace, où ils participent désormais à la production et à la vente d'armes informatiques offensives, souligne leur capacité d'adaptation[10]. Les individus qui commettent des cyberattaques peuvent être considérés comme exerçant une activité liée au mercenariat, voire une véritable activité de mercenaire, s'ils remplissent tous les critères requis (voir A/75/259, par. 71).

## A. Catégories des cyberacteurs concernés

### Cyberunités ou cybercommandements intégrés dans les forces armées officielles

22. Ces dernières années, la concurrence en matière de cyberexpertise a été exacerbée par les stratégies de cyberinfluence, qui se sont révélées désastreuses pour les relations géopolitiques contemporaines[11]. Certains États prennent part à ce qui a été décrit comme une « lutte informationnelle dans le cyberespace »[12] et intègrent des opérations de stratégie militaire d'influence dans leurs capacités militaires. L'évolution rapide des technologies numériques a profondément transformé les opérations militaires et a donné lieu à des investissements dans le développement de cyberunités ou cybercommandements intégrés aux forces armées conventionnelles. De plus, les formes classiques d'affrontement entre deux forces armées s'accompagnent maintenant d'opérations de cyberguerre, où les cyberunités mènent des activités qui peuvent être considérées comme défensives ou offensives, selon le point de vue[13]. Les cyberopérations peuvent être menées seules ou en association avec des opérations militaires traditionnelles. Cependant, le scénario le plus inquiétant reste celui qui implique des opérations de « guerre hybride ». Dans ce cas en effet, l'État répond par des cyberopérations militaires à une situation qui, selon les règles du droit international humanitaire, ne mériterait pas une réponse armée. La lutte informationnelle dans le cyberespace se complique même encore lorsque les forces armées conventionnelles sous-traitent certaines de leurs cyberactivités à un tiers.

### Acteurs n'appartenant pas aux forces armées officielles

23. Les entités non étatiques qui ne font pas partie des forces armées jouent un rôle extrêmement important et de plus en plus prépondérant dans la fourniture des

---

[10] Tom Burt, « Cyber mercenaries don't deserve immunity », site web de Microsoft, 21 décembre 2020. Consultable à l'adresse suivante : https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

[11] Voir https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf, p. 9–10.

[12] Voir https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf, p. 7–8.

[13] Neri Zilber, « The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments? », *Foreign Policy* (FP), 31 août 2018. Consultable à l'adresse suivante : https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/.

cyberservices aux États et en leur nom. Les attaques de cybersécurité menées par une nouvelle génération de sociétés privées dénommées « cybermercenaires » constituent une menace croissante en pleine évolution[14], et la démarcation entre les sphères privée et publique, dans ce domaine, est de plus en plus floue[15].

**Entités commerciales**

24. À la différence des entreprises de services de sécurité et de défense, qui disposent généralement de fonctions et de capacités privatisées dont l'État avait auparavant le monopole, les prestataires de services de cybersécurité sont apparus dans le secteur privé et s'y sont épanouis. Même quand les forces armées nationales les plus avancées ont élaboré, en interne, une expertise et des capacités en matière de cybersécurité, ces opérations militaires sophistiquées s'appuient fortement sur le secteur privé[16]. Les entreprises privées de cybersécurité comprennent des sociétés commerciales bien établies et des start up dynamiques qui ont gagné des parts dans ce marché en rapide expansion.

25. Les sociétés privées qui produisent les technologies et les logiciels qui nous intéressent dans la présente analyse peuvent être réparties en deux catégories. La première est constituée de grandes plateformes technologiques qui travaillent en collaboration avec les organismes publics pour permettre aux États d'accéder aux informations et d'exécuter des programmes de surveillance[17]. La seconde rassemble des sociétés beaucoup plus petites, en taille et en chiffre d'affaires, mais qui possèdent des capacités spécifiques pour la fabrication de produits susceptibles d'être utilisés dans des activités malveillantes. Le secteur des sociétés privées de cybersécurité est en pleine expansion et évolution. Par ailleurs, plusieurs entreprises de services de sécurité et de défense se sont tournées vers la cybersécurité, souvent grâce à l'acquisition de sociétés technologiques spécialisées qu'elles ont rattachées à leur groupe.

26. Les entreprises du secteur de la défense qui produisent habituellement des armes et des équipements militaires ont étendu leurs activités au secteur numérique. Ces entreprises d'armement ont surtout mis au point des services et des solutions de cybersécurité en interne, même si, dans certains cas, elles se sont également adjoint des sociétés de cybersécurité commerciales en tant que filiales pour renforcer leurs capacités. Le discours public de ces entreprises d'armement brouille volontairement la distinction entre, d'une part, les actions et les services conçus simplement pour renforcer la résilience du cyberespace et, d'autre part, les technologies dont les clients pourraient servir pour mener des opérations offensives, voire des activités malveillantes.

**Les menaces persistantes avancées**

27. Les menaces persistantes avancées désignent des groupes d'acteurs malhonnêtes ou criminels, qui cherchent à s'infiltrer de manière persistante dans les systèmes de cybersécurité des États ainsi que des acteurs publics et privés. Ces groupes bénéficient de moyens technologiques sophistiqués ainsi que de ressources financières et techniques importantes, ont des objectifs stratégiques à long terme et sont souvent soutenus, d'une certaine façon, par les gouvernements nationaux[18]. Ils disposent d'une capacité interne de développement d'armes offensives et peuvent mener des

[14] Voir la contribution d'Access Now, p. 1.
[15] Voir la contribution d'Ori Swed et de Daniel Burland, p. 15.
[16] Voir www.cmi.no/publications/file/6637-russian-use-of-private-military-and-security.pdf.
[17] Voir https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.
[18] Voir https://targetedthreats.net/media/1-ExecutiveSummary.pdf.

cyberopérations à grande échelle. Les cyberdivisions des forces armées nationales ont aussi recours aux menaces persistantes avancées. Des « pirates indépendants » peuvent également tester de façon répétée les cyberdéfenses des sociétés privées et des États. Les menaces persistantes avancées cherchent, par nature, à atteindre un objectif à plus long terme que le simple profit que l'on peut tirer rapidement de l'utilisation d'un logiciel rançonneur.

