# Veinte años después: el derecho internacional humanitario y la protección de las personas civiles contra los efectos de las ciberoperaciones durante los conflictos armados

**Laurent Gisel, Tilman Rodenhäuser y Knut Dörmann***

Laurent Gisel es jefe de la Unidad de Armas y Conducción de Hostilidades de la División Jurídica del Comité Internacional de la Cruz Roja (CICR) en Ginebra. Entre 2013 y 2020, se desempeñó como asesor jurídico principal, dirigió el Equipo de Informática y fue responsable del archivo de las normas que rigen la conducción de las hostilidades en el derecho internacional humanitario, incluida su aplicación durante la guerra urbana, las ciberoperaciones y las operaciones en el espacio ultraterrestre.

El Dr. Tilman Rodenhäuser es asesor jurídico del CICR, experto en ciberoperaciones durante conflictos armados, grupos armados no estatales y traslado de detenidos.

* Este artículo fue publicado en una versión anterior de los mismos autores con el título "The applicability and application of international humanitarian law to cyber warfare", *Chinese Review of International Law*, vol. 32, n.º 4, 2019. Para su publicación en este número de la *International Review*, ha sido ampliado y actualizado sustancialmente. Todo lo expresado en este artículo refleja las opiniones personales de los autores y no necesariamente las del CICR.

El Dr. Knut Dörmann es jefe de la Delegación del CICR ante la UE, la OTAN y el reino de Bélgica (Bruselas), y fue responsable jurídico y jefe de la División Jurídica (2007–2019). Con anterioridad, se había desempeñado como subjefe de la División Jurídica del CICR (2004–2007) y como asesor jurídico del CICR (1999–2004), incluso en cuestiones relativas a las ciberoperaciones.

## Resumen

*El uso de ciberoperaciones durante los conflictos armados y la cuestión de cómo se aplica el derecho internacional humanitario (DIH) a esas operaciones han evolucionado considerablemente durante los últimos veinte años. En nuestras distintas funciones dentro de la División Jurídica del Comité Internacional de la Cruz Roja (CICR), los autores de este artículo hemos seguido de cerca esa evolución y participado en debates de expertos gubernamentales y no gubernamentales sobre este tema. En este artículo, analizamos las cuestiones pertinentes en materia humanitaria, jurídica y de políticas. Primero, mostramos que el uso de ciberoperaciones durante los conflictos armados es ya una realidad y probablemente tendrá una mayor prominencia en el futuro. La evolución de las ciberoperaciones despierta numerosas preocupaciones en las sociedades actuales, cada vez más dependientes de la informática, donde una ciberoperación maliciosa puede causar interrupciones y daños considerables a las personas. Luego, presentamos una breve reseña de los debates multilaterales sobre el régimen jurídico y normativo que rige las ciberoperaciones durante los conflictos armados, con especial atención a los diversos argumentos sobre la aplicabilidad del DIH a las ciberoperaciones durante los conflictos armados y a la relación entre el DIH y la Carta de la ONU. Dejamos en claro que, en nuestra opinión, no hay dudas de que las ciberoperaciones durante los conflictos armados, o guerra cibernética, se rigen por el DIH –al igual que todas las armas, medios o métodos de guerra que utiliza un beligerante en un conflicto, sean nuevos o antiguos. En tercer lugar, en el apartado principal, nos centramos en cómo se aplica el DIH a las ciberoperaciones. Al analizar las posiciones jurídicas más recientes de los Estados y los expertos, recordamos los debates más notables de la pasada década, por ejemplo, respecto de qué ciberoperaciones constituyen un "ataque" de acuerdo con la definición del DIH y si los datos civiles gozan de una protección similar al de los "bienes de carácter civil". También repasamos las normas del DIH que se aplican a las ciberoperaciones que no constituyen ataques y los regímenes de protección especial para determinados actores e infraestructuras, como los establecimientos sanitarios y las organizaciones humanitarias.*

**Palabras clave**: ciberoperaciones, conflictos armados, guerra cibernética, costos humanos, derecho internacional humanitario.

