Capítulo 6

El Derecho Internacional como marco regulatorio de la ciberguerra

Mario Polloni Contardo[*]

Introducción

El propósito de este capítulo es presentar de una manera ordenada cómo y con qué extensión el Derecho Internacional regula las acciones desarrolladas por diversos actores en el marco de la llamada "ciberguerra". Un primer punto a tratar en este esfuerzo se orienta a distinguir el concepto de ciberguerra respecto de otros que, no obstante perteneciendo a un mismo género, responden a parámetros más amplios y a una naturaleza distinta del que restrictivamente se aplica en el entorno de conflicto armado, y por esta razón a la ciberguerra. Esta distinción se realiza solo en términos descriptivos, toda vez que su intención es dar un contexto a lo esencial del trabajo. Luego se avanza en la presentación de consideraciones y esfuerzos a nivel internacional para desarrollar políticas y cuerpos normativos –en general escasos– que orienten y regulen el uso pacífico del espacio cibernético y lo resguarden de su uso ilegal. A continuación se identifica el marco regulatorio de la ciberguerra en dos dimensiones. La primera está relacionada con el campo propio del *jus ad bellum*, es decir, las condiciones exigidas por el Derecho para que los recursos de la ciberguerra se empleen como medios y métodos de guerra en el contexto de un conflicto armado, y dentro de los cauces permitidos por el orden jurídico; la segunda de estas dimensiones

[*] Mario Polloni Contardo es Teniente Coronel (R) del Ejército de Chile. Oficial de Estado Mayor, Abogado, Pontificia Universidad Católica de Chile, Magíster en Asuntos de Seguridad Nacional, Colegio Naval de Postgrado de Monterrey, EE.UU., Magíster en Derecho Constitucional, Universidad de Talca.

tiene que ver con el *jus in bello*, el cómo se emplean estos recursos en el transcurso del conficto, teniendo siempre en vista el recaudo de bienes jurídicos, sociales y humanitarios que, no importando las causas que llevan a los Estados y actores al uso de la fuerza como medio de resolución de conflictos, deben ser protegidos a todo evento.

En lo particular, el trabajo en su parte final describe los aspectos esenciales del Manual de Tallinn, texto que, como se explicará, constituye el mayor esfuerzo para establecer reglas no vinculantes que establecen el marco para el uso de medios y métodos de ciberguerra en conflictos armados.

De esta manera se pretende dar respuesta a dos preguntas que constituyen imperativos que orientan este trabajo:

¿Qué regulaciones desde el punto de vista jurídico contempla la ciberguerra?

¿Qué consideraciones regulatorias contiene el DICA respecto de la ciberguerra?

Marco conceptual

La ciberguerra se enmarca en el concepto global de ciberseguridad, constituyendo una parte o especie de esta última. La ciberseguridad está orientada a establecer estructuras, procedimientos y mecanismos que permitan, en tiempo de paz y de conflictos, el uso del espacio para fines de desarrollo, a nivel individual como social. En este sentido, los Estados elaboran políticas de ciberseguridad que persiguen estos fines.

En el caso de Chile, la Política Nacional de Ciberseguridad declara como propósitos los siguientes:

- Resguardar la seguridad de las personas en el ciberespacio.
- Proteger la seguridad del país.
- Promover la colaboración y coordinación entre instituciones.
- Gestionar los riesgos del ciberespacio.

Afirma la Política Nacional de Ciberseguridad de Chile que "atendido el carácter global del ciberespacio, los riesgos y amenazas provienen de Chile y del exterior y se originan tanto en causas naturales como en actividades delictuales, por ejemplo, en labores de espionaje y vigilancia llevadas a cabo con diversos fines, afectando la confidencialidad, integridad, disponibilidad de los archivos de información en el ciberespacio, y con ello, los derechos de las personas"[1].

[1] Gobierno de Chile, *Política Nacional de Ciberseguridad 2017-2022,* p. 12.

Del concepto de ciberseguridad, es posible distinguir diversos tipos de amenazas que afectan el uso tranquilo del ciberespacio, que son el cibercrimen, el ciberterrorismo y la ciberguerra[2].

La ciberguerra, tema de interés para este trabajo, se puede definir como "conflicto entre Estados tecnológicamente avanzados, que se realiza mediante ciberataques aisladamente, o como parte de una guerra convencional. No obstante los conflictos y confrontaciones en el ciberespacio pueden no ocurrir en el contexto de una guerra ni en una confrontación general… [corresponde al] conjunto de acciones que se realizan para producir alteraciones en la información y en los sistemas del enemigo, a la vez que se protegen la información y los sistemas del atacante"[3].

Respecto del concepto de ciberguerra, es pertinente afirmar que en esta dimensión "…no es fundamental ni el tiempo, ni el espacio, ni el clima, ni el arsenal, ni el número de tropas, ni la movilización, ni las pérdidas de vidas humanas…el factor central de la ciberguerra radica en encontrar brechas de seguridad para afectar las redes de información y comunicación de otros Estados. Los ataques cibernéticos capitalizan las debilidades que tiene el sistema informático para extraer información estratégica o boicotear procesos vitales para la nación"[4].

Ciberguerra y Defensa

En un interesante trabajo, el investigador Victor Luke desarrolla aspectos que vinculan la infraestructura crítica de orden informática con la necesidad de preservar y defender esta infraestructura de ciberataques, tema que conduce a la ciberguerra como objeto de estudio desde la perspectiva del Derecho[5].

