Naciones Unidas A/76/151

Asamblea General

Distr. general
15 de julio de 2021
Español
Original: inglés

Septuagésimo sexto período de sesiones
Tema 74 del programa provisional*
Derecho de los pueblos a la libre determinación

Utilización de mercenarios como medio de violar los derechos humanos y obstaculizar el ejercicio del derecho de los pueblos a la libre determinación

Nota del Secretario General

El Secretario General tiene el honor de transmitir a la Asamblea General el informe del Grupo de Trabajo sobre la utilización de mercenarios como medio de violar los derechos humanos y obstaculizar el ejercicio del derecho de los pueblos a la libre determinación, de conformidad con lo dispuesto en la resolución 75/171 de la Asamblea y la resolución 42/9 del Consejo de Derechos Humanos.

* A/76/150.

21-09837X (S)

Se ruega reciclar

Informe del Grupo de Trabajo sobre la utilización de mercenarios como medio de violar los derechos humanos y obstaculizar el ejercicio del derecho de los pueblos a la libre determinación

Repercusión en los derechos humanos de la participación de mercenarios, agentes relacionados con ellos y empresas militares y de seguridad privadas en actividades cibernéticas

Resumen

En el presente informe, el Grupo de Trabajo sobre la utilización de mercenarios como medio de violar los derechos humanos y obstaculizar el ejercicio del derecho de los pueblos a la libre determinación examina el suministro de productos y servicios militares y de seguridad en el ciberespacio por parte de mercenarios, agentes relacionados con ellos y empresas militares y de seguridad privadas, así como sus repercusiones sobre los derechos humanos.

Existe una amplia gama de servicios militares y de seguridad que se prestan en el ciberespacio, como la recopilación de datos, la inteligencia y el espionaje. Los Estados y los agentes no estatales pueden contratar agentes privados a través de diferentes relaciones indirectas para proteger sus propias redes e infraestructuras, así como para llevar a cabo ciberoperaciones destinadas a debilitar la capacidad militar de las fuerzas armadas enemigas o socavar la integridad del territorio de otros Estados. Las personas que llevan a cabo ciberataques pueden causar daños a distancia, en distintas jurisdicciones. Por lo tanto, se puede considerar que estas personas realizan una actividad relacionada con los mercenarios, o incluso una actividad mercenaria, si se cumplen todos los criterios de calificación.

El objetivo del presente estudio temático es analizar las manifestaciones y actividades de estos agentes que se benefician del desarrollo, el mantenimiento y la explotación de las cibercapacidades, que se pueden utilizar en situaciones de hostilidades y en entornos tanto de conflicto como de no conflicto. En él se evalúan las repercusiones que esto puede tener en los derechos humanos, incluido el derecho de los pueblos a la libre determinación, y se analiza la cuestión de la regulación del suministro de productos y servicios militares y de seguridad en el ciberespacio.

Durante la preparación del presente informe, el Grupo de Trabajo estuvo compuesto por Jelena Aparac (Presidenta), Lilian Bobea, Ravindran Daniel, Chris Kwaja y Sorcha MacLeod.

Índice

Página

I. Introducción y contexto 4

II. Consideraciones relacionadas con las definiciones 5

III. Servicios militares y de seguridad en el ciberespacio: actividades, categorías de agentes y relaciones entre los agentes estatales y no estatales 7

A. Categorías de ciberagentes pertinentes 8

B. Relaciones entre los agentes estatales y no estatales 11

IV. Regulación de la función y la implicación de los mercenarios, los agentes relacionados con ellos y las empresas militares y de seguridad privadas en la prestación de ciberservicios 13

A. Carta de las Naciones Unidas 14

B. Derecho internacional de los derechos humanos y derecho internacional humanitario . . . 15

C. Derecho penal internacional 16

D. Derecho indicativo e iniciativas en curso 17

V. Repercusiones en los derechos humanos 19

VI. Conclusiones y recomendaciones 21

I. Introducción y contexto

1. El Grupo de Trabajo sobre la utilización de mercenarios como medio de violar los derechos humanos y obstaculizar el ejercicio del derecho de los pueblos a la libre determinación presenta este informe a la Asamblea General, de conformidad con lo dispuesto en la resolución 75/171 de la Asamblea General y la resolución 42/9 del Consejo de Derechos Humanos.

2. Con el fin de cumplir este mandato, el Grupo de Trabajo supervisa a los mercenarios y las actividades relacionadas con ellos en todas sus formas y manifestaciones, así como a las empresas militares y de seguridad privadas en distintas partes del mundo. Además, el Grupo de Trabajo estudia sus actividades y la repercusión que pueden tener en los derechos humanos, en particular el derecho a la libre determinación.

3. El presente informe se fundamenta sobre una amplia investigación documental y las contribuciones recibidas de los interesados pertinentes sobre la base de un llamamiento para la presentación de comunicaciones publicado por el Grupo de Trabajo en enero de 2021[1]. El 7 de diciembre de 2020, el Grupo de Trabajo organizó una consulta de expertos en línea sobre los mercenarios y los agentes relacionados en el contexto de la ciberseguridad y las nuevas tecnologías, con el fin de integrar sus resultados en el informe. El Grupo de Trabajo agradece a todos los que contribuyeron a la preparación del informe mediante la presentación de información y la participación en la consulta de expertos.

4. Los debates sobre las actividades de los mercenarios a lo largo de los años se han centrado en los modos de guerra tradicionales en los que los mercenarios participan en nombre de los Estados o de otros clientes. Más recientemente, los mercenarios, los agentes relacionados con ellos y las empresas militares y de seguridad privadas han participado activamente en el ciberespacio. En su informe sobre la evolución de las formas, tendencias y manifestaciones de los mercenarios y las actividades relacionadas con ellos (véase A/75/259), el Grupo de Trabajo se refirió a los denominados “cibermercenarios” como una categoría de agentes que pueden llevar a cabo actividades relacionadas con los mercenarios. Además, la cuestión del uso de las tecnologías y las transferencias de conocimientos se plantea de forma periódica en los informes anuales del Grupo de Trabajo en relación con diversos temas[2]. En el presente informe se analiza el suministro de productos y servicios militares y de seguridad en el ciberespacio por parte de los mercenarios, los agentes relacionados con ellos y las empresas militares y de seguridad privadas, así como sus repercusiones en los derechos humanos.

5. En sus análisis anteriores, el Grupo de Trabajo ha señalado la variedad de mercenarios y agentes relacionados con ellos que siguen influyendo en el curso de los conflictos armados contemporáneos, cometiendo abusos contra los derechos humanos y socavando el derecho a la libre determinación, incluso a través de ciberactividades. Hoy en día, el ciberespacio representa un importante escenario geoestratégico para los agentes estatales y no estatales, pues existe una variedad de entidades privadas que movilizan y aprovechan las cibercapacidades defensivas y ofensivas en la

[1] Véase https://www.ohchr.org/Documents/Issues/Mercenaries/WG/Webcall-SPM-GA76-SP.docx.
[2] Véanse A/75/259, párr. 50; A/HRC/45/9, párr. 39 y ss.; A/HRC/42/42.

búsqueda de intereses o programas indirectos, lo que tiene consecuencias devastadoras para el disfrute de los derechos humanos y para el derecho de los pueblos a la libre determinación.

6. En particular, el Grupo de Trabajo ha señalado anteriormente la naturaleza cada vez más asimétrica de los conflictos armados modernos, así como el aumento de la participación de los agentes privados (A/75/259). Aunque la guerra cinética tradicional sigue desempeñando una función importante en los conflictos contemporáneos, el uso de los ciberataques y otras ciberactividades es cada vez más frecuente a medida que las nuevas tecnologías se desarrollan y siguen evolucionando, incluso fuera de los conflictos armados tradicionales. Como consecuencia de esta evolución, los mercenarios contemporáneos y otros agentes se han adaptado al ciberespacio y han participado en él de manera más activa y, en algunos casos, se han convertido en un componente fundamental de las ciberoperaciones.