***

El uso de ciberoperaciones durante los conflictos armados y la cuestión de cómo se aplica el derecho internacional humanitario (DIH) a esas operaciones ha evolucionado considerablemente durante los últimos veinte años. Esto es cierto para los niveles operacional, jurídico y político. En el ámbito operacional, el uso de ciberoperaciones durante los conflictos armados ya es una realidad

y probablemente tendrá mayor prominencia en el futuro. La evolución de las ciberoperaciones despierta numerosas preocupaciones en las sociedades actuales, cada vez más dependientes de la informática, donde una ciberoperación maliciosa puede causar interrupciones y daños considerables a las personas. En los planos político y jurídico, mediante procesos multilaterales, los Estados han alcanzado acuerdos sobre algunos aspectos del régimen jurídico y normativo que regula las ciberoperaciones; no obstante, la aplicación del DIH a las ciberoperaciones durante los conflictos armados continúa siendo foco de intensos debates. Algunos Estados han publicado su posición sobre cómo se aplica el DIH a las ciberoperaciones durante los conflictos armados, y se han realizado numerosos estudios académicos sobre el tema. Así y todo, hay cuestiones fundamentales que siguen siendo controvertidas y sobre ellas no existe acuerdo entre los Estados y otros expertos o es necesario profundizar el análisis. Entre esos puntos controvertidos, se encuentra la noción de "ataque", la cuestión de cómo están protegidos los datos civiles contra las ciberoperaciones maliciosas y qué normas del DIH se aplican a las ciberoperaciones que no constituyen ataques. En sus diferentes funciones en la División Jurídica del Comité Internacional de la Cruz Roja (CICR), los autores de este artículo hemos seguido de cerca la evolución del uso de ciberoperaciones y los debates pertinentes, y hemos participado en debates de expertos gubernamentales y no gubernamentales sobre la aplicabilidad y la aplicación del DIH a las ciberoperaciones durante los conflictos armados desde su inicio.

Recientemente, el CICR publicó un documento de posición titulado *Derecho internacional humanitario y ciberoperaciones durante conflictos armados* que fue presentado ante el Grupo de Expertos gubernamentales (GEG) de las Naciones Unidas (ONU) y el Grupo de Trabajo de composición abierta (GTCA)[1]. En este artículo, desarrollamos esa posición y explicamos en primer lugar por qué los posibles costos humanos de las ciberoperaciones constituyen una preocupación humanitaria. Luego, dejamos en claro que el DIH se aplica a las ciberoperaciones durante los conflictos armados –y, por lo tanto, las limita– y repasamos la posición de distintos Estados sobre el tema. En tercer lugar, analizamos cuándo las ciberoperaciones pueden desencadenar un conflicto armado y cómo se relaciona ese umbral con la prohibición del uso de la fuerza y el derecho a la defensa propia de conformidad con la Carta de la ONU y el derecho internacional consuetudinario. En la última parte de este artículo, que es la más sustancial, profundizamos en algunas de las cuestiones aún no resueltas con respecto a la aplicación del DIH a las ciberoperaciones durante los conflictos armados y en las posiciones adoptadas por los Estados respecto de algunas cuestiones fundamentales.

1 CICR, *Derecho internacional humanitario y ciberoperaciones durante conflictos armados*, documento de posición dirigido al 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, 2019, disponible en https://www.icrc.org/es/document/derecho-internacional-humanitario-y-ciberoperaciones-durante-conflictos-armados (todas las referencias de internet fueron consultadas en agosto de 2020). Disponible también en la sección "Informes y documentos" de este número de la *International Review*.

Desde el punto de vista operacional, el uso de tecnologías cibernéticas ya es una realidad en los conflictos armados contemporáneos, y es probable que aumente con el tiempo. Algunos Estados han reconocido públicamente que ejecutaron ciberoperaciones en conflictos armados en curso. En particular, Estados Unidos, el Reino Unido y Australia revelaron que habían usado ciberoperaciones durante el conflicto con el Estado Islámico[2]. Existen, asimismo, informes públicos que indican que Israel usó ciberoperaciones contra Hamas y también se ha denunciado el uso de ciberoperaciones de Hamas contra Israel[3]. Otros países que participan en conflictos armados se han visto afectados por ciberoperaciones, como Georgia en 2008[4], Ucrania en 2015-2017[5] y Arabia Saudí en 2017[6], si bien no se sabe quiénes fueron los autores de esos ciberataques y la atribución de responsabilidades es dudosa. Así pues, no queda claro si esas operaciones tenían un nexo con los respectivos conflictos armados y, por lo tanto, si el DIH era aplicable. Además, ha habido informes sobre ciberoperaciones realizadas por Estados en otras situaciones, en las que la clasificación jurídica puede haber sido ambigua, o que incluso quedan