Desde el punto de vista de la infraestructura crítica, señala Luke que "…El satisfactorio funcionamiento de una sociedad moderna supone el eficiente desempeño de una serie de elementos tangibles e intangibles denominada *infraestructura crítica.* Este es un complejo sistema compuesto de

2 Jesús Reguera Sánchez, *Aspectos Legales en el Ciberespacio. La Ciberguerra y el Derecho Internacional Humanitario,* Grupo de Estudios en Seguridad Internacional, GESI, Universidad de Granada, p. 3.

3 Op. cit. Jesús Reguera Sánchez, *Aspectos Legales en el Ciberespacio. La Ciberguerra y el Derecho Internacional Humanitario,* p. 4.

4 Andrés Gaitán Rodríguez, *El Ciberespacio: un nuevo teatro de batalla para los conflictos armados del siglo XXI,* Bogotá, Escuela Superior de Guerra de Colombia, 2012, p. 30.

5 Víctor Luke. Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas. *Revista de Derecho Público, 0* (77), 2012, pp. 405-424. doi:10.5354/0719-5249.2012.30935

mecanismos, servicios, agencias, entes y bienes presentes en un país e incluso, dependiente de factores y elementos ubicados fuera de sus fronteras físicas. Esto hace de la *infraestructura crítica* una compleja red, cuyo comportamiento es difícil analizar y más aun prever"[6]. Agrega Luke que la razón básica que vincula a la Defensa Nacional con la protección de la infraestructura informática de un país radica en que la dependencia tecnológica abre un flanco de vulnerabilidad de enorme envergadura para todo el Estado; y esa vulnerabilidad se acentúa debido a la consolidación de la ciberguerra como una amenaza real a la seguridad de los Estados en el siglo XXI[7]. En este sentido, este autor concluye citando a la revista *Neewsweek Magazine*, "El peligro de un ciberataque es en la actualidad ampliamente reconocido por las sociedades avanzadas, las cuales son completamente dependientes de redes computacionales tanto para el funcionamiento del día a día como para la defensa nacional"[8].

De ahí que se haga necesaria la protección de aquellos "medios electrónicos, que sin ocupar un espacio físico, constituyen el terreno a través del que fluye una creciente cantidad de datos que incluso pueden controlar procesos físicos"[9]. Es por estos medios electrónicos que la ciberguerra y las armas informáticas dirigen su amenaza[10]. Por lo señalado, "las defensas apropiadas para este tipo de amenazas no son las armas convencionales sino las informáticas[11].

Estas consideraciones llevan a Luke afirmar que "…continuar concibiendo a la defensa nacional como una fuerza basada en la posesión de medios disuasivos de carácter físico es mantener una actitud anacrónica. Esto cobra especial relevancia frente a la aparición de amenazas que utilizan armas inmateriales, que se valen de defensas inéditas y que se despliegan en un campo de batalla virtual"[12].

6 Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 409.

7 Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 410.

8 Ibíd.

9 Ibíd.

10 Ibíd.

11 Ibíd.

12 Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 411.

Políticas y marco regulatorio del ciberespacio

El interés por establecer políticas y normas que regulen el uso del ciberespacio y aseguren la seguridad de la información se evidencia con claridad en la década de los 90, y se expresa en la presentación de la Federación Rusa de un proyecto de Resolución (A/RES/53/70) en la Primera Comisión de la Asamblea General de las Naciones Unidas, lo que generó en su momento la conformación del grupo de expertos gubernamentales, con integrantes de Estados Unidos, Rusia y China. A partir de esa fecha, y con mayor fuerza durante la última década, organizaciones regionales como la Organización del Tratado del Atlántico Norte (OTAN) y la Unión Europea han desarrollado iniciativas en términos de políticas y normas para asegurar un uso pacífico o regulado, en el caso de conflictos armados (*jus ad bellum, jus in bello*), del cibersepacio.

En este contexto, con ocasión del 72° período de sesiones de la Asamblea General de Naciones Unidas[13], celebrado durante septiembre de 2017, el ministro de Relaciones Exteriores de la Federación Rusa, Sergei Lavrov, planteó en su discurso ante la Asamblea General la existencia de un vacío de políticas y de normas en materia ciberespacial[14]. En este tema, llamó a rechazar la militarización del ciberespacio; a no permitir que este se convierta en una esfera de confrontación política, y a evitar que se use para infringir presión o daño económico, como diseminar el extremismo e ideologías terroristas. Para avanzar en esos esfuerzos, el canciller llamó a las Naciones Unidas a establecer normas de interés para todos los Estados y de comportamiento responsable en la esfera digital. Concluyó esta autoridad anunciando la preparación de un borrador de una convención universal de lucha contra el crimen cibernético, proponiendo que se comience a revisar en el actual período de sesiones[15].

La exposición del canciller de la Federación Rusa pone en evidencia el vacío normativo internacional en materia de uso pacífico del ciberespacio; por lo que, como se señaló, urge una regulación que satisfaga esta necesidad. Como parte de esta urgencia se inscriben las normas relacionadas con ciberseguridad, ciberdefensa y ciberguerra.