### Cybermilices

28. Les cybermilices constituent une autre catégorie d'acteurs, qui rassemble diverses organisations formées de volontaires. Pour cette raison, ces milices pourraient ne pas entrer dans la catégorie des mercenaires ou des acteurs apparentés. Elles diffèrent des menaces persistantes avancées en ce qu'elles ne sont pas aussi bien organisées ni financées, et qu'elles n'ont pas d'objectifs stratégiques à long terme. Il est possible de distinguer, théoriquement, plusieurs types de cybermilices offensives fondées sur le volontariat : le forum, la cellule et le modèle hiérarchique. Le forum est une structure ponctuelle de cybermilice organisée autour d'une plateforme centrale de communications où les membres partagent les informations et les outils nécessaires pour mener leurs cyberattaques contre une cible choisie. La cellule est, quant à elle, constituée d'individus qui cherchent à pirater, pour des raisons politiques, des objectifs sur de longues périodes. Enfin, le modèle hiérarchique copie la structure hiérarchique traditionnelle, et peut prendre la forme d'organisations de volontaires soutenues par les États ou de groupes auto-organisés et soudés d'acteurs non étatiques. Il faut également ajouter à ces catégories celle des groupes organisés de cyberprofessionnels, qui se portent volontaires pour repousser des cyberattaques [19].

### Personnes physiques

29. Les cyberexperts sont des experts en technologies de l'information. Ils exercent souvent leur métier en dehors de toute structure organisationnelle et mènent des recherches indépendantes afin de détecter les vulnérabilités ou les erreurs logicielles[20]. Ces personnes sont dénommées « chercheurs en sécurité » et peuvent vendre des informations concernant ces vulnérabilités à des concurrents[21]. Selon le contexte, ils sont souvent rémunérés pour leur travail sous forme de « prime aux bogues ». Ils entrent en contact avec leurs clients potentiels sur des portails en ligne.

### Cybercriminels

30. Les réseaux d'extorsion sont composés de criminels sans scrupules dont le but n'est pas nécessairement de perturber l'économie ou d'effectuer des sabotages politiques, mais plutôt d'utiliser les données stockées par une entreprise pour lui extorquer de l'argent. Ce sont des personnes ou des groupes qui travaillent pour leur propre compte et qui visent des services, des produits et des infrastructures fournis par les secteurs public et privé, dont dépendent des groupes entiers voire toute une population. Ils demandent des rançons, et la réponse par les victimes ciblée à cette demande de rançon a des répercussions économiques et politiques qui vont au-delà de cet acte unique, car elle détermine la possibilité de contagion et de multiplication

---

[19] Voir Rain Ottis, « Proactive defence tactics against on-line cyber militia », dans *Proceedings of the 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01–02 July*, Academic Publishing, Reading, 2010, p. 233–237.

[20] Steve Ranger, « Meet the hackers who earn millions for saving the web, one bug at a time », *ZDNet*, 16 novembre 2020. Consultable à l'adresse suivante : https://www.zdnet.com/article/meet-the-hackers-who-earn-millions-for-saving-the-web-how-bug-bounties-are-changing-cybersecurity/.

[21] Voir la contribution de la Ligue internationale des femmes pour la paix et la liberté.

de ce type d'attaques. Par exemple, les perturbations continuent jusqu'au paiement de la rançon.

## B. Relations entre acteurs étatiques et non étatiques

31. La collaboration des États avec ces acteurs en ligne peut prendre diverses formes. Quand l'État sous-traite officiellement une opération, il exerce une véritable supervision sur les actions des intermédiaires en choisissant et en sélectionnant les acteurs, en évaluant les possibles incidences de leurs actions et en les sanctionnant, en cas de manquement[22]. Les intermédiaires assument alors des responsabilités claires conformément aux législations et politiques nationales comme dans le cas des attaques anticipées contre les cybermenaces [23] détectées qui pèsent sur les infrastructures critiques[24]. Quand l'État est le commanditaire d'une opération, il ne fait que soutenir passivement les intermédiaires, mais ne met pas en place de dispositifs de supervision stricte de leurs actions[25]. Dans ce cas, les cadres de politique sont généralement assez lâches, voire absents, et la collaboration est ponctuelle et s'effectue par l'intermédiaire de « relations à l'intérieur d'un réseau »[26]. Quand l'État donne simplement son aval à une opération, il ne reconnaît pas les actions entreprises par les acteurs privés opérant à partir de son territoire[27].

32. En privatisant certaines opérations de renseignement et stratégies militaires d'influence, un État sous-traite à des acteurs privés des tâches qu'il n'est plus apte ou disposé à assumer. Divers prestataires effectuent donc des missions qui auraient été précédemment l'apanage des forces de sécurité publique ainsi que des tâches qui n'ont jamais été du domaine de ces dernières (voir A/74/244).

33. Il existe plusieurs raisons pour un État de sous-traiter des cyberservices à des acteurs non étatiques. De même que, souvent, les États ne disposent pas des capacités nécessaires pour utiliser les modes classiques d'opérations militaires, certains d'entre eux ne possèdent pas de cybercapacités suffisantes, d'autant plus que cette technologie est coûteuse et en constante évolution. D'autre part, il est possible que les États ne puissent pas entretenir ces cybercapacités et qu'ils préfèrent, par conséquent, les sous-traiter de manière ponctuelle. La demande pour les cybercapacités est en plein essor[28]. D'importantes lacunes en matière de capacité et de moyens d'action sont, en effet, apparues dans les États au moment même où l'offre en la matière a commencé à s'enrichir[29]. Le recours au recrutement d'acteurs privés ou à la sous-traitance peut aussi coïncider, dans certains États, avec une réduction du budget de la défense ou la tendance plus générale à confier au secteur privé la fourniture de services publics, dont les opérations militaires et les services de

---

[22] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge, 2018, p. 29.