II. Consideraciones relacionadas con las definiciones

7. El término “mercenario” se define en el artículo 47 del Protocolo Adicional I a los Convenios de Ginebra de 1949, en la Convención Internacional contra el Reclutamiento, la Utilización, la Financiación y el Entrenamiento de Mercenarios y en la Convención de la Organización de la Unidad Africana para la Eliminación de la Actividad de Mercenarios en África. No obstante, la definición de “mercenario” en el derecho internacional ha sido objeto de muchos análisis y reflexiones que se centran en su carácter excesivamente restrictivo. El Grupo de Trabajo reconoce que el alcance de la definición es problemático y que los criterios son difíciles de cumplir, especialmente en lo que respecta a las formas contemporáneas de actividades relacionadas con mercenarios, incluso cuando los agentes no estatales llevan a cabo estas actividades en el ciberespacio.

8. Además, ante la falta de una definición jurídica convenida internacionalmente, el Grupo de Trabajo ha definido anteriormente el término “empresas militares y de seguridad privadas” como entidades empresariales que prestan servicios militares o de seguridad remunerados por medio de personas físicas o personas jurídicas[3]. Pueden actuar tanto en situaciones de conflicto como de paz y son importantes proveedores de productos y servicios militares y de seguridad en la ciberesfera.

9. Aunque ninguna de las definiciones anteriores incluye una referencia explícita a las ciberactividades ni a los ciberagentes, es evidente que algunas medidas adoptadas en la ciberesfera pueden alcanzar el nivel de mercenarismo o considerarse actividades relacionadas con los mercenarios y también afectan a los derechos humanos tanto en los conflictos armados como en tiempos de paz. Dichas medidas podrían incluir ciberoperaciones maliciosas llevadas a cabo por ciberintermediarios, independientemente de su nacionalidad o del lugar en el que desarrollen sus operaciones o de si están actuando fuera de línea o en línea o causando daño de forma directa o indirecta[4]. Se entiende que las ciberoperaciones maliciosas implican el uso de medidas y operaciones deliberadas encaminadas a alterar, interrumpir, degradar o

[3] La definición completa figura en el documento A/HRC/15/25, anexo, artículo 2.

[4] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, Reino Unido, Cambridge University Press, 2018), pág. 31.

destruir redes o sistemas informáticos o engañarlos, o socavar de otro modo la confidencialidad, la integridad y la disponibilidad de las redes y los sistemas informáticos para las personas y las comunidades[5]. No se incluyen las tecnologías emergentes (por ejemplo, la tecnología de los drones) que tienen efectos cinéticos fuera de las redes de computadoras.

10. Sin embargo, el Grupo de Trabajo desea subrayar que los servicios militares y de seguridad prestados en el ciberespacio no deberían utilizarse para designar a las operaciones llevadas a cabo por los agentes relacionados con los mercenarios en general, sino que cada posible caso de entre esas categorías debe evaluarse a la luz de su contexto y sus circunstancias concretos (véase A/75/259, párr. 54).

11. En 2020, el Grupo de Trabajo reconoció la ciberguerra como un método de guerra que no solo permite infiltrarse, perturbar, dañar e incluso destruir objetos militares o civiles, sino que también puede causar graves daños humanos. El Comité Internacional de la Cruz Roja ha llegado a la conclusión de que, al igual que la guerra convencional, debe cumplir con el derecho internacional humanitario[6]. Esto es tanto más relevante cuanto que las capacidades estratégicas dependen cada vez más de las infraestructuras y la tecnología (véase A/75/259, párr. 42).

12. La transformación de los conflictos contemporáneos y la rápida evolución de las nuevas formas de guerra, junto con la falta de regulación, seguimiento y supervisión, así como las dificultades para investigar los delitos que se perpetran en las distintas jurisdicciones, impulsaron al Grupo de Trabajo a arrojar luz sobre este fenómeno. El acceso desigual de algunos países desarrollados y agentes ricos a las tecnologías y a los conocimientos técnicos relacionados también ha sido un motivo de preocupación para el Grupo de Trabajo.

13. El Grupo de Trabajo es consciente de que los contextos en los que operan los mercenarios repercuten en las mujeres, los niños y otros grupos de manera diferenciada y desproporcionada (véase A/75/259, párr. 5). Asimismo, señala las dificultades derivadas de la falta de una definición convenida internacionalmente de lo que constituye un ciberataque o las ciberhostilidades en el marco del derecho internacional humanitario y que, por lo tanto, actualmente es difícil desde el punto de vista conceptual situar las ciberhostilidades en el marco del derecho internacional humanitario y reconocer el incumplimiento y las violaciones.

14. Un elemento fundamental del debate en curso sobre cuándo, dónde y cómo se regulan y podrían regularse estas ciberactividades es la función de los agentes no estatales en las ciberactividades y la ciberguerra, en particular los mercenarios, los agentes relacionados con ellos y las empresas militares y de seguridad privadas, así como otras entidades privadas y comerciales. Por lo tanto, el Grupo de Trabajo trata de analizar en el presente informe una serie de servicios militares y de seguridad prestados en el ciberespacio que pueden generar actividades relacionadas con los mercenarios a fin de estimular un debate sobre la mejor manera de acotarlos y abordarlos (véase A/75/259, párr. 52). Además de la regulación, debe promoverse una

[5] Herbert S. Lin, “Offensive cyber operations and the use of force”, *Journal of National Security Law and Policy*, vol. 4, núm. 1 (13 de agosto de 2010), págs. 4 a 63; e ISO/IEC 27000:2009.

[6] Comité Internacional de la Cruz Roja, “Derecho internacional humanitario y ciberoperaciones durante conflictos armados”, documento de posición del CICR, noviembre de 2019.

cooperación eficaz en los ámbitos nacional e internacional entre los agentes pertinentes para hacer frente a este fenómeno.

III. Servicios militares y de seguridad en el ciberespacio: actividades, categorías de agentes y relaciones entre los agentes estatales y no estatales

15. Los servicios militares y de seguridad abarcan una serie de servicios entre los que se incluyen la recopilación de datos y el espionaje. Los Estados y los agentes no estatales pueden contratar agentes privados a través de diferentes relaciones indirectas para llevar a cabo operaciones ofensivas y defensivas encaminadas a proteger sus propias redes e infraestructuras, así como para llevar a cabo ciberoperaciones con el objetivo de debilitar la capacidad militar de las fuerzas armadas enemigas o socavar la integridad del territorio de otro Estado. Al utilizar su potencia de fuego cibernética ofensiva o defensiva, estos agentes están vinculados a intentos o medidas que pretenden identificar, invadir y distorsionar instalaciones militares o civiles fundamentales, con el objetivo de destruirlas.

16. Tal y como se ha mencionado más arriba, es importante señalar que los ciberservicios se prestan a los Estados fuera del contexto de los conflictos armados, incluso con fines no solo de recopilación de información y vigilancia, sino también de aplicación de la ley nacional y mantenimiento de la seguridad[7]. Además, los ciberservicios incluyen tanto la prestación de servicios de apoyo a los Estados en relación con las cibercapacidades existentes como el suministro de ciberproductos que puedan utilizar los Estados. Es importante señalar que se ofrece una amplia variedad de productos y servicios que se pueden adquirir en el mercado libre, lo que debe tenerse en cuenta a la hora de examinar la regulación de los ciberservicios.

17. Entre los múltiples tipos de ciberactividades y métodos de ciberoperaciones que se llevan a cabo actualmente se incluyen el sabotaje a través de programas maliciosos y programas secuestradores, el espionaje y la subversión que implica el suministro de información errónea y desinformación. En la práctica, estas actividades pueden consistir en la interrupción o el daño de infraestructuras clave, como el suministro de electricidad y agua, los hospitales y los servicios de vigilancia y comunicación, o también pueden facilitar el ataque o la incapacitación de los sistemas militares de defensa y de otro tipo.

18. En su labor en favor de las empresas privadas y los Estados, las empresas de ciberseguridad proporcionan defensas contra los ciberataques y la ciberguerra. Estas operaciones puramente defensivas incluyen cortafuegos, parches y programas antivirus, mientras que las medidas más activas, pero también defensivas, incluyen la creación de *honeypots* y *tar pits* y la señalización para advertir y atrapar a los atacantes[8]. Tanto si son pasivas como activas, estas operaciones defensivas se rigen según las directrices jurídicas existentes en relación con las operaciones de ciberseguridad.

[7] Véase la presentación de ICT for Peace.

[8] La información se obtuvo con carácter confidencial.