13 Naciones Unidas, Asamblea General, septuagésimo segundo período ordinario de sesiones de la Asamblea General, acceso a Internet el 25 de septiembre, http://www.un.org/es/ga/72/agenda/index.shtml

14 Naciones Unidas, Asamblea General, septuagésimo segundo período ordinario de sesiones de la Asamblea General, discurso del Ministro de Relaciones Exteriores de la Federación Rusa, Sergéi Lavrov, acceso a Internet el 25 de septiembre, , https://www.youtube.com/watch?v=jfMTKr7SGEk

15 Ibíd.

Asimismo, a nivel regional se destaca la existencia de esfuerzos para concordar en políticas y medidas que abordan esta temática en el ámbito de la ciberdefensa. En este contexto, en un ensayo presentado en el VII Congreso del Instituto de Relaciones Internacionales, celebrado en La Plata, República Argentina, entre el 26 y 28 de noviembre de 2014[16], la profesora Candela Justribó expone un estado de situación regional en materia de ciberseguridad y ciberdefensa, Como lo establece la autora, el propósito de su ensayo es "…poder reflexionar y analizar la posibilidad de unificar criterios y lineamientos en torno al rol del Instrumento Militar con respecto a la defensa en el ciberespacio dentro del ámbito de la Unión de Naciones Suramericanas (UNASUR), y su Consejo de Defensa Suramericano"[17].

En el marco señalado, la autora expone que el Plan de Acción correspondiente al 2012 incluyó la conformación de un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa. En esa línea, el Plan de Acción del 2013, también en el eje de "Políticas de Defensa", postuló como actividad a desarrollar el mantenimiento del grupo de trabajo creado el 2012 con el fin de que existiera la posibilidad de "establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa"[18].

Afirma la profesora Justribó que en el marco de la VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de UNASUR, celebrada en Paramaribo, República de Suriname, el 30 de agosto de 2013, se acordó instruir al "Consejo de Defensa Suramericano y al Consejo Suramericano de Infraestructura y Planeamiento (COSIPLAN) a evaluar la cooperación con otros consejos ministeriales competentes y avanzar en sus respectivos proyectos de defensa cibernética y la interconexión entre redes de fibra óptica en nuestros países con vistas a tornar más seguras nuestras telecomunicaciones"[19].

Como resultado de lo anterior, en el marco del Consejo de Defensa Suramericano, las ministras y ministros de Defensa retomaron lo expuesto en Paramaribo y revalidaron lo anunciado por ellos en torno a las amenazas cibernéticas e informáticas. En este sentido, ratificaron la necesidad de avanzar en las coordinaciones regionales en materia de ciberdefensa y aprobaron el Plan de Acción del año 2014, en donde por primera vez se incluyó una

16 Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* ensayo presentado en el VII Congreso del Instituto de Relaciones Internacionales, La Plata, Argentina, 26.27 y 28 de noviembre de 2014.

17 Op. cit., Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* p. 1.

18 Op. cit., Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* pp. 3-4.

19 UNASUR, VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado, Declaración de Paramaribo, numeral 29.

actividad didáctica concerniente a la defensa cibernética y respondiendo a la instrucción de la Declaración de Paramaribo, siendo esta un Seminario Regional de Ciberdefensa[20].

Unido a lo anterior, se conformó la segunda reunión del Grupo de Trabajo de Ciberdefensa (Argentina-Perú-Ecuador), mayo 2017, en el marco del Consejo de Defensa Suramericano, cuyo resultado se resume en cuatro puntos[21].

- Crear un foro regional del grupo de trabajo de ciberdefensa de los Estados miembros, con el fin de intercambiar conocimientos, experiencias y procedimientos de solución.
- Establecer una red de contactos de autoridades competentes para el intercambio de información y colaboración de manera permanente.
- Definir la plataforma y procedimientos de comunicaciones de la red de contactos.
- Profundizar y sistematizar la reflexión acerca de definiciones conceptuales de ciberdefensa y ciberseguridad (Declaración de Cartagena del Consejo de Defensa Suramericano, 2014).

Por último, siempre en el marco regional (UNASUR), el 7 de marzo de 2017 se llevó a efecto la 1ª Reunión Virtual del grupo de trabajo de ciberdefensa (Chile-Ecuador-Perú), con el objeto de "…coordinar los esfuerzos de los Ministerios de Defensa de Chile, Perú y Ecuador para establecer principios compartidos de armonización de criterios, definiciones y estrategias que permitan desarrollar una política de ciberdefensa"[22].

El Derecho y la ciberguerra

Ante la falta de normativa expresa en ciberseguridad, una pregunta que surge en el tema es qué normativa es aplicable a la ciberguerra. Esta pregunta es válida tanto para el ámbito del *jus ad bellum* como en el del *jus in bello.*

En el marco del *jus ad bellum* es posible identificar tres aproximaciones para definir cuándo un ciberataque puede ser calificado como un acto de guerra, por tanto de ciberguerra, y objeto de respuesta legal en el marco de un

20 Op. cit., Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* p. 4.
21 Ibíd.
22 UNASUR, Consejo de Defensa Suramericano, Acta 1ª Reunión Virtual Grupo de trabajo Ciberdefensa CDS-UNASUR, de 7 de marzo de 2017, p. 1.

