LA CIBERGUERRA Y EL DERECHO INTERNACIONAL HUMANITARIO

CDG (AD) FRANCISCO CARVAJAL MOLINA

La aplicabilidad del Derecho Internacional Humanitario en la ciberguerra y las ciberoperaciones.

CDG (AD) Francisco Carvajal M. (*)

En la planta nuclear de Chai Wan (Hong Kong), durante el año 2015, las bombas de refrigeración del reactor principal fallaron a tal punto que generaron una gran explosión por sobrecalentamiento, dejando cientos de muertos y heridos. El gobierno Chino inició una investigación y determinó que el "accidente" se debió al ataque cibernético que infectó el software principal de la planta, perdiendo los encargados el control total del sistema de seguridad, permitiendo a los perpetradores del ataque, apagar "a distancia" las bombas de refrigeración. Se descubrió que la acción fue cometida a miles de kilómetros de China mediante un RAT (*Remote Access Tool*) y que detrás existía toda una red de espionaje e infiltración por parte de gobiernos extranjeros, por lo tanto, la acción criminal prontamente se convirtió en una agresión militar que generó una crisis quedando el país *ad-portas* de un conflicto bélico.

Lo descrito anteriormente, es el tema central de la película *BlackHat* y aun cuando es toda una trama de ciencia ficción, los elementos técnicos usados en el ataque son reales y funcionan, como también lo es la voluntad que pudiera tener un Estado, o una organización, para infligir un daño bastante potente en la infraestructura crítica de un país, trasladando el conflicto bélico a una nueva dimensión espacial denominada *ciberespacio,* y como en toda guerra, existirá sufrimiento humano, daño colateral y víctimas civiles.

Dentro de este contexto es válido preguntarse si los mecanismos que ha diseñado la humanidad para aminorar el sufrimiento humano en los conflictos armados, independiente si es un combatiente o no, son aplicables en una ciberguerra, donde al parecer existiría un campo de batalla virtual y serían los computadores los que se enfrentarían en un combate digital.

Por lo anterior, el propósito de este trabajo se encuentra orientado a efectuar una breve descripción de qué se entiende por ciberguerra en el contexto actual, como se desarrollan las operaciones militares de ciberguerra y cuales son, o podrían ser, las consecuencias para el ser humano que hicieran necesarias aplicar el Derecho Internacional Humanitario y, por último, verificar si, *lex lata,* el ser humano se encuentra protegido o es necesario una *lex ferenda* en esta materia.

¿Qué se entiende por ciberguerra?

Como todo concepto social, encontrar una sola definición para ciberguerra es difícil, sin embargo, se encuentra ampliamente aceptado por el mundo militar, tanto así que ha sido plasmado en diversos textos académicos, operativos y legales, de hecho, Estados Unidos cuenta con una Doctrina de Operaciones en el Ciberespacio[1].

En el ámbito civil, el diccionario de Cambridge establece que ciberguerra[2] es:

> *La actividad de usar el internet para atacar a los computadores de un país con el objeto de dañar cosas como las comunicaciones y el sistema de transporte o los suministros de agua y electricidad: El uso de la ciberguerra puede desestabilizar el sistema financiero, de telefonía o la red energética.*
>
> *La ciberguerra ha cambiado fundamentalmente la seguridad nacional porque un ataque puede venir desde cualquier lugar.* (Cambrige University Press, 2019)

De la definición anterior, ya es posible advertir que, como toda operación militar, la ciberguerra

[1] Joint Publication 3-12 "Cyberspace Operations", del 08 de junio de 2018.

[2] Cambridge define Cyberwarfere, que, para efectos del presente trabajo, se entenderá como ciberguerra.

y sus respectivas operaciones, busca lograr un "efecto deseado", derivándose de esto el blanco a atacar, por lo tanto, lo importante no es si el blanco es destruido, neutralizado o degradado, sino que cause cierta condición en el enemigo. En ese orden de ideas, y tal como lo establece Cambridge, lo que se busca mediante las operaciones de ciberguerra es generar un cierto nivel de daño en algún sistema crítico del enemigo, que lo obligue a tomar determinadas acciones en favor del atacante o le produzca algún grado de vulnerabilidad que le permita al atacante continuar con lo planificado en su diseño operacional, no diferenciándose en lo conceptual de

cualquier operación militar tradicional.