[23] Amanda N. Craig, Scott J. Shackelford et Janine S. Hiller, « Proactive cybersecurity: a comparative industry and regulatory analysis », *American Business Law Journal*, vol. 52, nº 4, hiver 2015.

[24] Ellyne Phneah, « S'pore beefs up cybersecurity law to allow preemptive measures », *ZDNet*, 14 janvier 2013, consultable à l'adresse suivante : www.zdnet.com/sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/.

[25] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge, 2018.

[26] Arindrajit Basu et Elonnai Hickok, « Conceptualizing an international framework for active private cyber defense ». Consultable à l'adresse suivante : https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049_e1a28ac2850d49fbb6f52eeb9fc79ae7.pdf.

[27] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge, 2018.

[28] Voir la contribution de Krieg, p. 1.

[29] Ibid.

sécurité[30]. Qui plus est, cette sous-traitance peut permettre aux États d'échapper à l'association avec certaines cyberactivités dont ils sont responsables et de s'épargner ainsi l'attention et les conséquences qu'elles peuvent entraîner[31].

34. Le Groupe de travail observe qu'il est difficile de déterminer avec certitude les cas spécifiques où les États recourent à des mercenaires et à des acteurs apparentés, et sous-traitent la fourniture de cyberservices à des acteurs non étatiques. Il est également difficile d'établir la portée et la nature exactes de la fourniture de ces services, compte tenu du caractère extrêmement sensible des opérations concernées ainsi que du secret et de l'opacité qui entourent le secteur numérique. Nous avons besoin de recherches supplémentaires pour pouvoir déterminer l'identité de ces acteurs et le type de services qu'ils fournissent[32]. Les recherches actuelles sur la façon dont les acteurs étatiques et non étatiques font appel à des prestataires de cybercapacités et en quoi ces services consistent sont incomplètes et laissent à désirer. Le fait que la majorité des entreprises de ce secteur sont des sociétés non cotées en bourse est l'une des nombreuses raisons qui expliquent ce manque de précisions[33].

35. Cependant, les informations que nous possédons incitent fortement à penser que les États ont régulièrement recours à de tels services et que cette tendance va se poursuivre. Le fait que le secteur des cyberservices a connu une forte croissance permet également de le penser ainsi que l'habitude qu'avaient les États de sous-traiter à des acteurs non étatiques les fonctions militaires et de sécurité conventionnelles avant même que les cyberactivités prennent l'importance qu'elles revêtent aujourd'hui. Un État ne peut généralement pas soutenir le rythme auquel le secteur privé développe de nouvelles technologies[34]. Dans un contexte de développements technologiques rapides et d'investissements dans les technologies numériques et l'intelligence artificielle, le Groupe de travail croit fermement que les cyberservices et les cyberproduits continueront à être sous-traités à des acteurs non étatiques.

36. Les cyberattaques comportent plusieurs phases et étapes, et il est donc extrêmement difficile d'en imputer la responsabilité à leurs auteurs et aux clients de ceux-ci. Dans une attaque de botnet, par exemple, un « botmaster » infiltre un vaste réseau d'ordinateurs vulnérables et ordonne au groupe d'ordinateurs infectés d'attaquer un réseau victime. Remonter au botmaster impliquerait d'enquêter dans plusieurs pays et sur plusieurs juridictions[35]. C'est particulièrement inquiétant, car les cyberopérations sont susceptibles de porter gravement atteinte aux droits humains. Autre source de préoccupation importante : leurs auteurs peuvent franchir les frontières et ainsi échapper aux contrôles réglementaires et aux mécanismes de la responsabilité[36].

37. Les États ainsi que des acteurs non étatiques ont commencé à avoir recours à des acteurs privés pour mettre en action la cyberpuissance à cause du coût relativement faible de ce type d'opérations par rapport à la guerre conventionnelle, mais aussi parce qu'il est ainsi possible de se dissimuler derrière un auteur dont l'identité est très difficile à établir. L'utilisation d'un intermédiaire crée une séparation entre la cible et l'auteur, qui bénéficie en outre de l'anonymat presque total que confèrent les activités en ligne et des difficultés pour imputer rapidement la

[30] Contribution présentée sous scellés.
[31] Voir la contribution de Krieg, p. 1.
[32] Voir la contribution de la fondation ICT for Peace, p. 2.
[33] Voir la contribution de The Citizen Lab, p. 1.
[34] Voir la contribution de la fondation ICT for Peace, p. 2.
[35] David D. Clark et Susan Landau, « Untangling attribution », *Harvard National Security Journal*, vol. 2, nº 2, 2011.
[36] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge, 2018.

responsabilité d'une cyberopération[37]. Il est intéressant d'avoir recours à ce type d'acteurs, car, à la différence des États qui sont soumis au droit international des droits de l'homme et au droit international humanitaire, ils opèrent en dehors de ces cadres réglementaires, ce qui rend leur identification, leur arrestation et leur poursuite difficiles[38]. Cela permet donc à un État de se dissocier des cyberopérations et, partant, d'éviter d'attirer l'attention, d'être désigné comme responsable et de subir les conséquences de ces actes[39].

# IV. Réglementer le rôle et l'implication des mercenaires, des acteurs apparentés et des entreprises de services de sécurité et de défense dans la fourniture de cyberservices

38. Réglementer au niveau international le rôle et l'implication des mercenaires, des acteurs apparentés et des entreprises de services de sécurité et de défense dans la fourniture de cyberservices, dont les cyberattaques et les opérations de cyberguerre, présente un certain nombre de difficultés. Il est, notamment, difficile de : a) conceptualiser la nature des cyberactivités, y compris les opérations de cyberguerre et les cyberattaques ; b) déterminer la source des cyberattaques et des autres cyberactivités ; c) attribuer ces attaques ou activités à des personnes ou à des entités précises ; et d) découvrir la relation avec l'acteur non étatique ou l'État pour le compte duquel ces activités sont entreprises, le cas échéant. À cela s'ajoute la question de savoir si ces cyberactivités constituent une implication ou une participation directe ou indirecte dans des hostilités en cours. La portée de la réglementation actuelle en matière de cyberactivités et la mesure dans laquelle celles-ci devraient être réglementées au niveau international font l'objet de nombreux débats.

