Fuerza Aérea de Chile
Centro de Estudios Estratégicos y Aeroespaciales
Estrategia, Aeronáutica, Espacio, Tecnología & Innovación

BOLETÍN INFORMATIVO Y DE ANÁLISIS N° 46-2019 Santiago, 06 de JUNIO del 2019

Ciberguerra y Derecho Internacional Humanitario

Como todo cuerpo legal, el Derecho Internacional Humanitario (DIH) ha evolucionado conforme avanza la sociedad y los estados; la forma de hacer la guerra y la tecnología empleada en esta, por lo tanto, posterior a la firma del primer acuerdo, le sucedieron otros tres, que no hicieron más que perfeccionar los acuerdos adoptados con anterioridad, llegando incluso a comprender a la población civil en tiempo de guerra. El último acuerdo incorporado a los convenios de Ginebra fue durante el año 1950.

Diversos académicos han cuestionado la aplicabilidad del DIH en las acciones militares mediante operaciones de ciberguerra; sin embargo, el Comité Internacional de la Cruz Roja (ICRC por sus siglas en inglés), organización que nace junto con el Convenio de Ginebra y que tiene por objetivo brindar protección y asistencia humanitaria a las víctimas de conflictos armados, indica que la ciberguerra tiene límites y reglas, señalando también que la infraestructura informática civil se encuentra protegida de los ciberataques[1]. (ICRC, 2013)

Esta organización, para afirmar lo anterior, hace referencia al Manual Tallinn publicado en 2013 por Cambridge University Press, el cual fue elaborado por un grupo de expertos internacionales en el ámbito legal y militar, proceso en el cual la ICRC participó como observador a fin de verificar que el espíritu detrás de los convenios de Ginebra y del DIH fueran considerados.

Dicho manual, si bien no es vinculante, pretende ser una guía para que los Estados sigan discutiendo sobre el asunto, pudiendo incluso perfeccionarse aún más los convenios de Ginebra.

Sobre el Manual Tallinn

Para establecer una conexión entre la ciberguerra y el derecho internacional humanitario, el Manual indica que es necesario comprender, en primer lugar, los conceptos, *jus ad bellum* y *jus in bello.* El primero está relacionado con el derecho internacional de los estados a usar la fuerza como parte de su política y el segundo con el derecho internacional que regula la conducción del conflicto armado, también llamado Leyes de la Guerra o Derecho Internacional Humanitario.

En segundo lugar, es necesario comprender también que un ataque cibernético podrá ser considerado o no acto de guerra dependiendo de las circunstancias en las cuales se ejecuta, ya que no siempre puede ser atribuido a un Estado, aun cuando la primera impresión así lo haga parecer.

El manual, dentro de su estructura, realiza un análisis comparativo entre las definiciones acordadas para los conceptos de ciberguerra, ciberataque, ciberespacio, describiendo sus medios y objetivos. Además, realiza un análisis de cómo el Derecho Internacional, la Carta de las Naciones Unidas y el Derecho Internacional Humanitario pueden ser aplicados a diversas situaciones de la ciberguerra y los ciberataques.

Considerando la extensión y profundidad definidas para el presente trabajo, a continuación, sólo se describen las principales conclusiones a las cuales llega el grupo de expertos que elaboró el Manual, dejando de manifiesto que el análisis jurídico que las sustenta se encuentra detallado en el cuerpo del manual:

- Un Estado puede ejercer control sobre la infraestructura cibernética y las actividades dentro de su territorio soberano, lo cual no significa que pueda ejercer soberanía en el ciberespacio en sí, pero si por la ciber infraestructura que se encuentre en su territorio, entendiéndose esta última por los recursos de comunicaciones, almacenamiento y hardware sobre los que operan los sistemas de información.
- Durante un conflicto armado internacional, la ley de neutralidad también rige los derechos y obligaciones de los Estados con respecto a la infraestructura y las operaciones cibernéticas, entendiéndose estas últimas como el empleo de capacidades cibernéticas con el propósito de lograr objetivos mediante el uso del ciberespacio.
- Cualquier interferencia de un estado con infraestructura cibernética a bordo de una plataforma, donde sea que se encuentre, mientras goza de inmunidad soberana, constituye una violación de la soberanía.
- El mero hecho de que se haya iniciado una operación cibernética en una infraestructura cibernética gubernamental no es evidencia suficiente para atribuir la operación a otro Estado, sino que es una indicación de que ese otro Estado en cuestión podría estar asociado con la operación.

[1] Entendiéndose dentro del plano legal, y en especial del DIH.