19. No obstante, tanto las empresas de ciberseguridad privadas como las gubernamentales, así como los operadores corruptos, también tienen capacidades ofensivas, lo que constituye un ámbito de especial preocupación para el Grupo de Trabajo. Las capacidades ofensivas de las empresas de ciberseguridad pueden implementarse contra los Estados desarrollados, por ejemplo, en los ataques a la infraestructura electoral, los cuales se supone que llevan a cabo agentes patrocinados por el Estado o representantes que trabajan para los Estados. Las ciberactividades maliciosas también incluyen el ataque a los activos virtuales y a los proveedores de servicios de activos virtuales, así como los ataques a las empresas de defensa, incluso para acceder de forma ilegal a la tecnología militar (véase S/2021/211, anexo, párrs. 125 y 126). No existe un patrón unificador claro y aparente que caracterice a los agentes estatales y no estatales que adquieren estas tecnologías. Tanto los Estados democráticos como los no democráticos adquieren tecnologías ofensivas de proveedores externos, al igual que los Estados con cibercapacidades internas y los que carecen de tales recursos.

20. El mercado de las cibercapacidades ofensivas está creciendo rápidamente, está sujeto a poca regulación y ofrece la oportunidad de obtener un beneficio importante. En consecuencia, muchas empresas militares y de seguridad privadas convencionales están creando divisiones de ciberseguridad[9]. Independientemente de su procedencia, los proveedores de ciberseguridad, al igual que las empresas militares y de seguridad privadas más tradicionales, colaboran estrechamente con los Gobiernos nacionales y se convierten en extensiones del poder estatal, por lo que podrían considerarse representantes mercenarios.

21. Las distinciones entre los servicios ofensivos y defensivos y entre la transparencia y la ambigüedad en cuanto a la condición jurídica se puede aplicar a los servicios militares y de seguridad prestados en el ciberespacio. Los Estados y los agentes no estatales pueden contratar agentes privados no solo para proteger sus propias redes e infraestructuras, sino también para llevar a cabo ciberoperaciones destinadas a debilitar la capacidad militar de las fuerzas armadas enemigas o socavar la integridad del territorio de otro Estado. La presencia de mercenarios en el ciberespacio, donde actualmente participan en la producción y la venta de armas cibernéticas ofensivas, pone de manifiesto su capacidad de adaptación[10]. Se puede considerar que las personas que llevan a cabo ciberataques realizan una actividad relacionada con los mercenarios, o incluso una actividad mercenaria si se cumplen todos los criterios de calificación (véase A/75/259, párr. 71).

A. Categorías de ciberagentes pertinentes

Ciberunidades o cibercomandos integrados en las fuerzas armadas oficiales

22. En los últimos años, la competencia por los conocimientos cibernéticos especializados se vio estimulada por las estrategias de ciberinfluencia que

[9] W. J. Hennigan, “Defense contractors see opportunity in cybersecurity sector”, *Los Angeles Times*, 21 de enero. Disponible en http://www.latimes.com/business/la-fi-0122-cyber-defense-20150122-story.html.

[10] Tom Burt, “Cyber mercenaries don’t deserve immunity”, sitio web de Microsoft, 21 de diciembre de 2020. Disponible en https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

demostraron sus efectos devastadores en las relaciones geopolíticas modernas[11]. Algunos Estados están participando en lo que se ha descrito como una "lucha informativa en el ciberespacio"[12] y están incorporando las operaciones de las estrategias militares de influencia en sus capacidades militares. La rápida evolución de las tecnologías digitales ha transformado profundamente la guerra y ha impulsado las inversiones en el desarrollo de ciberunidades o cibercomandos integrados en las fuerzas armadas oficiales. Además, a las formas clásicas de guerra entre dos fuerzas armadas se suma ahora la ciberguerra, en la que las ciberunidades actúan en las delgadas líneas que separan las operaciones defensivas de las ofensivas[13]. Las ciberoperaciones se pueden llevar a cabo de manera independiente o en combinación con las operaciones militares convencionales. Sin embargo, la hipótesis más preocupante sigue siendo la relacionada con el caso de las "operaciones híbridas", en las que el Estado responde con sus operaciones cibermilitares en un contexto que no se consideraría que ha alcanzado el umbral del conflicto armado según las normas del derecho internacional humanitario. La lucha informativa en el ciberespacio es aún más compleja cuando las fuerzas armadas formales subcontratan algunas de sus ciberactividades a un tercero.

Agentes ajenos a las fuerzas armadas oficiales

23. Las entidades no estatales que no forman parte de las fuerzas armadas desempeñan una función muy importante y cada vez más amplia en la prestación de ciberservicios a los Estados y en su nombre. La amenaza creciente de la privatización de los ataques a la ciberseguridad a través de una nueva generación de empresas privadas denominadas "cibermercenarios" está proliferando[14], y la línea que separa las esferas privada y nacional es cada vez más difusa[15].

Entidades empresariales

24. A diferencia de las empresas militares y de seguridad privadas convencionales, que normalmente han privatizado funciones y capacidades que antes estaban monopolizadas por el Estado, los proveedores de ciberseguridad surgieron y prosperaron primero en el sector privado. Aunque los ejércitos más avanzados del mundo han desarrollado conocimientos y capacidades de ciberseguridad internos, incluso estas sofisticadas operaciones militares recurren en gran medida a los conocimientos en materia de ciberseguridad del sector privado[16]. Entre las empresas privadas de ciberseguridad se encuentran agentes con ánimo de lucro arraigados y ágiles empresas emergentes que han ganado cuotas de mercado en un mercado en rápida expansión.

---

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

[12] Véase https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf, págs. 7 y 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 de agosto de 2018. Disponible en https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/.

[14] Véase la presentación de Access Now, pág. 1.

[15] Véase la presentación de Ori Swed y Daniel Burland, pág. 15.

[16] Véase www.cmi.no/publications/file/6637-russian-use-of-private-military-and-security.pdf.

25. Las empresas privadas de *software* y tecnología que están comprendidas en el ámbito del análisis pueden dividirse en dos grupos. Una subcategoría está formada por grandes plataformas tecnológicas que trabajan en connivencia con entidades gubernamentales con el objetivo de que el Gobierno pueda acceder a la información y ejecutar programas de vigilancia[17]. La otra subcategoría está formada por empresas mucho más pequeñas y con un nivel de ingresos menor, pero con capacidades específicas para fabricar productos que pueden utilizarse para llevar a cabo actividades maliciosas. El sector de las empresas privadas de ciberseguridad está creciendo y evolucionando rápidamente. Además, varias empresas militares y de seguridad privadas se han introducido en el ámbito de la ciberseguridad, a menudo mediante la adquisición de empresas tecnológicas especializadas y su incorporación interna.

26. Las empresas del sector de la defensa que tradicionalmente producían armas y equipos militares han ampliado sus actividades al sector digital. Estos contratistas han desarrollado en gran medida soluciones y servicios de ciberseguridad internos, aunque algunos también han contratado a empresas comerciales de ciberseguridad como filiales para reforzar sus capacidades. Los mensajes públicos de las empresas de armamentos difuminan intencionadamente las líneas existentes entre las medidas y los servicios destinados exclusivamente a defender la resiliencia del ciberespacio y las tecnologías disruptivas que permitirían a los clientes emprender operaciones ofensivas y actividades potencialmente maliciosas.

Grupos de amenazas persistentes avanzadas

27. Los miembros de los grupos de amenazas persistentes avanzadas son agentes corruptos o delincuentes que se dedican a la penetración continua de los sistemas de ciberseguridad de los Estados y de los agentes públicos y privados. Son tecnológicamente sofisticados y poseen importantes recursos financieros y técnicos, tienen objetivos estratégicos a largo plazo y a menudo reciben algún tipo de apoyo de los Gobiernos nacionales[18]. Tienen capacidad de desarrollo de capacidades ofensivas internas y pueden llevar a cabo ciberoperaciones a gran escala. Las divisiones cibernéticas de los ejércitos nacionales también lanzan amenazas persistentes avanzadas. Los “piratas informáticos por cuenta ajena” también pueden poner a prueba de forma persistente las ciberdefensas de las empresas privadas y los Gobiernos. Por su propia naturaleza, los grupos de amenazas persistentes avanzadas están asociados a un objetivo a más largo plazo que el de obtener beneficios rápidos mediante el uso de programas secuestradores.