39. Les difficultés susmentionnées tiennent à l'opacité qui entoure les cyberactivités, leur source et les entités qui les mènent ainsi que la relation entre les États et les autres acteurs non étatiques. Cette dissociation, difficilement réalisable dans les conflits armés cinétiques traditionnels, bénéficie aux États et aux acteurs non étatiques, car elle leur permet de ne pas assumer la responsabilité de leurs actions. Qui plus est, elle rend la réglementation de ces activités beaucoup plus difficiles. La difficile identification des auteurs de cyberopérations et la volonté de dissocier ces opérations de celles des forces armées nationales afin qu'il soit possible de nier, de façon plausible, toute participation constituent évidemment un sérieux obstacle aux progrès de la réglementation de ce domaine.

40. Le cadre réglementaire international en vigueur comprend la Charte des Nations unies, le droit international humanitaire, le Manuel de Tallinn sur le droit international applicable à la cyberguerre, le droit pénal international, le droit international des droits de l'homme, le droit non contraignant et le droit interne.

## A. Charte des Nations unies

41. La Charte des Nations unies, et en particulier l'article 2, paragraphe 4, qui interdit de recourir à la menace ou à l'emploi de la force contre l'intégrité territoriale ou l'indépendance politique de tout État, doit jouer un rôle dans la réglementation et la répression des cyberactivités, y compris le mercenariat. En effet, les cyberactivités

[37] Voir la contribution de la Ligue internationale des femmes pour la paix et la liberté, p. 4.

[38] Ataa Dabour, « The rise of cyber-mercenaries », site web de Human Security Centre, 2021. Consultable à l'adresse suivante : www.hscentre.org/technology/the-rise-of-cyber-mercenaries/.

[39] Voir la contribution de la fondation ICT for Peace, p. 2.

peuvent être d'une telle ampleur et entraîner des conséquences telles qu'on peut les assimiler à un « emploi de la force », ce qui les fait tomber sous le coup de la Charte. De même, ces activités peuvent constituer une « agression armée » et faire naître le droit de légitime défense d'un État, conformément à l'article 51 de la Charte. Ces cyberactivités constituent-elles vraiment un emploi de la force ou une agression armée, en particulier du point de vue des principes de nécessité et de proportionnalité[40] ? C'est une question de fait et de degré, mais, étant donné la nature et les conséquences des cyberactivités modernes, on peut sans aucun doute, dans certaines circonstances, répondre par l'affirmative.

42. Il est encore plus difficile de déterminer si les cyberattaques ou autres activités du même type menées par les acteurs non étatiques relèvent des dispositions applicables de la Charte des Nations unies. Pour répondre à cette question, il faut savoir s'il est possible d'attribuer les actions de ces personnes physiques ou entités à un État particulier conformément aux articles sur la responsabilité de l'État pour fait internationalement illicite, étant donné que la Charte des Nations unies ne s'applique qu'aux situations mettant en jeu des États souverains.

43. Il peut être extrêmement difficile de prouver quel État est le commanditaire de ces actes, car les entités qui les commettent se tiennent à bonne distance de celui-ci. En outre, il peut s'avérer compliqué, voire impossible, de remonter à la source des cyberattaques : elles sont, en effet, lancées à distance et peuvent intégrer diverses composantes provenant de plusieurs lieux et divers acteurs, sans compter que leurs auteurs emploient des moyens pour éviter d'être détectés et identifiés.

## B. Droit international des droits de l'homme et droit international humanitaire

44. Les États sont tenus de respecter les règles du droit international des droits de l'homme aussi bien en temps de paix qu'en temps de guerre, sous réserve des exceptions et dérogations prévues. Ils doivent également garantir le respect de ces règles par les acteurs privés qui opèrent sur leur territoire grâce au droit interne et aux mesures de répression. La législation bien étoffée et établie en matière de protection des droits de l'homme au niveau international, avec ses divers traités, ses organes conventionnels et ses mécanismes de mise en œuvre, peut dès à présent servir à réglementer le cyberespace.

45. Dans sa déclaration au Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, la conseillère principale en matière de maîtrise des armements du Comité international de la Croix-Rouge a affirmé que les règles du droit international humanitaire s'appliquaient aux nouvelles formes de conflit armé, dont la cyberguerre[41]. Pour parvenir à cette conclusion, elle s'est appuyée sur l'avis consultatif de la Cour internationale de Justice sur la licéité de la menace de l'emploi d'armes nucléaires, dans laquelle la Cour a conclu que le droit international humanitaire s'appliquait aux armements et aux types de guerre actuels et futurs[42]. Même si tout le monde ne s'accorde pas encore sur l'interprétation précise à donner

[40] Voir https://international-review.icrc.org/fr/articles/le-jus-ad-bellum-peut-il-lemporter-sur-le-jus-bello-reaffirmer-la-separation-de-ces-deux.

[41] Déclaration de Véronique Christory au Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale à New York, le 10 septembre 2019.

[42] *Licéité de la menace ou de l'emploi d'armes nucléaires*, Avis consultatif, C.I.J., Recueil 1996, rendu le 8 juillet 1996 ; CICR, document de position sur le droit international humanitaire et les cyberopérations pendant les conflits armés, novembre 2019, p. 4.

à l'application des principes concernés du droit international humanitaire aux cyberopérations dans le contexte d'un conflit armé, il semble néanmoins que les règles s'appliquent bien en principe. Cette logique est confirmée par le Manuel de Tallinn sur le droit international applicable à la cyberguerre. Il est parfaitement clair sur la question : le « droit des conflits armés s'applique aux cyberopérations comme à toute autre opération entreprise dans le contexte d'un conflit armé ».