- Un ataque cibernético es una operación cibernética, ya sea ofensiva o defensiva, que razonablemente se espera que cause lesiones o la muerte a personas o daños o destrucción de objetos.
- Una operación cibernética constituye uso de la fuerza cuando su escala y efectos son comparables a las operaciones no cibernéticas que se elevan al nivel de "uso de la fuerza".
- Una operación cibernética que constituya una amenaza contra la integridad territorial o la independencia política de cualquier Estado, o que sea de cualquier otra manera incompatible con los propósitos de las Naciones Unidas, es ilegal.
- Un Estado que es blanco de una operación cibernética elevada al nivel de un ataque armado o uso de la fuerza, puede ejercer su derecho inherente de legítima defensa. Si una operación cibernética constituye o no un ataque armado depende de su escala y efectos.
- Las medidas relacionadas con operaciones cibernéticas emprendidas por los Estados en ejercicio del derecho de legítima defensa, de conformidad con el Artículo 51 de la Carta de las Naciones Unidas, deberán ser informadas inmediatamente al Consejo de Seguridad de las Naciones Unidas.
- Si el Consejo de Seguridad de las Naciones Unidas determina que un acto constituye una amenaza para la paz, una violación de la paz o un acto de agresión puede autorizar medidas coercitivas, incluidas las operaciones cibernéticas. Si el Consejo de Seguridad considera que tales medidas son inadecuadas, puede decidir sobre medidas más fuertes, incluidas las medidas de fuerza tradicional.
- Existe un conflicto armado internacional siempre que haya hostilidades, que pueden incluir o limitarse a operaciones cibernéticas, que se producen entre dos o más Estados.
- Los comandantes y otros superiores son responsables penalmente de ordenar operaciones cibernéticas que constituyen crímenes de guerra.
- Los comandantes también son penalmente responsables si sabían o, debido a las circunstancias del momento, debían saber que sus subordinados estaban cometiendo, estaban a punto de cometer o habían cometido crímenes de guerra y no tomaron todas las medidas razonables y disponibles para prevenir su comisión o para castigar a los responsables.
- La población civil, así como los individuos civiles, no deben ser objeto de ciberataques.
- Los ataques cibernéticos, o la amenaza de usarlos, cuyo propósito principal es difundir el terror entre la población civil, están prohibidos.
- Los objetos civiles son todos los objetos que no son objetivos militares. Los objetivos militares son aquellos objetos que, por su naturaleza, ubicación, propósito o uso, contribuyen de manera efectiva a la acción militar y cuya destrucción, captura o neutralización total o parcial, en las circunstancias que rigen en ese momento, ofrecen una ventaja militar definitiva. Los objetivos militares pueden incluir computadoras, redes de computadoras e infraestructura cibernética.
- Los objetos civiles no serán objeto de ciberataques. Las computadoras, las redes de computadoras y la infraestructura cibernética pueden ser objeto de ataques si son objetivos militares.

El trabajo realizado por el grupo de expertos corresponde a una interpretación de las normas antes mencionadas manteniendo el espíritu original del Derecho Internacional Humanitario, que no es otro que evitar y limitar el sufrimiento humano durante los conflictos armados, por lo tanto, tiene un alto valor para los estados que deseen profundizar en la materia y presenten mociones para actualizar formalmente las normas actuales en el seno de los organismos internacionales.

Al finalizar este trabajo, queda la sensación que el DIH es aplicable a la guerra cibernética. Sin embargo, aún no se aclara una serie de situaciones que harán en un momento dado, cuestionarse su utilidad y que tienen relación con la demostración concreta de si un determinado ataque provino o no desde un Estado, o más bien fue un acto criminal donde el DIH no opera. Además, si se demostrara que fue un acto hostil desde otro Estado ¿de qué forma se puede aplicar una acción de defensa proporcional, donde una opción sería degradar la capacidad enemiga para conducir ciberataques, si lo más probable es que se haya materializado desde un tercer país del cual solo usaron su territorio y conexiones?

¿Cómo es posible distinguir a un combatiente cibernético, al cual se le pueda neutralizar físicamente por la fuerza cinética?

Sin duda, las ciberoperaciones nos plantean una serie de desafíos desde el punto de vista legal, pudiendo fácilmente mimetizarse con los conceptos de guerra hibrida o terrorismo, quedando nuevamente la interrogante de cuando determinar si un determinado ciberataque es un acto de guerra o un acto criminal.

Las discusiones y desencuentros entre los teóricos seguirán sucediendo en este terreno, toda vez que muy probablemente no solo haya nuevas herramientas para hacer la guerra, sino que hoy es válido preguntarse si las dimensiones espacio temporales de la guerra en sí misma, siguen estando vigentes, o tal vez sea necesaria una revisión más profunda a la "corporalidad" del espíritu del DIH, toda vez que este último se mantiene vigente.

CDG (AD) FRANCISCO CARVAJAL MOLINA

Bibliografía

BBC. (2015, octubre 11). *BBC NEWS*. Retrieved from https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Cambrige University Press. (2019, Abril). *Cambridge Dictionary*. Retrieved Abril 2019, from https://dictionary.cambridge.org

ICRC. (2013, Junio). *International Committee of the Cross Red.* Retrieved from https://www.icrc.org