**Llamado a contribuciones: informe sobre provisión de productos y servicios militares y de seguridad en el ciberespacio por los “mercenarios cibernéticos”**

|  |  |
| --- | --- |
| **Fecha límite:** | 12 de febrero de 2021 |
| **Issued by:** | Grupo de trabajo sobre la utilización de mercenarios |
| **Propósito:** | Informar el informe del GT que se presentará el 76º período de sesiones de la Asamblea General en octubre de 2021 |

**Contexto**

Dos veces al año, el Grupo de Trabajo sobre la utilización de mercenarios solicita aportaciones para fundamentar sus estudios temáticos que se presentan en el Consejo de Derechos Humanos en su período de sesiones de septiembre y en la Asamblea General en octubre.

**Objetivos del informe**

El Grupo de Trabajo sobre la utilización de mercenarios identificó a los “ciber mercenarios” como una categoría de actores que realizan actividades relacionadas con los mercenarios. Esto implica una amplia gama de servicios militares y de seguridad prestados en el ciberespacio, incluida la recopilación de datos y el espionaje. Los Estados y los agentes no estatales pueden contratar agentes privados no solo para proteger sus propias redes e infraestructuras sino también con el objetivo de debilitar la capacidad militar de las fuerzas armadas enemigas o socavar la integridad del territorio de otro Estado. Las personas que llevan a cabo ciberataques puede causar daños de forma remota, a través de varias jurisdicciones. Por lo tanto, se puede considerar que realizan una actividad relacionada con los mercenarios, o incluso una actividad mercenaria si se cumplen todos los criterios de calificación.

Este estudio temático sobre la *provisión de productos y servicios militares y de seguridad en el ciberespacio por mercenarios cibernéticos y actores relacionados y su impacto en los derechos humanos* tiene por objeto evaluar cómo los mercenarios y los actores privados se benefician del desarrollo, mantenimiento y operación de las capacidades cibernéticas, que pueden utilizarse en conflictos armados y en entornos sin conflicto para violar los derechos humanos, incluido el derecho a la autodeterminación.

**Ámbito de estudio y preguntas clave**

El Grupo de Trabajo agradece las aportaciones de los Estados, organizaciones de la sociedad civil, académicos, organizaciones internacionales e intergubernamentales, instituciones nacionales de derechos humanos, empresas privadas, personas y cualquier otro actor interesado.

Si bien el Grupo de Trabajo agradece cualquier información que se considere pertinente al tema, está particularmente interesado en las áreas mencionadas a continuación. Al abordar las preguntas, proporcione **ejemplos, buenas prácticas y recomendaciones**, en la medida en que estén disponibles, que considere importantes en el contexto de este cuestionario, así como cualquier análisis sobre desarrollos futuros en esta área.

Tendencias y desarrollos actuales

1. ¿Quiénes son los clientes y/o beneficiarios de las capacidades y operaciones cibernéticas?

*Esto puede incluir, por ejemplo, actores estatales y no estatales que contratan “mercenarios cibernéticos” y otros actores que operan solos o a través de empresas militares y de seguridad privadas (EMSP) para adquirir capacidades cibernéticas, incluidos productos y servicios militares y de seguridad.*

1. ¿Cuál es el papel de los actores que operan solos o a través de EMPS, en a) desarrollar, b) mantener, c) vender, d) proporcionar capacidades cibernéticas (incluidos los productos o servicios militares o de seguridad cibernéticos) a terceros, o e) realizar ciberespionaje?
2. ¿Cuáles son los factores de motivación y las intenciones estratégicas de: a) los clientes para reclutar “mercenarios cibernéticos” y el tipo de relaciones que pueden tener con ellos; y b) los “mercenarios cibernéticos” y otros actores que operan solos o a través de EMPS en el espacio cibernético?

*Los factores motivacionales pueden incluir, por ejemplo, ganancia privada, compensación material, razones ideológicas y de otro tipo*.

1. ¿Cuáles son los tipos de servicios y productos cibernéticos disponibles (por ejemplo, software espía/malware, inteligencia artificial), incluido su propósito previsto tanto en situaciones de conflicto como de no conflicto?
2. ¿Qué papel juegan las nuevas tecnologías para causar daño de forma remota en el contexto de las operaciones cibernéticas y cuáles son los riesgos involucrados? ¿Cómo definiría “participar directamente en las operaciones cibernéticas”?

Marcos normativos y su aplicación

1. Sírvanse proporcionar información sobre los marcos legislativos, normativos y reglamentarios nacionales, regionales o internacionales (o a nivel internacional) con respecto a la conducta en el ciberespacio y su aplicación (por ejemplo, transparencia, comportamiento responsable).
2. Sírvanse proporcionar información sobre las normas y/o reglamentos específicos nacionales o regionales que rijan la provisión de productos y servicios de seguridad en el ciberespacio por actores que operan solos o a través de EMPS, y otros actores pertinentes.
3. Sírvanse proporcionar información sobre los marcos y mecanismos nacionales, regionales o internacionales existentes para investigar y responsabilizar a las personas, grupos, Estados o empresas por abusos en el ciberespacio, incluidos el espionaje, las operaciones, los servicios o productos cibernéticos ilegales, y su eficacia.

Impactos de las operaciones y capacidades cibernéticas realizadas por actores que operan solos o a través de EMSP en los derechos humanos y el DIH

1. Sírvanse describir cómo el desarrollo y el uso de capacidades, operaciones y servicios cibernéticos (por ejemplo, ataques a la infraestructura y datos digitales/físicos, vigilancia de personas) por actores que operan solos o a través de EMSP pueden causar y contribuir a abusos y violaciones de los derechos humanos en entornos sin conflictos.

*Esto incluye, por ejemplo, los derechos a la vida, a la integridad física y mental, a la autodeterminación, a la privacidad, a la salud, al voto, así como a la libertad de movimiento, de reunión y de asociación que podrían estar afectando a personas o grupos, como los defensores de derechos humanos, líderes de la oposición o periodistas.*

1. Sírvanse describir cómo el desarrollo y el uso de capacidades, operaciones y servicios cibernéticos por actores que operan solos o a través de EMSP pueden causar y contribuir a infracciones del derecho internacional humanitario durante los conflictos armados.

**Cómo y dónde enviar las contribuciones**

Las contribuciones pueden enviarse por correo electrónico, en formato accesible (documento Word), a [mercenaries@ohchr.org](mailto:mercenaries@ohchr.org), a más tardar el **12 de febrero de 2021**. Al enviar su respuesta, indique amablemente si tiene alguna objeción con respecto a que su respuesta se publique en este sitio web.

**Cómo se utilizarán las contribuciones**

Todas las contribuciones recibidas en formato Word se publicarán en esta página web, a menos que el remitente indique claramente que no desea que sus comentarios se hagan públicos al enviar su respuesta. Las contribuciones recibidas en formato PDF no se publicarán, pero estarán disponibles a pedido.