conflicto armado[23]. La primera es la aproximación universal. Lo más cercano es cuando Naciones Unidas declara una acción cibernética como constituyente de un acto de guerra. La dificultad para llegar a esta declaración es que Naciones Unidas no la ha realizado a la fecha y no existe un tratado universal que diga algo más al respecto. Ante esta situación, es complejo declarar un ciberataque como un acto de guerra[24]. La segunda aproximación es la que define un conjunto de Estados reunidos en una organización, como la que puede realizar la Organización del Tratado del Atlántico Norte (OTAN), pero esta declaración y la consiguiente acción para enfrentarla no ha ocurrido, y pudo haber sido esta la ocasión en el ciberataque a Estonia (2007). De haber reaccionado la OTAN al ciberataque de Estonia por considerarlo ilegal, pudo haber originado una respuesta del atacante según sus propios intereses[25]. La tercera aproximación es la unilateral; un Estado puede declarar que un ciberataque de ciertas características es un acto de guerra, y reaccionar con una respuesta en la misma línea. Si un Estado responde al ciberataque en el contexto de un acto de guerra, se podrá considerar esta como una respuesta legal o no, dependiendo si esta emplea una misma o diferente modalidad de ataque. En todo caso, nada obliga a un Estado a considerar el ciberataque como un acto de guerra[26].

En el marco del *jus in bello*, por su parte el Comité Internacional de la Cruz Roja (CICR) entrega una respuesta más precisa. Si se habla de una ciberguerra (entiéndase ataques informáticos dentro de un conflicto armado) establece el CICR que se debe aplicar la normativa del Derecho Internacional Humanitario; según Cordula Droege (2011), asesora legal del CICR, "El Derecho Internacional Humanitario o DIH solo entra en juego si las operaciones cibernéticas se cometen en el contexto de un conflicto armado, sea entre Estados, entre Estados y grupos armados organizados, o entre grupos armados organizados. Por ende, es preciso distinguir la cuestión general de seguridad cibernética, de la cuestión específica que representan las operaciones cibernéticas en un conflicto armado"[27]. Esta opinión, como se puede comprender, requiere la definición previa que declare un ciberataque como acto de guerra (*jus ad bellum*).

23 Martin C. Libicki, *Cyberdeterrence*, Prepared for the United States Air Force Approved for public release; distribution unlimited, Library of Congress Cataloging-in-Publication Data, 2009 https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG8

24 Ibíd.

25 Ibíd.

26 Ibíd.

27 Cordula Droege, *No hay lagunas jurídicas en el Ciberespacio*, Comité Internacional de la Cruz Roja, 16 de agosto de 2011, acceso en internet el 9 de octubre de 2017, en https://www.icrc.org

Para la asesora legal del CICR, el concepto de la guerra cibernética es un tanto impreciso y, al parecer, su significado varía según quién lo use. En el marco de este debate, a diferencia de las tradicionales operaciones militares cinéticas, la guerra cibernética se refiere a los medios y métodos de guerra que se basan en la tecnología de la información y se usan en el contexto de un conflicto armado en el sentido del derecho internacional humanitario[28]. En ese contexto, las operaciones cibernéticas pueden dar lugar a preocupaciones de índole humanitaria, en particular cuando sus efectos no se limitan a los datos contenidos en el sistema informático o en el ordenador afectado. En efecto, habitualmente se pretende que esas operaciones tengan efectos en el "mundo real". Por ejemplo, al interferir con los sistemas informáticos de apoyo, se pueden manipular los sistemas de tráfico aéreo, los sistemas de oleoductos o las plantas nucleares del enemigo. El potencial efecto humanitario de algunas operaciones cibernéticas es, como se ve, de enorme magnitud. Las operaciones cibernéticas realizadas hasta ahora, por ejemplo, en Estonia, Georgia e Irán, no parecen haber tenido consecuencias graves para la población civil. Sin embargo, al parecer es técnicamente factible interferir con los sistemas de control de los aeropuertos, otros sistemas de transporte, diques o plantas nucleares por medio del ciberespacio[29].

Por consiguiente, no se puede descartar la materialización de escenarios potencialmente catastróficos como la colisión de aeronaves, la emisión de sustancias tóxicas desde plantas químicas, o la perturbación de la infraestructura y los servicios vitales como las redes eléctricas o de abastecimiento de agua. Las principales víctimas de esas operaciones serían, con toda probabilidad, las personas civiles[30].

La inexistencia de un marco normativo aplicable de manera particular a la ciberguerra genera una complejidad representada por las características particulares del tipo de guerra que se libra en el espacio. Como lo recuerda Luke, el solo concepto de arma de guerra utilizado en las normas que regulan el conflicto bélico involucra más bien la idea de instrumentos kinéticos utilizados para atacar o defenderse, cuyos efectos son percibidos por los sentidos y producidos contra objetos corpóreos por medios físicos[31]. En esta materia profundiza: "Desde luego, una bayoneta perforando el pulmón de un soldado de infantería encaja dentro de tal concepto. Asimismo, la inhalación de agentes químicos como el Napalm, producen en el cuerpo de

28 Ibíd.
29 Ibíd.
30 Ibíd.
31 Op. cit., Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 414.

la víctima efectos materiales evidentes. Bombardeos aéreos por saturación, envenenamiento o corte de suministros de agua, destrucción de torres y redes eléctricas son también medios cuya utilización, legítima o ilegítima, encajan dentro de los conceptos de arma y conflicto armado del Derecho de Guerra. Sin embargo [concluye], la irrupción de la electrónica y la informática en el ámbito bélico obliga a efectuar algunas piruetas intelectuales a la hora de someter su utilización o abuso a las normas del Derecho de Guerra[32]".