2 V., en particular, Mike Burgess, Dirección de Señales de Australia, "Offensive cyber and the people who do it", discurso pronunciado en el Instituto Lowy, 27 de marzo de 2019, disponible en www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm; Paul M. Nakasone, "Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services", 14 de febrero de 2019, disponible en https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf; Jeremy Fleming, Sede de Comunicaciones del Gobierno del Reino Unido (GCHQ, por su sigla en inglés), "Director's speech at CyberUK18", 12 de abril de 2018, disponible en www.gchq.gov.uk/pdfs/speech/director-cyber-uk-speech-2018.pdf.

3 "Hackers interrupt Israeli Eurovision webcast with faked explosions", *BBC News*, 15 de mayo de 2019, disponible en www.bbc.co.uk/news/technology-48280902; Zak Doffman, "Israel responds to cyber attack with an air strike on cyber attackers in World First", Forbes, 6 de mayo de 2019, disponible en https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/. Si bien el presunto objetivo de la supuesta operación cibernética de Hamas no fue anunciado públicamente, se afirma que el ataque al edificio de Hamas con medios cinéticos se guió por informes de inteligencia de las Fuerzas de Defensa de Israel.

4 David Hollis, "Cyberwar case study: Georgia 2008", *Small Wars Journal*, 2010, disponible en https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

5 Andy Greenberg, "How an entire nation became Russia's test lab for cyberwar", *Wired*, 20 de junio de 2017, disponible en www.wired.com/story/russian-hackers-attack-ukraine/; Andy Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history", *Wired*, 22 de agosto de 2018, disponible en www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

6 Blake Johnson *et al.*, "Attackers deploy new ICS attack framework 'TRITON' and cause operational disruption to critical infrastructure", *FireEye Blogs*, 14 de diciembre de 2017, disponible en www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

comprendidas dentro de lo que a veces se denomina "zona gris"[7]. Esos ejemplos confirman el incremento del recurso a las ciberoperaciones en la última década, un cambio en la conducción de la guerra que podría continuar. De hecho, se afirma que un número cada vez mayor de Estados, entre los que se encuentran los cinco miembros permanentes del Consejo de Seguridad de la ONU, han desarrollado o están desarrollando capacidades militares cibernéticas[8]. Entre los ejemplos del uso de ciberoperaciones durante conflictos armados se encuentran el espionaje; la

7 P. ej., ha habido varios informes periodísticos –basados en fuentes oficiales anónimas– que afirman que Estados Unidos ejecutó ciberoperaciones contra Rusia e Irán, y que Israel realizó una ciberoperación cibernética contra un puerto iraní. V. Ellen Nakashima, "U.S. cyber command operation disrupted Internet access of Russian troll factory on day of 2018 midterms", *The Washington Post*, 27 de febrero de 2019, disponible en https://tinyurl.com/yxs8twyv; David E. Sanger y Nicole Perlroth, "U.S. escalates online attacks on Russia's power grid", *The New York Times*, 15 de junio de 2019, disponible en www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html; Julian E. Varnes y Thomas Gibbons-Neff, "U.S. carried out cyberattacks on Iran", *The New York Times*, 22 de junio de 2019, disponible en www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html; Joby Warrick y Ellen Nakashima, "Officials: Israel linked to a disruptive cyberattack on Iranian port facility", *The Washington Post*, 18 de mayo de 2020, disponible en https://tinyurl.com/y4onsrt9. Sobre las denominadas "zonas grises" y las tecnologías cibernéticas, v. Camille Faure, "Utilisation contemporaine et future des technologies cyber/numériques dans les conflits armés", en Gabriella Venturini y Gian Luca Beruto (eds.), *Whither the Human in Armed Conflict? IHL Implications of New Technology in Warfare*, 42.ª mesa redonda sobre temas actuales del derecho internacional humanitario, Instituto Internacional de Derecho Humanitario, San Remo, 2020 (en prensa); Gary Corn, "Punching on the edges of the grey zone: Iranian cyber threats and state cyber responses", *Just Security*, 11 de febrero de 2020, disponible en www.justsecurity.org/68622/punchingon-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/. Sobre el umbral de aplicación del DIH, v., más adelante, el apartado "Ciberoperaciones regidas por el DIH".