Cibermilicias

28. Otra categoría es la de las llamadas cibermilicias, que engloban una serie de organizaciones respaldadas por voluntarios. Como tal, esas milicias no pertenecen a la categoría de los mercenarios o de los agentes relacionados con ellos. Se diferencian de los grupos de amenazas persistentes avanzadas en que no están tan bien organizados ni financiados y carecen de objetivos estratégicos a largo plazo. Un modelo teórico para las cibermilicias ofensivas basadas en el voluntariado

[17] Véase https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.

[18] Véase https://targetedthreats.net/media/1-ExecutiveSummary.pdf.

distingue entre el foro, la célula y la jerarquía. El foro es una estructura de cibermilicia especial que se organiza en torno a una plataforma central de comunicaciones, en la que los miembros comparten la información y las herramientas necesarias para llevar a cabo ciberataques contra el objetivo elegido. El modelo celular se materializa en las células de piratas informáticos, que se dedican al pirateo informático por motivos políticos durante largos períodos de tiempo. La jerarquía refleja el modelo estructural tradicional, que puede plasmarse en organizaciones de voluntarios patrocinadas por el gobierno, así como en agentes no estatales cohesionados y autoorganizados. En la categoría de cibermilicias también se incluyen grupos organizados de ciberprofesionales que se ofrecen como voluntarios para repeler ciberataques[19].

Personas

29. Los ciberexpertos que poseen conocimientos técnicos en tecnología de la información suelen trabajar al margen de cualquier estructura orgánica y realizan investigaciones independientes destinadas a detectar vulnerabilidades o errores en los programas informáticos[20]. Estas personas se conocen como investigadores de seguridad y pueden vender información relacionada con esas vulnerabilidades a los adversarios[21]. Dependiendo del contexto, a menudo se les compensa por esta labor mediante pagos conocidos como “recompensa por errores”. Se conectan con clientes potenciales a través de portales en línea.

Ciberdelincuentes

30. Las redes de extorsión penal son agentes delincuentes corruptos cuyo objetivo no es necesariamente perturbar la economía ni llevar a cabo un sabotaje político, sino utilizar la posesión de datos empresariales como mecanismo de extorsión. Son personas o grupos que trabajan en beneficio propio y que se centran en los servicios, los productos y las infraestructuras que proporcionan los sectores público y privado, y de los que dependen comunidades y poblaciones enteras. Extorsionan los rescates y la respuesta a la demanda de rescate por parte de las víctimas seleccionadas tiene consecuencias económicas y políticas que van más allá del acto individual en sí, con respecto a la posible expansión y perpetuación de este tipo de ataques. Por ejemplo, las disrupciones continúan hasta que se paga un rescate.

B. Relaciones entre los agentes estatales y no estatales

31. La interacción del Estado con estos ciberagentes puede adoptar diferentes formas. En el caso de la delegación, el Estado ejerce una clara supervisión de las medidas adoptadas por los representantes a través del análisis y la selección de los agentes, la sanción punitiva y una clara evaluación de las posibles repercusiones[22].

---

[19] Véase Rain Ottis, “Proactive defence tactics against on-line cyber militia”, en *Proceedings of the 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01-02 July* (Reading, Reino Unido, Academic Publishing, 2010), págs. 233 a 237.

[20] Steve Ranger, “Meet the hackers who earn millions for saving the web, one bug at a time”, ZD Net, 16 de noviembre de 2020. Disponible en www.zdnet.com/article/meet-the-hackers-who-earn-millions-for-saving-the-web-how-bug-bounties-are-changing-cybersecu.

[21] Véase la presentación de la Liga Internacional de Mujeres por la Paz y la Libertad.

[22] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, Reino Unido, Cambridge University Press, 2018), pág. 29.

En este caso, se asignan responsabilidades claras a los representantes a través de los canales de la legislación y la política nacionales, por ejemplo, para llevar a cabo ataques anticipatorios contra las ciberamenazas percibidas[23] en la infraestructura crítica[24]. En caso de orquestación, el Estado presta apoyo pasivo a los representantes, pero no establece mecanismos claros de supervisión de sus operaciones[25]. Por lo general, esto se consigue mediante marcos normativos vagamente definidos o ausentes y una colaboración especial a través de "relaciones en red"[26]. En el modelo sancionador, el Estado no reconoce las medidas llevadas a cabo por los agentes privados que actúan desde su territorio[27].

32. Mediante el proceso de privatización de algunas de las operaciones informativas y estrategias militares de influencia, un Estado subcontrata a agentes privados aquellas tareas que ya no puede o no quiere realizar. Múltiples proveedores realizan tareas que antes podían llevar a cabo las fuerzas de orden público, como también tareas adicionales que nunca fueron del ámbito de las fuerzas de seguridad estatales (véase A/74/244).

33. Los Estados subcontratan ciberservicios a agentes no estatales por varias razones. Del mismo modo que los Estados carecen a menudo de las capacidades necesarias para los modos de guerra tradicionales, es posible que algunos Estados no posean suficientes cibercapacidades, especialmente cuando la tecnología correspondiente está en constante evolución y conlleva un costo importante. Asimismo, es posible que los Estados no puedan mantener esas cibercapacidades y, por tanto, prefieran subcontratarlas según las necesidades. La demanda de cibercapacidades está en auge[28]. Ha coincidido con una gran escasez de capacidad y de medios en los Estados, y ha sido una consecuencia de esta[29]. La transición a la contratación de agentes privados o a la subcontratación puede estar relacionada en algunos Estados con la reducción de los presupuestos de defensa y con la orientación general a la participación del sector privado en la prestación de servicios públicos que incluirán las operaciones militares y los servicios de seguridad[30]. Además, esta subcontratación puede permitir a los Estados desvincularse de las ciberactividades y evitar el escrutinio y las consecuencias[31].

34. El Grupo de Trabajo señala la dificultad de identificar con certeza ejemplos concretos en los que los Estados utilizan mercenarios y agentes relacionados con ellos

---

[23] Amanda N. Craig, Scott J. Shackelford y Janine S. Hiller, "Proactive cybersecurity: a comparative industry and regulatory analysis", *American Business Law Journal*, vol. 52, núm. 4 (invierno de 2015).

[24] Ellyne Phneah, "S'pore beefs up cybersecurity law to allow preemptive measures", ZDNet (14 de enero de 2013). Disponible en 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, Reino Unido, Cambridge University Press, 2018).

[26] Arindrajit Basu y Elonnai Hickok, "Conceptualizing an international framework for active private cyber defense". Disponible en https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049_e1a28ac2850d49fbb6f52eeb9fc79ae7.pdf.

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

[28] Véase la presentación de Krieg, pág. 1.

[29] *Ibid.*

[30] La información se presentó con carácter confidencial.

[31] Véase la presentación de Krieg, pág. 1.

y subcontratan la prestación de ciberservicios a agentes no estatales. Asimismo, resulta complicado determinar el alcance y la naturaleza exactos de la prestación de esos servicios, debido al carácter sumamente sensible de esas operaciones y el carácter secreto y la opacidad que caracterizan al sector cibernético. Es necesario realizar un mayor análisis para determinar qué agentes prestan determinado tipo de servicios[32]. La investigación actual sobre la forma en que los agentes estatales y no estatales contratan cibercapacidades y sobre el tipo de servicios que están adquiriendo es imperfecta e incompleta. El carácter incompleto del panorama se debe a diferentes factores, entre ellos el hecho de que la mayoría de las empresas que trabajan en este ámbito son empresas privadas (que no cotizan en bolsa)[33].

35. Sin embargo, la información recibida indica claramente que este tipo de contratación y subcontratación está en curso y continuará en el futuro. Además, se puede suponer con cierta seguridad que se está produciendo como consecuencia del gran crecimiento del sector de los ciberservicios y el hecho de que, antes de la ampliación de la función de las ciberactividades, los Estados subcontrataban las funciones de seguridad tradicionales y las funciones militares a agentes no estatales. Normalmente, los Gobiernos no pueden mantener el ritmo al que el sector privado desarrolla las nuevas tecnologías[34]. En el contexto de la rápida evolución tecnológica y de las inversiones en tecnologías digitales e inteligencia artificial, el Grupo de Trabajo cree firmemente que los ciberservicios y los ciberproductos seguirán subcontratándose a agentes no estatales.