El problema que se advierte en la perspectiva jurídica es cómo aplicar las normas de dicho marco jurídico a la ciberguerra. En este sentido, Luke afirma que "subsumir normas que fueron creadas para aplicarse a acciones y objetos con existencia corpórea, a una realidad compuesta de cosas inmateriales genera problemas que la interpretación analógica no siempre logra resolver. Las armas informáticas solo consisten en información, en pulsos eléctricos organizados bajo códigos lógicos que expresados en un lenguaje matemático pueden traducirse en órdenes ejecutables por un computador"[33]. Asimismo, agrega que[34]:

> *Estas armas tienen como blanco otros códigos, otros sistemas de información, cosas que aun siendo inmateriales permiten en una creciente medida, el efectivo desempeño de toda una sociedad. Las particularidades de este tipo de armas generan una serie de interrogantes desde el punto de vista jurídico. Por ejemplo, surge la duda sobre si se puede concebir como agresión una acción que no ha implicado el traspaso de fronteras físicas protegidas por la soberanía de un Estado, ni la movilización de tropas, ni la muerte de soldados o civiles en el Estado víctima del ataque, ni la destrucción de bienes físicos como edificios, represas o caminos. Asimismo, es objeto de debate determinar si un ataque informático que logra causar un perjuicio físico o económico de carácter sustancial en el Estado Víctima, justifica o no, desde el punto de vista del Derecho Internacional, una respuesta armada de este o la responsabilidad de aquel.*

En este escenario jurídico de incertidumbre, el CICR entrega una visión que en algo aclara el punto, nuevamente en el ámbito del *jus in bello*. Señala el CICR que si bien el DIH no contenga referencias específicas a las operaciones cibernéticas no significa que esas operaciones no estén sujetas a sus normas. Si los medios y métodos de la guerra cibernética producen los mismos efectos en el mundo real que las armas convencionales (destrucción, desorden, daños, lesiones o muerte), se rigen por las mismas normas que las armas

32 Ibíd.
33 Ibíd.
34 Ibíd.

convencionales[35]. Agrega el CICR que la tecnología evoluciona sin cesar, y el DIH es suficientemente amplio para abarcar todas las nuevas tecnologías. El DIH prohíbe o limita el uso de determinadas armas (por ejemplo, las armas químicas o biológicas, o las minas antipersonal). Pero por medio de sus normas generales regula todos los medios y métodos de guerra, incluido el uso de todas las armas. En particular, el artículo 36 del Protocolo adicional I a los Convenios de Ginebra establece lo siguiente: "Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante"[36].

Concluye el CICR señalando que más allá de la obligación concreta que impone a los Estados Partes, la norma precedente demuestra que las disposiciones generales del DIH se aplican a las nuevas tecnologías. Esto no excluye la posibilidad de que sea necesario seguir desarrollando esta rama del derecho a medida que evolucionen las tecnologías o que sus consecuencias humanitarias se comprendan mejor. La determinación de esa necesidad incumbe a los Estados. Mientras tanto, es importante destacar que no hay lagunas jurídicas en el ciberespacio. Más allá de esta afirmación, se plantean muchas preguntas acerca de la forma de aplicar el DIH en la práctica[37].

Sin perjuicio de lo señalado por el CICR, lo cierto es que la ciberguerra se encuentra huérfana de un marco normativo más preciso y con mayores certezas. En especial, este marco es requerido por los órganos y cuerpos militares y técnicos que emplean estos medios en el marco de un conflicto armado. Como se puede comprender, a veces en un conflicto armado la línea que marca la diferencia entre lo legal y lo ilegal respecto del uso de medios y métodos puede resultar confuso. Las condiciones del campo de batalla hacen difícil marcar con exactitud cuándo se está dentro o fuera de lo permitido, en particular considerando la aplicación de los principios que orientan el derecho internacional humanitario (distinción, proporcionalidad). De ahí la importancia de contar con reglas claras para el uso de medios y métodos de guerra en ciberguerra.

La falta de respuesta jurídica precisa en ciberguerra, en particular en el campo del *jus in bello*, genera la necesidad avanzar en la identificación de propuestas que, aun cuando en un carácter no vinculante, entreguen caminos que orienten la conducta de los Estados y de las partes combatientes, en

35 Op. cit., Droege, Cordula, *No hay lagunas jurídicas en el Ciberespacio.*
36 Ibíd.
37 Ibíd.

particular las Fuerzas Armadas, al momento de decidir el uso del ciberespacio para fines militares, en el ámbito de un conflicto armado. De esto trata el siguiente apartado.

Hacia el desarrollo de un marco normativo en ciberguerra

Un punto de especial y previa consideración en materia de ciberguerra es que los medios y métodos de ciberguerra no están, en principio, prohibidos. Es decir, la ciberguerra, a diferencia del cibercrimen y el ciberterrorismo, como tal no cae *per se* en el campo de la ilegalidad. En ese contexto, el Derecho está llamado a establecer un conjunto de normas que regulen y precisen el uso de los medios y métodos de ciberguerra, en orden a prohibir o restringir su empleo, y por esta vía evitar que su uso genere consecuencias que resulten desproporcionadas o dañen a personas y recursos que no están relacionadas con el ámbito militar o bélico del conflicto[38].