46. Cependant, une fois de plus, cette façon d'aborder la question n'est pas sans difficulté, à cause notamment du rôle des acteurs non étatiques qui fournissent de tels cyberservices. Il n'existe pas de consensus au niveau international sur la définition de « cyberattaque » (ou « hostilités en ligne ») dans le droit international humanitaire. Toutefois, la notion d'« attaque » elle-même est de la première importance, surtout en rapport avec le principe de discrimination et la distinction entre les objectifs militaires et les objectifs civils. La nature militaire ou civile des objectifs peut être sujette à interprétation, mais cette interprétation ne dépend pas du type d'opérations militaires employé pendant l'attaque. Que l'attaque soit menée au moyen d'opérations de guerre cinétique ou en ayant recours à des cybertechnologies, il convient, dans les deux cas, de respecter la nature civile de l'objectif.

47. Un autre sujet de préoccupation concerne le statut d'une cyberopération pendant un conflit armé et, plus particulièrement, la possibilité de déterminer si l'opération constitue une participation directe aux hostilités, ce qui serait suffisant pour caractériser leurs auteurs comme des mercenaires au sens de l'article 47 du Protocole additionnel I aux Conventions de Genève de 1949, ou si elle présente un lien suffisamment étroit avec un conflit armé spécifique. Dans certains cas, les cyberattaques qui cherchent à détruire les capacités et les infrastructures d'un État pourraient être considérées comme une participation directe aux hostilités de la part d'un acteur non étatique dans le contexte d'un conflit armé[43]. Déterminer si une cyberactivité en particulier est susceptible d'affecter la capacité militaire d'une partie à un conflit et de lui porter préjudice, en établissant un lien suffisamment étroit entre l'acte et le conflit armé, est une question de fait et de degré. Au-delà de ces aspects juridiques, la question a aussi des implications plus pratiques, car il n'est pas toujours possible de déterminer si une cyberattaque ou une autre cyberactivité plus subtile a eu lieu. L'interprétation de tous les concepts dépendra certainement de la pratique des États.

48. En ce qui concerne plus spécifiquement les mercenaires, toute personne qui répond à cette définition n'a pas droit au statut de combattant ni aux protections y afférentes. Qui plus est, actuellement, les mercenaires peuvent être poursuivis pour le simple fait d'avoir participé aux (cyber)hostilités, même si un État ou un acteur non étatique les a engagés à cette fin. Ils peuvent être poursuivis pour des activités liées au mercenariat du moment que le droit interne concerné prévoit des dispositions pour réprimer ces actes. Par ailleurs, conformément à l'article premier commun des Conventions de Genève de 1949, les États s'engagent à respecter et à faire respecter la convention, ce qui suppose de veiller à ce que les entités qui travaillent pour leur compte, dont potentiellement des acteurs non étatiques, agissent conformément au droit international humanitaire.

49. En conséquence, certains estiment que la définition classique de « mercenaire » n'est peut-être plus adaptée à l'évolution des moyens de faire la guerre et des formes de conflits contemporains, qui se caractérisent par le recours à la cyberguerre ou à

[43] Nils Melzer, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, CIRC, Genève, mai 2009. Consultable à l'adresse suivante : www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf.

d'autres cyberactivités, ou du moins y font appel. Cela signifie qu'il faut sans doute repenser la façon de définir un mercenaire dans le cyberespace[44].

50. Une autre question, qui devra être envisagée dans le cadre de l'application au cyberespace du droit international humanitaire, est de savoir si les divers régimes juridiques qui s'appliquent aux conflits armés internationaux et non internationaux, devront s'appliquer de la même façon aux cyberservices. Il faudra déterminer, en observant l'évolution de la cyberguerre et des cyberopérations, si la distinction traditionnelle est toujours pertinente.

51. En outre, il reste un problème fondamental à résoudre. Le droit international humanitaire fournit un cadre réglementaire bien établi et complet, qui pourrait être appliqué aux cyberactivités, mais celui-ci n'est applicable qu'en temps de guerre. Or, de nombreuses cyberactivités, peut-être même la majorité d'entre elles, sont menées en temps de paix, ce qui pourrait suggérer que le droit international humanitaire ne s'y applique pas.

## C. Droit pénal international

52. Le droit pénal international s'applique à toute personne physique qui commet un crime international et la Cour pénale internationale est compétente en cas de crime de guerre, de crime contre l'humanité, de génocide et de guerre d'agression. Par conséquent, si des cyberservices fournis par des personnes physiques satisfont à une ou plusieurs caractéristiques d'un ou plusieurs crimes, et que d'autres critères applicables sont remplis, la Cour pénale internationale pourrait être compétente pour les actes criminels commis par des mercenaires et des acteurs apparentés dans le cyberespace. Le droit pénal international peut se révéler utile dans la mesure où le concept de responsabilité des supérieurs hiérarchiques peut permettre de surmonter certaines difficultés liées à l'identification et la localisation de l'auteur réel. Les supérieurs des personnes qui sont impliquées dans la commission du crime, en ordonnant, par exemple, de mener une cyberattaque dévastatrice, ou qui s'abstiennent de prévenir une telle attaque seraient ainsi tenus pour responsables[45]. En plus des difficultés déjà mentionnées, le droit pénal international oblige à prouver de manière incontestable, lors d'une procédure internationale, que le crime a eu lieu, ce qui correspond aux exigences les plus strictes en matière de preuve. D'autre part, vu que plusieurs États peuvent participer à une même cyberopération, des problèmes de compétence et de complémentarité peuvent se poser, ce qui est susceptible de créer des obstacles supplémentaires pour enquêter sur les faits et poursuivre leurs auteurs.

53. La Convention internationale contre le recrutement, l'utilisation, le financement et l'instruction de mercenaires et la Convention de l'Organisation de l'Union Africaine sur l'élimination du mercenariat en Afrique criminalisent le mercenariat dans le cadre de conflits armés, ce qui crée un fondement juridique supplémentaire pour poursuivre et sanctionner les activités liées au mercenariat. Les États qui ratifient ces conventions devraient transposer les dispositions concernées dans leur droit interne et permettre ainsi à leurs tribunaux de poursuivre les activités des mercenaires.