8 Además de Estados Unidos y el Reino Unido, Francia se ha fijado el objetivo de "adquir[ir] capacidades de defensa cibernética" para defenderse de "Estados extranjeros o grupos terroristas [que] podrían atacar la infraestructura crítica". Francia, Agence Nationale de la Sécurité des Système d'Information, *Information System Defence and Security: France's Strategy*, 2011, disponible en www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf. El *White Paper on China's Military Strategy* de 2015 revela que "en respuesta al creciente desarrollo de las capacidades militares cibernéticas de otros Estados, China desarrollará capacidades militares cibernéticas de defensa". V. Gobierno de China, *White Paper on China's Military Strategy*, 2015, disponible en www.gov.cn/zhengce/2015-05/26/content_2868988.htm. Rusia no ha sido tan explícita sobre el tema, pero en la doctrina sobre seguridad de la información de la Federación de Rusia, se reconoce que "la actualización del sistema de seguridad de la información de las Fuerzas Armadas de la Federación de Rusia, otras tropas, formaciones y cuerpos militares, incluidas las fuerzas y los medios de confrontación de información" es un "área clave para garantizar la seguridad de la información en el ámbito de la defensa nacional". V. Ministerio de Asuntos Exteriores de la Federación de Rusia, *Doctrine of Information Security of the Russian Federation*, 5 de diciembre de 2016, disponible en https://tinyurl.com/y6yhp7pv. V. también Ministerio de Defensa de la Federación de Rusia, "Western MD operators repelled cyberattack of the simulated enemy in the course of the Union Shield – 2015", 2015, disponible en https://eng.mil.ru/en/news_page/country/more.htm?id=12056193@egNews. Para una apreciación general de la proliferación de las herramientas cibernéticas, v. Anthony Craig, "Understanding the proliferation of cyber capabilities", Council on Foreign Relations, 2018, disponible en www.cfr.org/blog/understanding-proliferation-cybercapabilities. Según el índice cibernético del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR), en 2012 cuarenta y siete Estados contaban con programas de ciberseguridad que asignaban algunas funciones a sus fuerzas armadas (UNIDIR, *The Cyber Index: International Security Trends and Realities*, doc. ONU UNIDIR/2013/3, Ginebra, 2013, p. 1), mientras que en 2020 Digital Watch Observatory registró veintitrés y treinta Estados de los que había evidencias o indicios, respectivamente, de que tenían capacidades cibernéticas (Digital Watch Observatory, "UN GGE and OEWG", disponible en https://dig.watch/processes/un-gge).

determinación de objetivos; las operaciones de información con el fin de debilitar la moral y la voluntad de combatir del enemigo; la interrupción, la adulteración o la obstaculización de los sistemas de comunicaciones del enemigo con el fin de impedir la coordinación de la fuerza; y las ciberoperaciones de apoyo a operaciones cinéticas[9]. Un ejemplo de estas últimas es la inhabilitación de las estaciones de radar del enemigo que dan apoyo a los ataques aéreos[10]. Asimismo, como se observa en diversas ciberoperaciones de la última década –que no necesariamente ocurrieron en el contexto de un conflicto armado–, las ciberoperaciones contra redes eléctricas, sistemas de asistencia de salud, plantas nucleares u otra infraestructura crítica pueden causar daños humanos considerables[11]. En el plano jurídico, los debates en torno a si el derecho internacional humanitario se aplica a las ciberoperaciones durante los conflictos armados, cómo se aplica y si las limita comenzaron hace más de veinte años[12]. Los procesos de redacción de los dos Manuales de Tallin sobre derecho internacional aplicable a la guerra cibernética (Manuales de Tallin) demostraron que existe un consenso amplio entre los expertos respecto de que el DIH se aplica en el ciberespacio y que sus normas y principios básicos pueden y deben aplicarse cuando se conducen ciberoperaciones durante un conflicto armado[13]. Como se observa en las opiniones divergentes que se encuentran en los Manuales de Tallin, en un número creciente de posiciones de Estados y en el nutrido corpus de publicaciones académicas sobre temas relacionados con la cibernética, varios aspectos de cómo se aplican algunas normas del DIH en este terreno aún no se han analizado en profundidad y existen desacuerdos sobre otras cuestiones, incluso sobre algunas de las más estudiadas (v., más adelante, el apartado sobre

9 CICR, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, https://blogs.icrc.org/law-and-policy/category/special-themes/avoiding-civilian-harm-during-military-cyber-operations/.