Señalado lo anterior, es posible comentar que el trabajo ya citado de Luke presenta un marco de análisis que resulta útil para comprender las dificultades que reviste construir un modelo de derecho que aplique con eficiencia en la regulación de la ciberguerra[39]. A modo de síntesis, y luego de descartar propuestas que la doctrina internacional plantea respecto de normas vigentes que podrían servir como marco jurídico en la materia[40], este marco de análisis se construye de las siguientes variables o premisas.

- Mientras la regulación en ciberguerra no exista, los Estados deben valerse del Derecho vigente.
- En el Derecho vigente no hay claridad acerca de cómo o por qué podría perseguirse la responsabilidad de los Estados agresores.
- Existen dificultades que sortear para admitir la viabilidad para la aplicación del derecho vigente. Estas dificultades tiene que ver con:

[38] En esta materia, la Regla 12 del Manual de Tallinn, que será citado a continuación, ilustra el punto. Esta regla señala que "Una ciberoperación, o una amenaza de ciberoperación, constituyen una amenaza ilegal de fuerza cuando la acción amenazadora, si es llevada a cabo, sería un uso de fuerza ilegal".

[39] Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* pp. 415-421.

[40] Estas doctrinas son 4: 1) sobre tratados de no proliferación nuclear, 2) sobre tratado antártico y derecho del Espacio; 3)Convención de las Naciones Unidas sobre Derecho de los Tratados del Mar, 4) sobre asuntos de Asistencia Legal. En Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* pp. 416-417.

  - Establecer si frente a un ataque informático se está bajo las normas del *jus ad bellum* o bajo las normas del *jus in bello.*
  - Establecer si un ciberataque logra calificar como un uso de la fuerza prohibido; esto debido al tipo de arma que se emplea en este tipo de ataque, diferente al carácter kinético que tienen las de guerra convencional.
- Respecto de la calificación de uso de la fuerza prohibido, existen dos escuelas. La primera es la que resta importancia a los medios con que se lleva a cabo el ataque y se concentra en los daños provocados; la segunda, que cualquier cosa distinta a un ataque armado no está prohibida por el derecho Internacional.
- La propuesta en orden a adecuar el Derecho Internacional vigente a la ciberguerra conduce a dos soluciones distintas. La primera es homologar los ciberataques a ataques armados convencionales. La segunda, reconstruir estas agresiones hacia conductas típicas de la ley penal del país víctima.

Hacia la construcción de un marco normativo. El Manual de Tallinn

El curso de acción hasta ahora elegido para cubrir el vacío regulatorio existente en materia de ciberguerra es la homologación del Derecho vigente a este ámbito. En efecto, y como lo propone el CICR, no existiendo desarrollo normativo especial y vinculante en ciberguerra, lo que se formula es aplicar el actual marco regulatorio del derecho internacional de los conflictos armados. En particular la Carta de la Organización de Naciones Unidas en lo referente a la legalidad en la decisión de uso de la fuerza, *jus ad bellum*, y las reglas del derecho internacional que regulan, con arreglo al derecho humanitario, *jus in bello,* el uso de la fuerza durante el conflicto para evitar daños innecesarios a los propios combatientes, a la población civil y sus bienes.

Para lo anterior, se ha avanzado en el desarrollo doctrinario desde el campo académico, proponiendo un conjunto de reglas que, derivadas del marco jurídico vigente, permiten su aplicación a la ciberguerra. El trabajo más relevante es el proyecto llevado a cabo por 20 renombrados académicos, los que, por una invitación del Centro de Excelencia Cooperativo en CiberDefensa, de la Organización del Tratado del Atlántico Norte (NATO, por sus siglas en inglés), durante tres años estudiaron el derecho internacional aplicable a la ciberguerra. Este trabajo dio vida en el 2013 al llamado "Manual de Tallinn" –en adelante "el Manual"–, el que propone 95 reglas no vinculantes que regulan el ejercicio de este tipo de guerra en el

ciberespacio[41]. Como señala el Manual en su parte introductoria, su texto se enfoca a tópicos de soberanía, responsabilidad de los Estados, unido a los ya señalados *jus ad bellum y jus in bello,* para finalizar con las leyes de la neutralidad. Para cada uno de estos ámbitos el Manual explicita reglas particulares, acompañada de comentarios que las relacionan con normas del derecho convencional y consuetudinario. Estos comentarios explican además cómo el grupo de expertos convocados interpretó las normas existentes al contexto cibernético, incluyendo por último en estos comentarios los desacuerdos en el trabajo de interpretación[42].

El Manual de Tallinn, texto de cuidadosa elaboración, y que sugiere un marco regulatorio, no vinculante, para su aplicación en el marco del conflicto, abarca una categoría de materias diversas, las que van desde la responsabilidad de los Estados, reglas para el uso de la fuerza, reglas de conducción de hostilidades, hasta materias acerca de neutralidad de los Estados y relativos a ocupación. Respecto de esta propuesta, interesa de manera particular señalar lo siguiente de acuerdo con los criterios y reglas del Manual.