## D. Droit non contraignant et initiatives en cours

54. En plus des cadres contraignants du droit international, un certain nombre d'initiatives multilatérales et multipartites visant divers auteurs et encourageant un comportement responsable lors du recours aux technologies de l'information et des

[44] Voir la contribution de Van der Waag-Cowling, Van Niekerk et D[r] Ramluckan, p. 4.
[45] Voir la contribution d'Access Now, p. 10.

communications ont été lancées au cours des dix dernières années. Il peut s'agir de cadres normatifs non contraignants, comme le Cybersecurity Tech Accord et le Charter of Trust, qui s'adressent aux acteurs privés. Des groupes d'experts indépendants comme le Global Commission on the Stability of Cyberspace et celui qui a rédigé le Manuel de Tallinn ont également formulé des recommandations sur les normes et le droit international applicables. D'autres initiatives multipartites comme l'Appel de Paris pour la confiance et la sécurité dans le cyberespace sont destinées tant au secteur privé qu'à la société civile et aux États.

55. Au niveau du Conseil des droits de l'homme, un Groupe de travail intergouvernemental à composition non limitée joue un rôle important dans l'élaboration du contenu pour un cadre réglementaire international relatif à la réglementation, à la supervision et au contrôle des activités des entreprises de services de sécurité et de défense. Du fait de l'évolution rapide des contextes opérationnels et des services fournis, tout mécanisme réglementaire ainsi élaboré devrait utiliser les termes « services » et « activités » plutôt qu'« entreprises de services de sécurité et de défense » afin de détecter plus efficacement les violations du droit international humanitaire ou du droit international des droits de l'homme[46].

56. Deux groupes constitués par l'Assemblée générale afin d'examiner l'ensemble des questions liées à la sécurité dans le domaine des technologies de l'information et des communications pourraient fournir des orientations à cet égard : le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (voir la résolution 73/27 de l'Assemblée générale) et le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale (voir la résolution 73/266 de l'Assemblée générale). Ces deux groupes examinent six domaines principaux : menaces existantes et potentielles ; règles, normes et principes pour un comportement responsable des États ; droit international ; mesures de renforcement de la confiance ; et dialogue institutionnel régulier.

57. En mars 2021, le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale a adopté un rapport de consensus comprenant plusieurs recommandations non contraignantes pour tous les États Membres. Même si aucune recommandation n'aborde la question des mercenaires et des acteurs apparentés, le rapport mentionne plusieurs fois les droits de l'homme et insiste sur le fait que certains acteurs non étatiques disposent maintenant de capacités en technologies de l'information et des communications auxquelles seuls les États avaient auparavant accès. Le rapport précise que l'augmentation constante des incidents créés par l'utilisation malveillante des technologies de l'information et des communications (TIC) par des acteurs étatiques et non étatiques est inquiétante (voir A/AC.290/2021/CRP.2, par. 16). Dans sa résolution 75/240 du 31 décembre 2020, l'Assemblée générale a décidé de constituer un nouveau Groupe de travail à composition non limitée jusqu'en 2025, et le Groupe de travail sur l'utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes estime que c'est une excellente occasion pour examiner la question des mercenaires et des acteurs apparentés opérant dans le cyberespace.

58. Dans son rapport de consensus de 2021, le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États

[46] Voir déclaration de Jelena Aparac, présidente du Groupe de travail sur l'utilisation de mercenaires. Consultable à l'adresse suivante : www.ohchr.org/EN/HRBodies/HRC/IGWG_PMSCs/Pages/Session2.aspx.

dans le cyberespace dans le contexte de la sécurité internationale a affirmé de nouveau que « les États ne doivent pas avoir recours à des intermédiaires pour commettre des faits internationalement illicites au moyen des TIC, et devraient faire en sorte que des acteurs non étatiques ne puissent pas commettre de tels actes à partir de leur territoire »[47]. Ces propos, même s'ils ne constituent pas une norme de droit international, condamnent les États qui ont recours à des intermédiaires ou qui leur donnent leur aval. Le Groupe d'experts gouvernementaux a souligné que les efforts accomplis par les États pour promouvoir le respect et l'application des droits de l'homme ainsi que ceux pour s'assurer de l'utilisation responsable et sécurisée des TIC devraient être complémentaires, se renforcer mutuellement et aller de pair. Il a également reconnu que la surveillance de masse peut avoir des répercussions négatives sur les droits humains, y compris le droit à la vie privée[48].

59. Les nouvelles initiatives normatives constituent, selon certains, un « régime complexe » pour la cybersécurité, qui tient plus de la concentration d'efforts que d'un véritable instrument contraignant.

# V. Incidences sur les droits humains

60. Incontestablement, les cyberactivités ont des incidences sur les normes et règles en matière de droits humains, et peuvent entraîner des violations, dans les conflits armés et en temps de paix, de toute une série de droits. Le Groupe de travail rappelle ses conclusions : les risques et les effets, en fonction du genre, des activités menées à bien par les entreprises de services de sécurité et de défense ont de nombreux points communs, indépendamment de leur taille et des services fournis (voir A/74/244, par. 6). En outre, il a identifié des groupes particulièrement touchés par les mercenaires et les acteurs apparentés engagés par les États, comme les défenseurs et défenseuses des droits de l'homme, les personnes migrantes, les dirigeants et dirigeantes de l'opposition et les journalistes ainsi que les personnes lesbiennes, gays, bisexuelles, transgenres, intersexes et de genre non conforme aux catégories établies dans le contexte de la violence fondée sur le genre.