10 Sharon Weinberger, "How Israel spoofed Syria's air defense system", *Wired*, 4 de octubre de 2007, disponible en www.wired.com/2007/10/how-israel-spoo/; Lewis Page, "Israeli sky-hack switched off Syrian radars countrywide", *The Register*, 22 de noviembre de 2007, disponible en www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/.

11 En noviembre de 2018, el CICR convocó a una reunión de expertos para realizar una evaluación realista de las capacidades cibernéticas y sus posibles consecuencias humanitarias a la luz de sus características técnicas. V. Laurent Gisel y Lukasz Olejnik (eds.), *ICRC Expert Meeting: The Potential Human Cost of Cyber Operations,* CICR, Ginebra, 2019, disponible en www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf. V. también Sergio Caltagirone, "Industrial cyber attacks: A humanitarian crisis in the making", *Humanitarian Law and Policy Blog*, 3 de diciembre de 2019, disponible en https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/. En *Global Risks Report 2020*, el Foro Económico Mundial (FEM) sitúa los ataques cibernéticos entre los diez principales riesgos tanto por probabilidad como por impacto; v. FEM, *The Global Risks Report 2020*, 2020, p. 3, disponible en https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

12 V. Consejo General del Departamento de Defensa de Estados Unidos, *An Assessment of International Legal Issues in Information Operations*, 1999, disponible en https://fas.org/irp/eprint/io-legal.pdf; para uno de los primeros estudios académicos sobre estas cuestiones, v. Knut Dörmann, "Computer network attack and international humanitarian law", 2001, disponible en www.icrc.org/en/doc/resources/documents/article/other/5p2alj.htm.

13 V. Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 (Manual de Tallin); Michael N. Schmitt y Liis Vihul (eds.), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, segunda edición, Cambridge University Press, Cambridge, 2017 (Manual de Tallin 2.0).

"Los límites que impone el DIH al uso de las capacidades cibernéticas durante los conflictos armados"). En el plano político, los debates recientes y actuales que han tenido y tienen lugar en el seno de la ONU demuestran que llegar a un acuerdo sobre la aplicabilidad del DIH a las ciberoperaciones y profundizar el estudio de cómo podrían interpretarse sus normas sigue siendo complicado[14]. Los debates en torno a cuestiones relativas a la "seguridad de la información" se iniciaron en 1998, cuando la Federación de Rusia presentó una primera resolución al respecto ante la Asamblea General de la ONU. Esos debates se han intensificado en los últimos años. Desde 2004, ha habido seis reuniones consecutivas de Grupos de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. En 2018, la Asamblea General de la ONU también estableció el GTCA, que se reúne al mismo tiempo que los GEG. Ambos grupos tienen, entre otros, el cometido de examinar "la aplicación del derecho internacional a la utilización de las [tecnologías de la información y las comunicaciones] por los Estados"[15]. Esos debates deberían basarse en las importantes conclusiones a las que arribaron los GEG previos. En 2013 y 2015, los Estados que integraban el GEG señalaron que "el derecho internacional, en particular la Carta de las Naciones Unidas, era aplicable" en la esfera de las tecnologías de información y las comunicaciones y citaban "los principios jurídicos internacionales establecidos, entre ellos, de ser aplicables, los principios de humanidad, necesidad, proporcionalidad y distinción"[16]. Aun así, de los debates recientes en esos procesos de la ONU, y según el análisis que se hará más adelante, se desprende que no es sencillo llegar a un acuerdo sobre la aplicabilidad del DIH a las ciberoperaciones y avanzar en el estudio de cómo deben interpretarse sus normas.