- Atribuye la responsabilidad del Estado cuando personas o ciberestructuras de su jurisdicción realizan actos contrarios al Derecho Internacional.
- Determina el hecho del uso de la fuerza de medios y métodos cibernéticos como constitutivo de conflicto armado cuando estos llegan al nivel o intensidad de uso de la fuerza de medios convencionales, calificado así por el derecho internacional. Es por tanto una metodología de homologación de unos respecto de otros. El indicador para medir esta intensidad está dado fundamentalmente por el nivel de daño causado (escala y efectos de la operación cibernética).
- El derecho a defensa de un Estado ante ataques cibernéticos, como la decisión de uso de la fuerza del Consejo de Seguridad de Naciones Unidas, puede incluir tanto medidas de fuerza convencionales como cibernéticas.
- La existencia de un conflicto armado, internacional, o sin el carácter de internacional, puede verificarse ante el solo uso de medios y métodos cibernéticos, no requiriéndose necesariamente el uso de otros medios convencionales para calificarlos como tales.

41 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, London, Cambridge , Cambridge University Press, 2013.

42 El 2017 se publicó el Manual de Tallinn 2.0, de Derecho Internacional aplicable a ciberoperaciones. Esta versión, preparada durante 4 años a partir del 2013, abarcó además aspectos del derecho internacional en ciberguerra en regímenes legales de tiempo de paz. Para el presente estudio, esta versión 2.0 del Manual se toma solo a modo referencial, toda vez que no modifica de manera sustancial las materias que son tratadas en la versión del 2013.

- Define como sujetos de ciberataques a la categoría de personas que el derecho internacional humanitario entiende y define como personas que participan del conflicto. Al mismo tiempo establece como personas protegidas de ciberataques a las que este mismo derecho internacional humanitario protege.
- Identifica los medios de ciberguerra como ciberarmas y sus cibersistemas asociados y métodos de ciberguerra como cibertácticas, cibertécnicas y procedimientos por los que son conducidas las hostilidades.
- Identifica de manera particular como objetivos militares los computadores, redes de computación e infraestructura cibernéticas, tanto de uso militar permanente como aquellos que presentan uso dual, o de uso generalmente civil pero que de manera transitoria se les asigna uso militar. Incluye también la *data* contenida en estos sistemas.
- Aplica de manera homóloga a la ciberguerra las normas de derecho internacional humanitario referidos a conductas y precauciones en el ataque.

En esta revisión de criterios y reglas que establece el Manual, interesa comentar de manera particular la Nº 22. Esta califica como conflicto armado el hecho de que un Estado realice sobre otros ciberataques, sin necesariamente el uso de otros medios y métodos de guerra. Se estima que esta calificación abre un espacio discrecional mayor para que el Estado "agredido" por el ciberataque, sin empleo de otras armas, califique este ataque como constituyente de conflicto armado y, en consecuencia, se arrogue el derecho de responder al amparo de legítima defensa, o al Consejo de Seguridad de actuar en tal sentido, no solo con medios y métodos cibernéticos, sino también en virtud de lo establecido en la regla Nº 14, con medios convencionales. Esta regla, constituiría por tanto una ampliación en la aplicación del principio de la legítima defensa.

Comentarios finales

Estos comentarios pretenden destacar aquellos aspectos que resultan relevantes de la relación existente entre la ciberguerra y el Derecho.

Un primer punto a comentar es constatar la pertenencia de la ciberguerra a un género mayor y que, junto con esta, albergar otras formas de uso del ciberespacio con el fin de generar efectos dañosos en un adversario, o bien efectos lucrativos prohibidos. La ciberseguridad está llamada a evitar los

daños que produce el cibercrimen, el ciberterrorismo y la ciberguerra. Esta última, dependiendo de la doctrina de los respectivos Estados, comprendida a su vez en el marco de la ciberdefensa.

Teniendo como característica común a todas estas formas el uso del ciberespacio, desde la perspectiva del Derecho existe una diferencia fundamental de la ciberguerra respecto de las otras. Esta radica en el hecho de que el uso del ciberespacio en el contexto de un conflicto armado, para fines de conseguir los objetivos e intereses de las partes, no está por regla general prohibido. Más bien, y ya que los medios y métodos cibernéticos son asimilados al concepto de armas destinadas a producir daño en el adversario, la decisión de empleo (*jus ad bellum*) y la forma de empleo (*jus in bello*) están llamados a ser regulados, pero no prohibidos, por el Derecho. Esta regulación debiese estar orientada, primero, a establecer las condiciones de legalidad en la decisión del uso de estos medios y métodos; segundo, a definir formalmente el carácter jurídico de los mismos, definiéndolos, como se ha visto en este trabajo, de una manera similar al resto de las armas que se emplean en un conflicto; por último, a precisar respecto de la forma legal de uso de estos medios y métodos cibernéticos en el marco del conflicto.

Un segundo aspecto a constatar es la inexistencia de un marco jurídico regulatorio vinculante a nivel internacional, al menos en materias no cubiertas por las normas concernientes a cibercrimen. Esta carencia tiene, como se comprenderá, efectos directos en el campo de la ciberguerra. No obstante esta realidad, a nivel regional se aprecian los esfuerzos para generar políticas y reglas en materia de ciberseguridad y ciberdefensa, entre estas, las que se tratan en el marco de UNASUR, esfuerzos que todavía se encuentran en un estado incipiente. También destaca la visión del CICR, en la que propone la aplicación del Derecho Internacional Humanitario vigente a la ciberguerra. Por último, a nivel nacional, la dictación de la Política Nacional de Ciberseguridad y el mandato a desarrollar una política en ciberdefensa, permite albergar la posibilidad de avanzar en aspectos regulatorios más concretos.