61. Les formes nouvelles et émergentes de guerre peuvent avoir des répercussions importantes sur les objectifs militaires et sur la population civile, et entraîner des violations du droit international humanitaire ainsi que des droits et libertés des personnes, dans le contexte des conflits armés ou dans d'autres contextes. Le Groupe de travail a indiqué précédemment qu'il est aujourd'hui admis que la cyberguerre permet non seulement de s'infiltrer parmi des objectifs militaires et civils, de les perturber, de les endommager, voire de les détruire, mais aussi de nuire gravement aux êtres humains[49]. Le cybersabotage peut avoir des effets secondaires catastrophiques sur le fonctionnement de certaines infrastructures critiques et porter ainsi atteinte à la santé, à la sûreté et à la sécurité du public. C'est pourquoi ce sont le droit à la vie et le droit de ne pas être soumis à la torture ou à d'autres traitements ou peines cruels, inhumains ou dégradants, qui sont les premiers menacés par les cyberopérations.

### Droits à la vie privée et à la liberté d'expression

62. Les droits à la vie privée et à la liberté d'expression sont susceptibles d'être violés dans tous les contextes. Quand des mercenaires et des acteurs apparentés sont

[47] Voir https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf, par. 71, point g).

[48] Ibid., par. 39 et 37.

[49] CICR, « Le droit international humanitaire et les cyberopérations pendant les conflits armés », document de position, novembre 2019.

déployés pour attaquer les États, ils deviennent invariablement des outils essentiels pour violer la souveraineté et l'intégrité territoriale de ces États, ce qui a également des conséquences sur l'exercice du droit à la vie privée.

63. Ce droit peut également être bafoué par la surveillance et la collecte de renseignements. Il est très préoccupant de constater que des cyberopérations visent la société civile et perturbent, en particulier, le travail des défenseurs et défenseuse des droits de l'homme et des journalistes, dans le but d'étouffer toute opposition et de renforcer le contrôle d'un État sur sa population. Bien entendu, les gouvernements emploient depuis toujours diverses méthodes pour suivre et surveiller leurs citoyens, dissidents, opposants politiques et défenseurs des droits de l'homme, mais les outils technologiques dont ils disposent aujourd'hui, comme les logiciels malveillants et espions, leur permettent de le faire à moindre coût et d'élargir la couverture géographique de leur surveillance ainsi que sa portée et son ampleur, et de mener ainsi une répression numérique plus complète que jamais[50]. Certains logiciels espions, qui permettent de surveiller leurs cibles à distance, en sont une illustration parfaite[51].

64. D'autre part, il a été suggéré que le contrôle exercé par certains États sur le contenu en ligne ainsi que la diffusion d'informations fausses et la désinformation peuvent violer le droit à la liberté d'expression. Les cyberopérations menées ou commanditées par les gouvernements peuvent porter atteinte à l'intégrité du cyberespace, à la liberté d'expression et à d'autres libertés civiles dont jouissent non seulement les personnes, mais aussi les groupes et les sociétés, dans leur ensemble[52]. La surveillance ciblée pousse également certains à s'autocensurer, ce qui affecte directement la capacité des journalistes et des défenseurs et défenseuses des droits de l'homme à mener leurs enquêtes ainsi qu'à former et entretenir des relations avec des sources d'information[53].

65. Les technologies de surveillance développées, gérées et parfois utilisées par les sociétés privées jouent un rôle déterminant dans la modification des routes migratoires, qui s'éloignent des zones de détection pour se diriger vers des zones qui sont hors de portée des dispositifs de surveillance. Les migrants sont donc contraints d'emprunter des itinéraires moins directs et plus dangereux, ce qui augmente la difficulté matérielle du voyage ainsi que les atteintes, la douleur et la souffrance physiologiques et psychologiques qui sont souvent à l'origine de décès dus à des coups de chaleur, à une déshydratation grave et à d'autres maladies pendant les voyages par voie maritime ou terrestre[54].

66. Les cybercapacités ont des répercussions néfastes importantes sur les institutions et les personnes : elles affaiblissent la capacité des États à fournir une protection et à assurer le bien-être de larges portions de la population, et font obstacle à la jouissance des droits humains. Les attaques qui visent les systèmes électoraux, par exemple, violent directement les droits démocratiques fondamentaux des citoyens à la représentation, ce qui les prive de leur droit de vote. De plus, selon certains rapports, des pays lancent régulièrement des cyberattaques sur des cibles civiles et emploient, pour cela, des mercenaires numériques qui piratent des sociétés privées ou

[50] Voir la contribution de The Citizen Lab, p. 8.
[51] A/HRC/41/35, par. 9 ; Bill Marczak et coll., « Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries », site web de Citizen Lab, 18 septembre 2018.
[52] S/2021/569, par. 103.
[53] Voir A/HRC/38/35/Add.2, par. 53 ; A/HRC/41/35 par. 26.
[54] A/HRC/45/9, par. 44-45.

ébranlent les forces armées étrangères en utilisant les outils en ligne pour manipuler l'information ou diffuser de la propagande en vue de modeler les opinions[55].

67. Certaines cyberattaques auraient également provoqué des dégâts matériels généralisés, notamment aux réseaux électriques, aux institutions financières et aux ministères[56]. La destruction de bases de données contenant des informations sur les citoyens pourrait rapidement entraîner l'arrêt complet des administrations et des entreprises privées, et causer plus de dommages aux civils que la destruction d'objectifs physiques[57].

### Autodétermination

68. L'utilisation de produits et de services militaires et de sécurité dans le cyberespace par les entreprises de cybersécurité pourrait empêcher l'exercice du droit des peuples à disposer d'eux-mêmes. Ces acteurs sont, en effet, en mesure d'exercer une influence sur certaines insurrections internes d'une manière qui pourrait, à terme, compromettre le droit à l'autodétermination (voir A/71/318, par. 20).