36. Los ciberataques tienen varias etapas y pasos, por lo que atribuir la responsabilidad a los autores y a sus clientes es extremadamente difícil. En un ataque de *botnet*, por ejemplo, un *botmaster* se infiltra en una gran red de ordenadores vulnerables y dirige la red de equipos comprometidos para atacar una red de víctimas. La localización del ataque hasta el *botmaster* abarcaría varios países y varias jurisdicciones[35]. Esto plantea importantes problemas debido a la posibilidad de socavar de manera significativa los derechos humanos. La posibilidad de que los representantes cibernéticos se desplacen a través de las fronteras y escapen así a los mecanismos de control y responsabilidad regulados es un motivo de gran preocupación[36].

37. Tanto los Estados como los agentes no estatales han empezado a utilizar agentes privados para hacer ver su poder cibernético, habida cuenta de los costos relativamente bajos de esas operaciones en comparación con los de la guerra convencional y de la posibilidad de ocultarse detrás de un agente cuya identidad es muy difícil de descubrir. El uso de un representante genera un nivel de separación entre el autor y su objetivo, que se beneficia además del alto grado de anonimato disponible en línea y de las dificultades que implica atribuir la responsabilidad de una ciberoperación de manera oportuna[37]. La ventaja de recurrir a estos agentes radica en que, a diferencia de los Estados que están sujetos a los protocolos de derecho

[32] Véase la presentación de ICT for Peace, pág. 2.
[33] Véase la presentación de The Citizen Lab, pág. 1.
[34] Véase la presentación de ICT for Peace, pág. 2.
[35] David D. Clark y Susan Landau, “Untangling attribution”, *Harvard National Security Journal*, vol. 2, núm. 2 (2011).
[36] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, Reino Unido, Cambridge University Press, 2018).
[37] Véase la presentación de la Liga Internacional de Mujeres por la Paz y la Libertad, pág. 4.

internacional de los derechos humanos y de derecho internacional humanitario, estos actúan fuera del ámbito de dichos protocolos, lo que dificulta la atribución, las detenciones y el enjuiciamiento[38]. Esto permite a su vez que un Estado se desvincule de las ciberoperaciones y, en consecuencia, evite el escrutinio y la atribución de responsabilidad en sentido general y de responsabilidad civil[39].

IV. Regulación de la función y la implicación de los mercenarios, los agentes relacionados con ellos y las empresas militares y de seguridad privadas en la prestación de ciberservicios

38. La regulación de la función y la participación de los mercenarios, los agentes relacionados con los mercenarios y las empresas militares y de seguridad privadas en la prestación de ciberservicios, incluidos los ciberataques y la ciberguerra, a nivel internacional plantea un número importante de desafíos y dificultades. En particular, están relacionados con a) la conceptualización de lo que constituyen las ciberactividades, incluidos la ciberguerra y los ciberataques; b) la identificación del origen de los ciberataques y otras ciberactividades; c) la atribución de dichos ataques o actividades a personas o entidades concretas; y d) la identificación de la relación entre el agente no estatal y el Estado en cuyo nombre se llevan a cabo dichas actividades, si es que se llevan a cabo, y la cuestión de si determinadas ciberactividades constituyen una implicación o una participación directa o indirecta en las hostilidades en curso. Existen amplios debates y deliberaciones que se centran en el alcance de la actual reglamentación en relación con las ciberactividades y en la medida en que deberían regularse a nivel internacional.

39. Estas dificultades se derivan de la naturaleza opaca de las ciberactividades, de su origen y de las entidades que las llevan a cabo, así como de la relación existente entre los Estados y los demás agentes no estatales. Esta desvinculación, que no es tan fácil de lograr en el contexto de un conflicto armado cinético tradicional, beneficia a los agentes estatales y no estatales, ya que los protege potencialmente de la responsabilidad por sus acciones; sin embargo, hace que la regulación de esas actividades resulte mucho más difícil. La cuestión de la atribución de las ciberoperaciones y el asunto de la desvinculación intencionada de dichas operaciones de las fuerzas armadas del Estado, de manera que pueda haber una "negación plausible", es evidentemente un problema grave a la hora de promover la regulación.

40. El marco regulatorio internacional existente incluye la Carta de las Naciones Unidas, el derecho internacional humanitario, el *Tallinn Manual on the International Law Applicable to Cyber Warfare*, el derecho penal internacional, el derecho internacional de los derechos humanos, el derecho indicativo y el derecho nacional.

A. Carta de las Naciones Unidas

41. La Carta de las Naciones Unidas, y en particular el Artículo 2, párrafo 4, que prohíbe la amenaza o el uso de la fuerza contra la integridad territorial y la

[38] Ataa Dabour, "The rise of cyber-mercenaries", 2021. Disponible en www.hscentre.org/technology/the-rise-of-cyber-mercenaries/.

[39] Véase la presentación de ICT for Peace, pág. 2.

independencia política de cualquier Estado, debe desempeñar una función en la regulación y la sanción de las ciberactividades, incluidas las actividades mercenarias. Esto se basa en el hecho de que las ciberactividades pueden ser de tal escala y efecto como para constituir un "uso de la fuerza" y, por lo tanto, pueden estar prohibidas según la Carta de las Naciones Unidas. Del mismo modo, estas actividades pueden alcanzar el umbral de un "ataque armado", lo que desencadena el derecho de un Estado a actuar en legítima defensa, de conformidad con el Artículo 51 de la Carta de las Naciones Unidas. El hecho de que estas ciberactividades cumplan los umbrales pertinentes, en particular en lo que respecta a los principios de necesidad y proporcionalidad[40], es una cuestión de hecho y de grado, pero no cabe duda de que, dada la naturaleza y los efectos de las ciberactividades modernas, podrían cumplir esos umbrales en circunstancias particulares.

42. Sin embargo, una cuestión más difícil que hay que considerar es si los ciberataques u otras actividades realizadas por agentes no estatales implicarían las disposiciones pertinentes de la Carta de las Naciones Unidas. La respuesta dependería de si las medidas llevadas a cabo por esas personas o entidades son atribuibles a un Estado concreto en virtud del proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, dado que la Carta de las Naciones Unidas solo se aplica a situaciones que se producen entre Estados soberanos.

43. La cuestión de la atribución puede plantear grandes desafíos desde el punto de vista probatorio, dado que las entidades que prestan servicios de ciberactividad trabajan a menudo a una distancia considerable del Estado y el origen de los ciberataques puede ser difícil o imposible de rastrear, pues se inician a distancia y pueden incluir diferentes aportaciones de diferentes lugares y agentes. Además, existe, por supuesto, un uso deliberado de mecanismos encaminados a evitar la detección y la atribución de los ataques.

B. Derecho internacional de los derechos humanos y derecho internacional humanitario

44. Los Estados están obligados a respetar las normas internacionales de derechos humanos, tanto en tiempos de paz como durante los conflictos armados, con las excepciones y derogaciones pertinentes y específicas. Los Estados también están obligados a garantizar el cumplimiento por parte de los agentes privados dentro de su territorio a través de la legislación nacional y su aplicación. El amplio y desarrollado marco de protección de los derechos humanos a nivel internacional, con sus diversos tratados, órganos de supervisión y mecanismos de aplicación, es un medio adecuado para la regulación del ciberespacio.

45. En su declaración en el grupo de trabajo de composición abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, el Comité Internacional de la Cruz Roja afirmó que las normas del derecho internacional humanitario se aplican a las nuevas formas de

[40] Véase https://international-review.icrc.org/es/articulos/puede-prevalecer-el-jus-ad-bellum-sobre-el-jus-bello-reafirmar-la-separacion-de-estas-dos.

conflicto armado, incluida la ciberguerra[41]. Para llegar a esta conclusión, se basa en la opinión consultiva de la Corte Internacional de Justicia en el caso relativo a la legalidad o el uso de las armas nucleares, en la que la Corte determinó que el derecho internacional humanitario se aplica a las armas y los tipos de guerra actuales y futuros[42]. Aunque existe un debate en curso acerca de una interpretación específica con respecto a la aplicación de los principios pertinentes del derecho internacional humanitario a las ciberoperaciones en el contexto de los conflictos armados, parece que las normas se aplican en principio. Este enfoque se confirma en el *Tallinn Manual* con respecto a la ley aplicable a la ciberguerra. En el Manual se afirma de forma inequívoca que el derecho de los conflictos armados se aplica a las ciberoperaciones como a otras operaciones realizadas en el contexto de un conflicto armado.