Lo anterior, sin embargo, no resuelve el aspecto preciso de la ciberguerra. Como fue señalado, el ámbito específico en que esta se da, la guerra o el conflicto armado, no está prohibido, sino circunscrito a condiciones especiales para decidir su uso y para regular el empleo de medios y métodos una vez iniciado. La ausencia de normas en la materia, como ha sido advertido en este trabajo, ha abierto el campo a discurrir diversas formas de solución en el ámbito internacional. En definitiva, la que ha prevalecido es la de homologar las normas generales respecto de la autorización de uso de la fuerza establecidas en la Carta de Naciones Unidas y del derecho de guerra en convenciones y tratados acerca de derecho internacional humanitario, a

los medios y métodos de ciberguerra. En este sentido, se puede afirmar que esta forma de solución incorpora a la ciberguerra como una forma especial de uso de fuerza en el marco de un conflicto armado.

El poner atención a un marco normativo en materia de ciberguerra, aun cuando sea difícil de distinguir, es algo a considerar para un país como Chile. En este sentido, señala Luke que "Para aquellos Estados cuyas fortalezas no se basan en su arsenal bélico ni en su poder económico sino en su prestigio, el respeto del Derecho Internacional es un factor de suma relevancia. Por ello, el costo de llevar a cabo acciones u omisiones que puedan considerarse como un uso ilegal de la fuerza (o tan solo una ilegítima amenaza de su uso), puede ser sumamente alto en términos de prestigio internacional"[43]. Concluye que "Frente a este hecho y considerando que Chile mantiene una política exterior que otorga alta importancia al prestigio, un conocimiento acabado del marco jurídico internacional que lo protege y obliga frente a las amenazas a la seguridad propias del siglo XXI, es esencial"[44].

En consideración a lo anterior, es pertinente destacar al actual valor de uso del Manual de Tallinn. Si bien sus reglas no generan obligaciones a los Estados por su carácter no vinculante, lo que incluye a Chile, una lectura y análisis preliminar de sus contenidos lleva a afirmar que estas no son contrarias ni al actual Derecho Internacional (*jus ad bellum* y *jus in bello*) ni al propio Derecho Nacional. Por lo mismo, de confirmarse lo anterior con un estudio más acabado, sería pertinente evaluar la posibilidad de incorporarlas a las respectivas doctrinas operacionales de las Fuerzas Armadas de los Estados, en particular de Chile. Esta propuesta, en particular, no se distancia del Derecho Internacional Humanitario de carácter convencional, toda vez que este constituye un marco o estándar de exigencia mínimo que se exige a los Estados. A partir de este mínimo, los Estados pueden adoptar disposiciones que restrinjan más aún el empleo de medios y métodos, entre estos lo de naturaleza cibernética. Constituye por tanto una materia que podría someterse a consideración de las respectivas unidades de doctrina de las ramas castrenses.

43 Op. cit., Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 415.

44 Ibíd.

Bibliografía

Textos

Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* ensayo presentado en el VII Congreso del Instituto de Relaciones Internacionales, La Plata, Argentina, 26.27 y 28 de noviembre de 2014.

Gobierno de Chile, *Política Nacional de Ciberseguridad 2017-2022.*

Gaitán Rodríguez, Andrés *El Ciberespacio: un nuevo teatro de batalla para los conflictos armados del siglo XXI,* Bogotá, Escuela Superior de Guerra de Colombia, 2012.

Luke, V. (2012). Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas. *Revista de Derecho Público.*

Reguera Sánchez, Jesús, *Aspectos Legales en el Ciberespacio. La Ciberguerra y el Derecho Internacional Humanitario,* Grupo de Estudios en Seguridad Internacional, GESI, Universidad de Granada.

Tallinn Manual on the International Law Applicable to Cyber Warfare, London, Cambridge, Cambridge University Press, 2013.

Internet

Carilini Agnese, *ISIS: Una nueva amenaza en la era digital,* Madrid, Instituto Español de Estudios Estratégicos (i.e.e.e.es), 129/2015, (Documento en línea, 1 de diciembre de 2015), en internet http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO129-, [Fecha de consulta el 05 de diciembre de 2017].

En Gobierno de Chile, *Una Política Nacional de Ciberseguridad para Chile,* en internet, http://www.ciberseguridad.gob.cl/noticias/una-politica-nacional-de-ciberseguridad-para-chile/, [Fecha de consulta, el 14 de septiembre de 2017].

Naciones Unidas, Asamblea General, septuagésimo segundo período ordinario de sesiones de la Asamblea General, en Internet http://www.un.org/es/ga/72/agenda/index.shtml, [Fecha de consulta, el 25 de septiembre de 2017].

UNASUR, VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado, Declaración de Paramaribo, numeral 29.

UNASUR, Consejo de Defensa Suramericano, Acta 1° Reunión Virtual Grupo de trabajo Ciberdefensa CDS-UNASUR, (Documento en línea 7 de marzo de 2017).

Gobierno de Chile, depósito de instrumento de adhesión. En internet http://www.minrel.gov.cl/chile-deposita-el-instrumento-de-adhesion-al-convenio-de-budapest-sobre/minrel/2017-04-21/175923.html, [Fecha de consulta el 16 de diciembre de 2017].