## VI. Conclusions et recommandations

69. **L'évolution des technologies et leur passage au numérique ont une incidence directe sur toutes les sphères de la vie civile. Le secteur militaire est également de plus en plus dépendant des technologies numériques. L'accélération de la transition numérique est illustrée par l'adéquation de plus en plus complète entre la sphère de l'information et le cyberespace, ce qui peut avoir des répercussions négatives sur les populations en temps de paix comme en temps de guerre.**

70. **Le Groupe de travail a tenu compte de l'évolution de la fourniture de services et de produits militaires et de sécurité dans le cyberespace par les mercenaires, les acteurs apparentés et les entreprises de services de sécurité et de défense ainsi que de ses incidences sur la jouissance des droits humains. Il a observé qu'il était difficile de s'en tenir aux activités de ceux qui répondent à la définition de « mercenaire » en vigueur dans le cadre juridique international et a donc adopté une approche plus globale en examinant différentes sortes d'acteurs et de manifestations susceptibles de renvoyer plus souplement au concept d'activités liées au mercenariat.**

71. **Le Groupe de travail a observé avec inquiétude que certains États, volontairement ou par omission, dissimulent leur participation à des opérations de cybermalveillance et cherchent à exercer une influence militaire stratégique en refusant d'assumer leurs responsabilités au regard du droit international, notamment pour des violations et des atteintes commises par des acteurs non étatiques recrutés à cette fin. Pourtant, le recrutement d'acteurs privés pour fournir des services militaires et de sécurité dans le cyberespace n'exempte pas les États de leurs obligations en vertu du droit international.**

---

[55] Paul D. Shinkman, « America Is losing the cyber war », site web d'U.S. News and World Report, 29 septembre 2016. Consultable à l'adresse suivante : www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries.

[56] Neri Zilber, « The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments? », *Foreign Policy* (FP), 31 août 2018. Consultable à l'adresse suivante : https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/.

[57] CICR, « Le droit international humanitaire et les cyberopérations pendant les conflits armés », document de position, novembre 2019.

72. **Face à l'évolution rapide et à la nouveauté des manifestations des acteurs liés au mercenariat, les États et les autres parties prenantes doivent donc se saisir sans délai de cette question. Le présent rapport propose des considérations qui doivent leur servir au moment d'élaborer une réglementation plus efficace des acteurs du cyberespace en vue de faire respecter, de protéger et de réaliser le droit des peuples à l'autodétermination, d'assurer une protection aux civils en situation de conflit armé, et de sauvegarder les principes de non-intervention et d'intégrité territoriale. L'examen de cette réglementation devrait s'appuyer sur le cadre juridique international relatif aux mercenaires, quelles qu'en soient les lacunes, et sur le cadre plus général du droit international humanitaire et du droit international des droits de l'homme.**

**Recommandations**

73. **Pour empêcher et atténuer les répercussions négatives sur les droits humains des activités des mercenaires, des acteurs apparentés et des entreprises de services de sécurité et de défense dans le cyberespace, les États devraient s'abstenir de recruter, d'utiliser, de financer et de former des mercenaires, et inscrire l'interdiction de ces activités dans leur droit interne tout en réglementant efficacement les entreprises de services de sécurité et de défense.**

74. **Les États devraient s'engager à la transparence quand ils recourent à des services de soutien militaire et traduire cet engagement sur le plan opérationnel. Ils devraient ainsi rendre publiques, rapidement et de manière suffisamment détaillée, les informations relatives à la nature des services en question, aux procédures de passation de marchés, aux conditions des contrats et à l'identité des prestataires de services. Ils ne devraient pas invoquer systématiquement des questions de sécurité nationale pour restreindre l'accès à de telles informations. Au contraire, les restrictions de l'accès aux informations devraient répondre aux critères des principes de légalité, de nécessité et de proportionnalité, conformément au droit à la liberté d'expression.**

75. **Les États doivent enquêter sur toute allégation de violation du droit international humanitaire et d'atteinte aux droits humains par des mercenaires, des acteurs apparentés, et des entreprises de services de sécurité et de défense, engager des poursuites, prononcer des sanctions, s'il y a lieu, et prévoir des recours effectifs pour les victimes. Les enquêtes, poursuites et procès doivent respecter et garantir le droit à un procès équitable et la loyauté de la procédure.**

76. **Au niveau international, les États devraient engager un dialogue sur les formes changeantes et nouvelles que prennent les mercenaires, en particulier ceux, quelle que soit leur nature, qui opèrent dans le cyberespace, sur les menaces qu'ils représentent pour le droit international humanitaire et le droit international des droits de l'homme, ainsi que sur les moyens de lutter plus efficacement contre eux. Les organisations internationales et régionales, la société civile et des experts devraient participer à ce dialogue, qui tiendra compte des outils existants et des initiatives en cours.**

77. **Les États devraient reprendre les discussions avec le Groupe de travail intergouvernemental à composition non limitée chargé d'élaborer le contenu d'un cadre réglementaire international relatif à la réglementation, à la supervision et au contrôle des activités des entreprises de services de sécurité et de défense[58], y compris sur les questions de la fourniture de cyberservices par celles-ci et les opérations de cyberguerre qu'elles mènent. Un instrument juridiquement contraignant est nécessaire pour régir le cyberespace. Un cadre**

[58] Voir résolution 36/11 du Conseil des droits de l'homme.

**juridique international apporterait certitude et prévisibilité grâce à des obligations légales claires, qui peuvent être imposées par des instances spécialisées de règlement des différends. La fragmentation des régimes de gouvernance entretient la confusion réglementaire et désavantage souvent les pays en développement et les acteurs de la société civile.**

78. **Le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale devraient continuer à examiner les risques que font courir aux droits humains la participation de mercenaires et d'acteurs apparentés aux cyberopérations.**

79. **S'agissant des activités des mercenaires, des acteurs apparentés et des entreprises de services de sécurité et de défense qui sont associés à des acteurs armés non étatiques, les États devraient établir et mettre en avant des procédures internationales afin d'élaborer, d'évaluer et de perfectionner des mécanismes pour établir plus clairement et officiellement les obligations des acteurs armés non étatiques en vertu du droit international des droits de l'homme, notamment des critères propres à déterminer leur capacité à honorer les obligations en matière de respect des droits humains.**