46. Sin embargo, una vez más, este enfoque no está exento de dificultades, sobre todo teniendo en cuenta la función de los agentes no estatales que prestan estos ciberservicios. No existe ninguna definición convenida internacionalmente de lo que constituye un ciberataque o las ciberhostilidades dentro del derecho internacional humanitario. No obstante, el concepto de "ataque" en sí mismo es significativo, principalmente en relación con el principio de distinción y con lo que constituyen los objetivos militares y civiles. El carácter militar o civil de los objetivos puede ser objeto de interpretación, pero esta interpretación no depende del método de guerra utilizado durante el ataque. Tanto si el ataque se lleva a cabo a través de medios cinéticos de guerra como a través del uso de cibertecnologías, debe respetarse el carácter civil del objeto.

47. Otra cuestión de interés es la condición de una ciberoperación durante un conflicto armado y, más concretamente, el hecho de determinar si la operación constituye una participación directa en las hostilidades, lo cual es relevante para cumplir los criterios de clasificación como mercenario según el artículo 47 del Protocolo Adicional I a los Convenios de Ginebra de 1949, o si tiene un vínculo suficiente con el conflicto armado específico. En algunos casos, los ciberataques encaminados a destruir las capacidades y la infraestructura del Estado equivaldrían a la participación directa en las hostilidades de un agente no estatal en el contexto de un conflicto armado[43]. Es una cuestión de hecho y de grado el hecho de determinar si una ciberactividad concreta puede afectar a la capacidad militar de una parte de un conflicto, y si es probable que cause daño a una parte de un conflicto, con un vínculo suficiente entre el acto y el conflicto armado. Además de los aspectos jurídicos, esta cuestión tiene también una dimensión más práctica, ya que no siempre es posible descubrir la ocurrencia de ciberataques o ciberactividades más sutiles. La

[41] Declaración de Véronique Christory, asesora principal de control de armas del Comité Internacional de la Cruz Roja, ante el grupo de trabajo de composición abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, Nueva York, 10 de septiembre de 2019.

[42] *Legalidad de la Amenaza o el Empleo de Armas Nucleares, Opinión consultiva, I.C.J. Reports 1996*, publicada el 8 de julio de 1996. CICR, documento de posición sobre el derecho internacional humanitario y las ciberoperaciones durante los conflictos armados, noviembre de 2019, pág. 4.

[43] Nils Melzer, *Guía para interpretar la noción de participación directa en las hostilidades según el derecho internacional humanitario* (Ginebra, CICR, mayo de 2009). Véase https://www.icrc.org/es/doc/assets/files/other/icrc_003_0990.pdf.

interpretación de todos los conceptos dependerá probablemente de la práctica de los Estados.

48. En relación con los mercenarios, más concretamente, las personas que se ajustan a la definición de mercenario no tienen derecho a la condición de combatiente y a sus protecciones inherentes. Lo que es más importante, actualmente pueden ser procesados por el mero hecho de haber participado en las hostilidades, independientemente de que un agente estatal o no estatal los haya contratado para participar en las (ciber)hostilidades. Asimismo, pueden ser procesados por el hecho de haber participado en las actividades mercenarias siempre que el régimen nacional correspondiente establezca tales disposiciones jurídicas. Además, de acuerdo con el artículo 1 común de los Convenios de Ginebra de 1949, los Estados están obligados a hacer respetar el Convenio y esto incluye garantizar que las entidades que actúan en su nombre, entre las que se pueden incluir agentes no estatales que actúan en nombre de los Estados, intervengan de acuerdo con el derecho internacional humanitario.

49. En consecuencia, se ha señalado que la definición tradicional de mercenario puede no adecuarse a la evolución de los medios de guerra y a los conflictos contemporáneos que se caracterizan por el uso de la ciberguerra u otras ciberactividades o al menos implican su uso, lo que pone de manifiesto la necesidad de reconceptualizar la comprensión de lo que constituye un mercenario dentro del ámbito cibernético[44].

50. Otra cuestión que se plantea, y que habrá que tener en cuenta en relación con la aplicación del derecho internacional humanitario en el ámbito cibernético, tiene que ver con los diferentes regímenes jurídicos que se aplican a los conflictos armados internacionales y a los no internacionales, y con el hecho de determinar si habrá que adoptar ese mismo enfoque en relación con los ciberservicios. Se plantea también la cuestión de si, con la evolución de la ciberguerra y las ciberoperaciones, se puede mantener la distinción tradicional.

51. Además, existe una cuestión fundamental que se deriva del hecho de que, aunque el derecho internacional humanitario proporciona un marco regulatorio muy desarrollado y exhaustivo que puede aplicarse a las ciberactividades, por supuesto, solo se aplica en tiempos de conflicto armado. Es cierto que muchas ciberactividades, y quizás la mayoría, se producen fuera del contexto de un conflicto armado y, por tanto, no se aplicaría el régimen normativo del derecho internacional humanitario.

C. Derecho penal internacional

52. El derecho penal internacional se aplica a cualquier persona física que cometa un delito internacional, y la Corte Penal Internacional tiene jurisdicción sobre los crímenes de guerra, los crímenes de lesa humanidad, el genocidio y la guerra de agresión. Por lo tanto, si los ciberservicios prestados por personas físicas satisfacen uno o más elementos de uno o más delitos y se cumplen otros criterios relevantes, la Corte Penal Internacional podría tener jurisdicción sobre los actos delictivos cometidos por mercenarios y agentes relacionados con ellos en la ciberesfera. El derecho penal internacional puede resultar útil en la medida en que la doctrina de la

[44] Véase la presentación de Van der Waag-Cowling, Van Niekerk y el Dr. Ramluckan, pág. 4.

responsabilidad de mando podría ayudar a superar algunos de los obstáculos relacionados con la identificación y la localización del autor real. Los superiores de estas personas que estén implicados en la comisión del delito, como, por ejemplo, por haber ordenado la comisión de ciberataques devastadores, o que no impidan estos ciberataques maliciosos no deben eludir la rendición de cuentas[45]. Además de los desafíos ya indicados anteriormente, el derecho penal internacional exige que los delitos se demuestren en los procesos internacionales más allá de toda duda razonable, la norma probatoria más estricta. Asimismo, dado que las ciberoperaciones pueden implicar a varios Estados, es posible que surjan problemas de jurisdicción y complementariedad que podrían generar desafíos adicionales para las investigaciones y los enjuiciamientos.

53. Tanto la Convención Internacional contra el Reclutamiento, la Utilización, la Financiación y el Entrenamiento de Mercenarios como la Convención de la Organización de la Unidad Africana para la Eliminación de la Actividad de Mercenarios en África tipifican como delito el mercenarismo, lo que crea una base jurídica alternativa para el enjuiciamiento y el castigo de las actividades relacionadas con los mercenarios. Los Estados que ratifiquen estas convenciones deben transponer la disposición correspondiente a sus regímenes jurídicos nacionales, lo que permitirá que los tribunales nacionales puedan procesar las actividades de los mercenarios.

D. Derecho indicativo e iniciativas en curso

54. Además de los marcos jurídicos internacionales vinculantes, en el último decenio han surgido una serie de iniciativas multilaterales y de múltiples partes interesadas que se dirigen a diferentes agentes y tratan de fomentar el comportamiento responsable durante el uso de la tecnología de la información y las comunicaciones. Entre ellas se encuentran los marcos normativos no vinculantes dirigidos a los agentes privados, como el Cybersecurity Tech Accord y la Charter of Trust instaurada por Siemens. Los grupos de expertos independientes, como la Comisión Mundial sobre la Estabilidad del Ciberespacio y el Grupo Independiente de Expertos que redactó el *Tallinn Manual*, elaboraron recomendaciones sobre las normas y el derecho internacional aplicable. Otras iniciativas de múltiples partes interesadas, como el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio, se han dirigido al sector privado, la sociedad civil y los Gobiernos.

55. En el Consejo de Derechos Humanos, un grupo de trabajo intergubernamental de composición abierta desempeña una función importante a la hora de elaborar el contenido de un marco regulatorio internacional para la regulación, el seguimiento y la supervisión de las actividades de las empresas militares y de seguridad privadas. Debido a la rápida evolución de los contextos operativos y de los servicios prestados, cualquier mecanismo de regulación que se desarrolle a través de este proceso debería hacer referencia a “servicios” o “actividades” en lugar de a “empresas militares y de seguridad privadas” como opciones terminológicas más eficaces para plasmar los abusos de los derechos humanos o del derecho internacional humanitario[46].