Una vez aclarado lo anterior, se está en condiciones de establecer que la ciberguerra es el término acuñado para diferenciar dentro de un contexto general, al conjunto de operaciones que utilizan las herramientas del espectro informático, operando en el interior del ciberespacio, para atacar a un enemigo, entendiéndose el ciberespacio como aquel espacio "no físico" compuesto por las redes de información que utilizan los computadores y sistemas informáticos[3] para conectarse y comunicarse entre si.

Es necesario precisar que a lo menos existen dos grandes clasificaciones donde es posible enmarcar las operaciones de ciberguerra: Aquellas que buscan entrar a un sistema informático para inutilizarlo, bloquearlo o saturarlo; y aquellos que buscan entrar al sistema para controlarlo y ejecutar acciones sin que los administradores puedan darse cuenta y menos evitarlas.

Si bien estas operaciones utilizan el campo de batalla "virtual", buscan generar un efecto en el terreno físico, como se explicará en los ejemplos que a continuación se mencionan.

El 12 de septiembre de 2018 se activó en el mundo entero un virus informático llamado *wanna cry*, que encriptaba la información de los computadores haciéndolos inaccesibles para sus usuarios, pidiéndoles a cambio un pago en cryptomonedas[4] para su desbloqueo.

Si bien es cierto, el ataque fue estrictamente virtual, el servicio de salud de Inglaterra se vio fuertemente afectado toda vez que los sistemas para agendar citas médicas colapsaron debiendo ser canceladas alrededor de 19.000 de ellas, produciendo millones de libras en H/H perdidas, además de las molestias para los usuarios. También se detectaron fallas en el sistema de semáforos y red de metro en algunas ciudades de Rusia generando caos vial, como también bloqueos en los servidores de las empresas españolas Telefónica, Gas Natural e Iberdrola, sin mencionar en detalle los efectos físicos para los usuarios.

Otro ejemplo que pudo haber generado consecuencias desastrosas, fue la destrucción física de cientos de centrifugas de la central nuclear iraní Natanz el año 2010, mediante la inyección de un virus informático en su red que tomó el control de las centrifugas, acelerándolas y frenándolas de forma errática hasta el punto de producirles un daño físico. Cabe destacar que los técnicos presentes en dicho evento, al percatarse de lo que sucedía, no fueron capaces de desconectarlas de forma manual toda vez que el virus también había inhabilitado los sistemas de emergencia. Este es considerado el primer ataque cibernético concebido específicamente para generar un daño físico de forma directa e inmediata, llegando incluso a denominar al virus informático como una *cyberweapon.* Las investigaciones estiman, sin que llegue a confirmarse a la fecha, que el ataque habría sido una acción de sabotaje planificado y ejecutado por los gobiernos de Estados Unidos e Israel

[3] Entiéndase sistema informático al conjunto completo de software y hardware, relacionados entre si, que tienen el propósito de procesar información para ser utilizada en diversas áreas, como seguridad, toma de decisiones, control de sistemas de producción, comunicaciones, transporte, etc.

[4] Tipo de dinero virtual que existe sólo en el ciberespacio. En la actualidad, esta comenzando poco a poco ser validado por entidades financieras, pero no de forma generalizada.

para detener el programa nuclear iraní. (BBC, 2015)

Como es posible advertir solo en estos dos ejemplos, existiendo miles de casos mas, que un ciberataque puede generar un daño físico a la infraestructura crítica de cualquier país, o bien generar tal nivel de inutilización de sus sistemas informáticos, que, sin producirle un daño físico directo, pueda generar un caos de grandes proporciones que, por acción indirecta produzca un daño físico.