En el ámbito regional, ya en 2009 los Estados miembros de la Organización de Cooperación de Shanghái (OCS) habían identificado que "[e]l desarrollo y el uso de armas informáticas" y "la preparación y la conducción de la guerra informática" constituían una importante amenaza en el campo de la seguridad internacional de la información, pero no se pronunciaron respecto del régimen

14 V., en especial, GTCA, "Initial 'pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security", 11 de marzo de 2020, disponible en https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf.

15 Asamblea General de la ONU, res. 73/27, "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional", doc. ONU A/RES/73/27, 11 de diciembre de 2018, párr. 5; Asamblea General de la ONU, res. 73/266, "Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional", doc. ONU. A/RES/73/266, 2 de enero de 2019, párr. 3.

16 Asamblea General de la ONU, "Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional: Nota del Secretario General", doc. ONU A/70/174, 22 de julio de 2015, párrs. 24, 28(d).

jurídico aplicable[17]. Se han mantenido debates en torno a la aplicación del derecho internacional, incluido el DIH, en la Organización Consultiva Jurídica Asiático Africana (AALCO) (que estableció un Grupo de Trabajo de composición abierta sobre la aplicación del derecho internacional en el ciberespacio en 2015)[18], la Mancomunidad de Naciones[19], la Unión Europea[20], la Organización del Tratado del Atlántico Norte (OTAN)[21] y la Organización de Estados Americanos (OEA)[22], entre otras organizaciones.

## Los posibles costos humanos de las ciberoperaciones

El avance de las tecnologías de la información y las comunicaciones, entre las que se encuentra la comunicación a través de redes informáticas (ciberespacio), ofrece enormes beneficios y oportunidades a los Estados, las sociedades y las personas en las esferas social y económica, en el ámbito del desarrollo y en el sector de la información y las comunicaciones, entre otras. La comunidad internacional, las sociedades y cada uno de nosotros individualmente dependemos cada vez más de las herramientas digitales. Esta tendencia –que probablemente se haya acelerado con la pandemia de COVID-19, que se propagaba en el momento de redacción de este artículo– incrementa nuestra dependencia del funcionamiento continuo de esas tecnologías y, por lo tanto, aumenta nuestra vulnerabilidad a las ciberoperaciones. En consecuencia, la rápida evolución del ciberespacio y de la tecnología de la información, y los posibles costos humanos de las ciberoperaciones, exige una supervisión y una evaluación constantes.

La utilización de herramientas cibernéticas como medio o método de guerra ofrece a las fuerzas armadas la posibilidad de lograr sus objetivos sin causar necesariamente daños directos a los civiles o daños físicos a la infraestructura civil. Según las circunstancias, el uso de ciberoperaciones podría permitir que se atacara un objetivo militar y, a la vez, se redujeran los daños incidentales previstos para los bienes de carácter civil, a diferencia de la utilización de otros medios de

17 Acuerdo de Cooperación para garantizar la seguridad internacional de la información entre los Estados miembros de la OCS, Ekaterimburgo, 16 de junio de 2009 (Acuerdo OCS); traducción no oficial del Ministerio de Defensa de la Federación de Rusia, "The State and the prospects of Russian military cooperation on international information security (A collection of papers)", 2014, pp. 77 y siguientes. V. también, p. ej., J. Fleming, nota 2 *supra*, p. 5.

18 V. AALCO, *International Law in Cyberspace*, doc. n.º AALCO/58/DAR ES SALAAM/2019/SD/17, disponible en www.aalco.int/Final%20Cyberspace%202019.pdf.

19 V. Declaración sobre el ciberespacio de la Mancomunidad de Naciones pronunciada durante la Reunión de Jefes de Gobierno de la Mancomunidad de Naciones celebrada en Londres, 16-20 de abril de 2018, disponible en https://thecommonwealth.org/commonwealth-cyber-declaration.

20 V., p. ej., Conclusiones del Consejo Europeo, reunión del Consejo de Asuntos Exteriores, doc. n.º 11357/13, 25 de junio de 2013.

21 V., p. ej., la Declaración de Gales pronunciada por los Jefes de Estado y de Gobierno que participaron en la reunión de la OTAN celebrada en Gales, 5 de septiembre de 2014, párr. 72, disponible en www.nato.int/cps/en/natohq/official_texts_112964.htm.