[45] Véase la presentación de Access Now, pág. 10.

[46] Véase la declaración de Jelena Aparac, Presidenta del Grupo de Trabajo sobre la utilización de mercenarios. Disponible en www.ohchr.org/EN/HRBodies/HRC/IGWG_PMSCs/Pages/Session2.aspx.

56. La Asamblea General ha establecido dos grupos para examinar cuestiones generales de seguridad en el ámbito de la tecnología de la información y las comunicaciones que podrían proporcionar orientación al respecto: el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (véase la resolución 73/27 de la Asamblea General) y el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional (véase la resolución 73/266 de la Asamblea General). En ambos procesos se analizan seis ámbitos principales, entre los que se incluyen las amenazas existentes y potenciales; las normas, las reglas y los principios de comportamiento responsable de los Estados; el derecho internacional; las medidas de fomento de la confianza; la creación de capacidad; y el diálogo institucional periódico.

57. En marzo de 2021, el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional aprobó por consenso un informe en el que se resumían algunas recomendaciones no vinculantes para todos los Estados Miembros. Aunque ninguna de las recomendaciones aborda la cuestión de los mercenarios o de los agentes relacionados con ellos, el informe contiene varias referencias a los derechos humanos, y se reconoce el hecho de que algunos agentes no estatales han demostrado tener capacidades en materia de tecnología de la información y las comunicaciones que antes solo estaban al alcance de los Estados. En el informe se señaló que el continuo aumento de los incidentes de uso malintencionado de las tecnologías de la información y las comunicaciones (TIC) por parte de agentes estatales y no estatales era una tendencia preocupante (véase A/AC.290/2021/CRP.2, párr. 16). En su resolución 75/240, de 31 de diciembre de 2020, la Asamblea General decidió organizar un nuevo Grupo de Trabajo de composición abierta hasta 2025 y el Grupo de Trabajo sobre la utilización de mercenarios como medio de violar los derechos humanos y obstaculizar el ejercicio del derecho de los pueblos a la libre determinación considera que ello ofrece una valiosa oportunidad para debatir la cuestión de los mercenarios y los agentes relacionados con ellos que operan en la ciberesfera.

58. En su informe aprobado por consenso de 2021, el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional reafirmó que “los Estados no deben recurrir a terceros para cometer actos internacionalmente ilícitos utilizando las TIC, y deben tratar de garantizar que su territorio no sea utilizado por agentes no estatales para cometer esos actos”[47]. Si bien esto no establece una norma jurídica para los Estados, sí condena la orquestación y la sanción por parte de los Estados a los representantes. El Grupo de Expertos Gubernamentales señaló que las actividades realizadas por los Estados para fomentar el respeto y la observancia de los derechos humanos y garantizar el uso responsable y seguro de las tecnologías de la información y las comunicaciones (TIC) deben ser esfuerzos complementarios, que se refuercen mutuamente y sean interdependientes, al tiempo

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

que reconoció que la vigilancia masiva puede tener efectos negativos en los derechos humanos, incluido el derecho a la privacidad[48].

59. Se ha dicho que las iniciativas normativas emergentes constituyen un "complejo de regímenes" para la ciberseguridad que implica un acuerdo de esfuerzos más que un instrumento jerárquico vinculante.

V. Repercusiones en los derechos humanos

60. Es innegable que las ciberactividades afectan a las normas y reglas de los derechos humanos y tienen la capacidad de causar violaciones tanto en los conflictos armados como en tiempos de paz, y, por lo tanto, de afectar a toda una variedad de derechos. El Grupo de Trabajo recuerda la conclusión de que los riesgos y las repercusiones de género causados por las actividades realizadas por las empresas militares y de seguridad privadas comparten muchas características comunes, independientemente de su tamaño y de los servicios prestados (véase A/74/244, párr. 6). Además, el Grupo de Trabajo ha señalado los grupos que se ven especialmente afectados por los mercenarios y los agentes relacionados con ellos contratados por los Estados, como los defensores de los derechos humanos, los migrantes, los líderes de la oposición y los periodistas, así como las personas lesbianas, gais, bisexuales, transgénero, intersexuales y con identidad de género no conforme en el contexto de la violencia de género.

61. Las formas de guerra nuevas y emergentes pueden tener una repercusión significativa tanto en los objetivos militares como en la población civil y pueden dar lugar a violaciones del derecho internacional humanitario, así como de los derechos y las libertades de las personas en el contexto de los conflictos armados y de otro tipo. El Grupo de Trabajo señaló anteriormente que la ciberguerra ha sido reconocida como un método de guerra que no solo permite infiltrarse, perturbar, dañar e incluso destruir bienes de carácter militar o civil, sino que también puede causar graves daños humanos[49]. El cibersabotaje puede tener grandes efectos secundarios en el funcionamiento de la infraestructura crítica, lo que puede debilitar la salud pública y la seguridad. En este contexto, el derecho a la vida y el derecho a no ser sometido a torturas y otros tratos inhumanos o degradantes son los principales derechos que corren el riesgo de vulnerarse en las ciberoperaciones.

Derecho a la privacidad y la libertad de expresión

62. En todos los contextos, existe el riesgo de vulnerar el derecho a la privacidad y el derecho a la libertad de expresión. Cuando se designa a los mercenarios y los agentes relacionados con ellos para atacar a los Estados, se convierten invariablemente en las herramientas fundamentales para debilitar la soberanía y la integridad territorial de dichos Estados, lo que también impide el ejercicio del derecho a la privacidad.

63. El derecho a la privacidad también puede verse comprometido por la vigilancia y la recopilación de información. Existe una gran preocupación por las

[48] *Ibid.*, párrs. 39 y 37.

[49] CICR, "Derecho internacional humanitario y ciberoperaciones durante conflictos armados", documento de posición, noviembre de 2019.

ciberoperaciones dirigidas a la sociedad civil y, en particular, a los defensores de los derechos humanos y a los periodistas encaminadas a perturbar sus actividades para sofocar la disidencia y aumentar el control por parte de un Estado sobre su población. Aunque los Gobiernos llevan mucho tiempo empleando diferentes métodos para vigilar y rastrear a sus ciudadanos, los disidentes, los opositores políticos y los defensores de los derechos humanos, las herramientas tecnológicas disponibles en la actualidad, como los programas maliciosos y los programas espía, les permiten hacerlo a un menor costo, así como ampliar el alcance geográfico de la vigilancia y aumentar su ámbito y escala, lo que permite a los Gobiernos llevar a cabo una represión digital más completa que nunca[50]. Ciertas formas de programas espía son ejemplos paradigmáticos de instrumentos que permiten supervisar los objetivos a distancia[51].

64. Además, se ha indicado que el derecho a la libertad de expresión puede verse vulnerado por el control que ejercen algunos Estados sobre los contenidos de Internet o por la difusión de desinformación e información errónea. Las ciberoperaciones subversivas dirigidas o contratadas por clientes gubernamentales pueden socavar la integridad de la ciberesfera, la libertad de expresión y otras libertades civiles no solo de las personas, sino de los grupos y las sociedades en general[52]. La vigilancia selectiva también crea incentivos para la autocensura y menoscaba de manera directa la capacidad de periodistas y defensores de los derechos humanos de llevar a cabo investigaciones, y de forjar y mantener relaciones con fuentes de información[53].

65. Las tecnologías de vigilancia desarrolladas, mantenidas y a veces gestionadas por empresas privadas también influyen de forma decisiva en el cambio en las rutas migratorias, que se alejan de las zonas detectables y se dirigen a aquellas que están fuera del alcance del equipo de vigilancia. Así pues, los migrantes se ven obligados a tomar rutas menos directas y más peligrosas en las travesías migratorias por vía acuática o terrestre, lo que aumenta la dificultad física del desplazamiento, así como los daños fisiológicos y mentales, el dolor y el sufrimiento, que con frecuencia provocan la muerte por insolación, deshidratación severa y otras enfermedades[54].