Como ejemplos hipotéticos de inutilización de sistemas informáticos, se podría mencionar un ciberataque que produzca la inhabilitación de los sistemas de control ferroviario de cualquier país de Europa[5], aparejado también por la degradación de los sistemas de comunicaciones que les impida a los controladores a ejecutar de forma segura un plan de contingencia. Una situación como la descrita, incrementaría de forma importante las probabilidades de ocurrencia de un accidente que implique daño material y pérdida de vidas humanas.

Otro ejemplo dentro de un contexto de conflicto bélico, es la intervención del sistema de Mando y Control de cualquier fuerza militar, mediante la inyección de un virus informático programado para entregar datos erróneos, pero creíbles, respecto de la actividad enemiga, lo cual podría generar confusión y una mala toma de decisiones que le permita al enemigo actuar libremente en determinadas circunstancias.

Comprobado que la ciberguerra puede producir daño físico, ya sea de forma directa o indirecta, y no solo a fuerzas militares, sino que a la infraestructura critica de un país, que, en caso de atacarse, podría generar un daño importante a la población civil, como lo podría ser un ciberataque a los centros de control de tráfico aéreo que produzcan el accidente de una aeronave civil; el sabotaje a las centrales hidroeléctricas que priven de suministro eléctrico a ciudades enteras; etc., es necesario analizar la pertinencia del Derecho Internacional Humanitario en este contexto.

En primer lugar, es necesario recordar que el Derecho Internacional Humanitario (DIH) nació para evitar y limitar el sufrimiento humano en caso de conflicto armado, regulando una serie de acciones, tácticas y uso de armamento, consagrándose como parte del Derecho Internacional. Aun cuando sus orígenes los podemos encontrar incluso en la historia hispánica de américa latina, cuando se firmó el "Tratado de Armisticio y Regularización de la Guerra", entre la Gran Colombia y el Reino de España en 1820, donde una de sus cláusulas establecía que las partes en disputa acordaban hacer la guerra *"como lo hacen los pueblos civilizados"* acordando el intercambio de prisioneros y acabar con la guerra a muerte, son los tratados de Ginebra a partir de 1864, su fuente de mayor trascendencia. Estos tratados marcan el inicio formal de este tipo de derecho, teniendo como factor común el concepto que existe detrás del nombre del primer acuerdo: *el mejoramiento de la suerte que corren los militares heridos en los ejércitos de campaña.*

Como todo cuerpo legal, el 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 mas 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 se 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 victimas de

[5] Tomando en cuenta la compleja red ferroviaria de ese continente y lo dependiente que son los Estados de ella.

conflictos armados, indica que la ciberguerra si tiene límites y reglas, señalando también que la infraestructura informática civil se encuentra protegida de los ciberataques[6]. (ICRC, 2013)

Esta organización, para afirmar lo anterior, hace referencia al Manual Tallinn publicado en 2013 por Cambridge University Press, el cual fue confeccionado 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 aun mas 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 como el Derecho Internacional, la Carta de las Naciones Unidas y el Derecho Internacional Humanitario pueden ser aplicado a diversas situaciones de la ciberguerra y los ciberataques.

Considerando la extensión y profundidad definidas para el presente trabajo, a continuación, solo 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 sustentan se encuentra detallas 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 si, 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 esta últimas como el empleo de capacidades cibernéticas con el propósito de lograr objetivos en o 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.
- 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.

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

- 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 mas 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 si es aplicable a la guerra cibernética, sin embargo, aun no se aclaran 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 mas bien fue un acto criminal donde el

DIH no opera. Además, si se demostrara que fue un acto hostil desde otro Estado ¿de que forma se puede aplicar una acción de defensa proporcional, donde una opción seria degradar la capacidad enemiga para conducir ciberataques, si lo mas 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 si misma, siguen estando vigentes, o talvez sea necesaria una revisión mas profunda a la "corporalidad" del espíritu del DIH, toda vez que este último se mantiene vigente.

(*) Oficial de la Fuerza Aérea de Chile, alumno del Curso de Estado Mayor de la Armada de Chile año 2019. Su perfil profesional está ligado al área de recursos humanos habiéndose desempeñado en diferentes niveles decisionales de la Institución.

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