66. Las repercusiones de las cibercapacidades se traducen en efectos nocivos sustanciales tanto para las instituciones como para las personas, lo que afecta negativamente a la capacidad de los Gobiernos para proporcionar protección y garantizar el bienestar de grandes sectores de la población y obstaculiza el disfrute de los derechos humanos. Los ataques a los sistemas electorales, por ejemplo, repercuten de forma directa en los derechos democráticos fundamentales de representación de los ciudadanos a los que se priva de su derecho de voto. Además, se informó de que algunos países lanzan habitualmente ciberataques contra zonas civiles, con el fin de piratear a las empresas privadas o debilitar a las fuerzas militares extranjeras, mediante el uso de herramientas en línea para manipular la información o la

[50] Véase la presentación de The Citizen Lab, pág. 8.
[51] A/HRC/41/35, párr. 9; Bill Marczak y otros, “Hide and seek: tracking NSO Group’s Pegasus spyware to operations in 45 countries”, Citizen Lab, 18 de septiembre de 2018.
[52] S/2021/569, párr. 103.
[53] Véanse A/HRC/38/35/Add.2, párr. 53; A/HRC/41/35, párr. 26.
[54] A/HRC/45/9, párrs. 44 y 45.

propaganda digital y cambiar las opiniones de los demás y mediante el empleo de mercenarios digitales para llevar a cabo la labor[55].

67. Según se informa, existen ciberataques que causan daños físicos generalizados, incluso en las redes de suministro eléctrico, las instituciones financieras y los ministerios gubernamentales[56]. La destrucción de las bases de datos que contienen información relativa a los civiles podría paralizar rápidamente los servicios gubernamentales y las empresas privadas y, por tanto, causar un mayor daño a los civiles que la destrucción de objetos físicos[57].

Libre determinación

68. En cuanto al derecho a la libre determinación, mediante el uso de productos y servicios militares y de seguridad en el ciberespacio, las empresas de ciberseguridad podrían obstaculizar de forma considerable el ejercicio del derecho de los pueblos a la libre determinación. Estos agentes tienen el potencial de influir en las insurgencias internas por medios que, en última instancia, pueden menoscabar el derecho a la libre determinación (véase A/71/318, párr. 20).

VI. Conclusiones y recomendaciones

69. **El desarrollo y la digitalización de las tecnologías tienen una repercusión directa en todas las esferas de la vida civil. El ámbito militar también depende cada vez más de las tecnologías digitales. La creciente tendencia a la digitalización se refleja en una mayor convergencia del espacio de la información y el ciberespacio y puede tener repercusiones negativas en las poblaciones en tiempos de paz y durante los conflictos armados.**

70. **El Grupo de Trabajo ha analizado la evolución del suministro de productos y servicios militares y de seguridad en el ciberespacio por parte de los mercenarios, los agentes relacionados con ellos y las empresas militares y de seguridad privadas, así como las consecuencias correspondientes para el disfrute de los derechos humanos. Señaló los desafíos que comporta centrarse únicamente en las actividades que se ajustan a la definición de "mercenario" según el marco jurídico internacional aplicable y adoptó un enfoque más amplio consistente en examinar una variedad de agentes y manifestaciones que encajaban en un concepto más adaptable de las actividades relacionadas con el mercenarismo.**

71. **El Grupo de Trabajo observó con preocupación que algunos Estados, ya sea por comisión u omisión, ocultan su participación en ciberoperaciones maliciosas, y tratan de obtener influencia militar estratégica eludiendo sus responsabilidades en virtud del derecho internacional, incluidas las relativas a**

[55] Paul D. Shinkman, "America Is losing the cyber war", sitio web de U.S. News and World Report, 29 de septiembre de 2016. Disponible en 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 de agosto de 2018. Disponible en https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/.

[57] CICR, "Derecho internacional humanitario y ciberoperaciones durante conflictos armados", documento de posición, noviembre de 2019.

las violaciones y los abusos cometidos por agentes no estatales contratados para este fin. Sin embargo, la contratación de agentes privados para prestar servicios militares y de seguridad en el ciberespacio no exime a los Estados de sus obligaciones en virtud del derecho internacional.

72. **Por consiguiente, las manifestaciones nuevas y en evolución de los agentes relacionados con el mercenarismo exigen la atención urgente de los Estados y otros interesados pertinentes. En el presente informe se proporcionan consideraciones que deben tenerse en cuenta para apoyar a los Estados y otros agentes a la hora de regular a las actividades de los agentes en el ciberespacio de manera más eficaz, con miras a garantizar el respeto, la protección y el cumplimiento del derecho de los pueblos a la libre determinación, proteger a los civiles en situaciones de conflicto armado y salvaguardar los principios de no intervención y de integridad territorial. Los debates en torno a la regulación deberían basarse en el marco jurídico internacional relativo a los mercenarios, a pesar de sus deficiencias, y en el marco general de la legislación internacional humanitaria y de derechos humanos.**

Recomendaciones

73. **A fin de prevenir y mitigar los efectos negativos para los derechos humanos causados por los mercenarios y los agentes relacionados con ellos y las empresas militares y de seguridad privadas en el ciberespacio, los Estados deberían abstenerse de reclutar, utilizar, financiar y entrenar a mercenarios y deberían prohibir esa conducta en su legislación nacional y regular de manera eficaz las empresas militares y de seguridad privadas.**

74. **Los Estados deberían garantizar y poner en práctica la transparencia en lo que respecta a la contratación de servicios de apoyo militar, incluso en las ciberoperaciones, y hacer pública la información sobre la naturaleza de los servicios, los procedimientos de contratación, las condiciones de los contratos y los nombres de los proveedores de servicios de manera suficientemente detallada y oportuna. No deberían emplear preocupaciones de seguridad nacional como justificación general para restringir el acceso a esa información; por el contrario, toda limitación del acceso a la información debe reunir las condiciones de ser legal, necesaria y proporcional, en consonancia con el derecho a la libertad de expresión.**

75. **Los Estados deben investigar, juzgar y sancionar las presuntas violaciones del derecho internacional humanitario y los abusos contra los derechos humanos cometidos por mercenarios, agentes relacionados con ellos y empresas militares y de seguridad privadas, y proporcionar recursos eficaces a las víctimas. En las investigaciones, los procesos y los juicios, se debe respetar y garantizar el derecho a un juicio imparcial y al debido proceso.**

76. **En el plano internacional, los Estados deberían entablar un diálogo sobre las formas nuevas y en evolución de los mercenarios y, en particular, aquellos que actúan en la ciberesfera en todas sus formas, los riesgos que plantean para el derecho internacional humanitario y las normas de derechos humanos y las formas de abordarlas y contrarrestarlas con mayor eficacia. En todo diálogo de esa índole deberían participar organizaciones internacionales y regionales, la**

sociedad civil y expertos, y se deberían examinar los instrumentos e iniciativas existentes.

77. **Los Estados deberían revitalizar las conversaciones con el grupo de trabajo intergubernamental de composición abierta encargado de elaborar el contenido de un marco regulatorio internacional para la regulación, el seguimiento y la supervisión de las actividades de las empresas militares y de seguridad privadas[58], incluso en los casos en los que prestan ciberservicios y actúan en el contexto de la ciberguerra. Se necesita un instrumento jurídicamente vinculante que regule el ciberespacio. Un marco jurídico internacional aportaría seguridad y previsibilidad a través de obligaciones jurídicas claras que pueden hacerse cumplir mediante foros especializados en la resolución de conflictos. La fragmentación de los regímenes de gobernanza fomenta la confusión normativa y a menudo perjudica a los países en desarrollo y a los agentes de la sociedad civil.**

78. **El Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional deberían examinar más en profundidad las preocupaciones en materia de derechos humanos derivadas de la participación de mercenarios y agentes conexos en las ciberoperaciones.**

79. **En lo que respecta a las actividades de los mercenarios, los agentes relacionados con ellos y las empresas militares y de seguridad privadas asociadas con agentes no estatales armados, los Estados deberían acordar y apoyar procesos internacionales para determinar, evaluar y seguir desarrollando mecanismos para reconocer más clara y oficialmente las obligaciones internacionales en materia de derechos humanos de los agentes no estatales armados, incluidos criterios para determinar la capacidad de estos últimos de cumplir sus obligaciones en materia de derechos humanos.**

[58] Véase la resolución 36/11 del Consejo de Derechos Humanos.