22 V. OEA, *Derecho internacional y ciberoperaciones: Mejora de la transparencia. Cuarto Informe*, doc. OEA CJI/doc. 603/20 rev.1 corr.1, 5 de marzo de 2020, disponible en http://www.oas.org/es/sla/cji/docs/CJI_doc_603-20_rev1_corr1.pdf.

guerra. En los debates intergubernamentales recientes, algunos Estados hicieron hincapié en que, si se emplean de manera responsable y de conformidad con el derecho internacional, "el uso de las TIC [tecnologías de la información y las comunicaciones] en contextos militares puede ser preferible al uso de armas cinéticas y puede contribuir a la reducción de las tensiones"[23]. Por el contrario, como se ha comentado, los Estados miembros de la OCS han advertido sobre los peligros del "desarrollo y el uso de armas informáticas" y "la preparación y la conducción de la guerra informática"[24].

La realización de ciberoperaciones con criterios diferenciadores, de conformidad con el DIH y que no afecten a la población civil puede ser difícil de lograr desde el punto de vista tecnológico. La interconectividad que caracteriza al ciberespacio implica que cualquier elemento que posea una interfaz con internet puede verse afectado por una ciberoperación conducida desde cualquier lugar del mundo. Un ciberataque a un sistema específico puede tener repercusiones en otros sistemas, independientemente de dónde se localizan. Existe un riesgo real de que las herramientas informáticas –sea deliberadamente o por error– puedan tener efectos diversos y a gran escala en la infraestructura civil crítica. La naturaleza interconectada del ciberespacio también implica que todos los Estados deberían preocuparse de su regulación eficaz: "Los ataques lanzados contra un Estado pueden afectar a muchos otros, dondequiera que estén ubicados e independientemente de si participan en el conflicto"[25]. Las ciberoperaciones ejecutadas en los últimos años –principalmente en situaciones que no son de conflicto armado– han demostrado que el software malicioso puede propagarse por el mundo en un instante y afectar la infraestructura civil y el suministro de servicios esenciales[26]. En consecuencia, muchos autores advierten que los ataques cibernéticos industriales suponen "una crisis humanitaria en ciernes"[27].

23 "UK response to Chair's initial 'pre-draft' of the Report of the OEWG on developments in the field of information and telecommunications in the context of international security", disponible en https://front.un-arm.org/wp-content/uploads/2020/04/20200415-oewg-predraft-uk.pdf. V. también CICR, nota 9 *supra*; Gary Corn, "The potential human costs of eschewing cyber operations", *Humanitarian Law and Policy Blog*, 31 de mayo de 2019, disponible en https://blogs.icrc.org/law-and-policy/2019/05/31/potential-human-costs-eschewing-cyber-operations/.

24 Acuerdo OCS, nota 17 *supra*, art. 2.

25 Helen Durham, "Cyber operations during armed conflict: 7 essential law and policy questions", *Humanitarian Law and Policy Blog*, 26 de marzo de 2020, disponible en https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.

26 Algunos ejemplos son el software malicioso CrashOverride, el programa de secuestro de archivos WannaCry, el programa de barrido NotPetya y el software malicioso Triton. CrashOverride afectó el suministro de electricidad en Ucrania; WannaCry tuvo efectos en hospitales de varios países; NotPetya infectó el sistema informático de un gran número de empresas; Triton estaba diseñado para interrumpir los sistemas de control industrial y, según se sabe, se utilizó en ataques a plantas petroquímicas de Arabia Saudí. Para un análisis de esta cuestión, v. Laurent Gisel y Lukasz Olejnik, "The potential human cost of cyber operations: Starting the conversation", *Humanitarian Law and Policy Blog*, 14 de noviembre de 2018, disponible en https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/.

27 V. S. Caltagirone, nota 11 *supra*.

El sector sanitario parece ser particularmente vulnerable a los ataques cibernéticos[28]. El sector avanza hacia una digitalización y una interconectividad cada vez mayores, lo que aumenta la dependencia digital y la superficie de ataque, una tendencia que probablemente continúe en los próximos años. Con demasiada frecuencia, esa evolución no va acompañada de una mejora en la ciberseguridad[29]. Esta vulnerabilidad se volvió especialmente visible durante la pandemia de COVID-19, cuando los hospitales y otros establecimientos sanitarios de distintos Estados sufrieron interrupciones en su funcionamiento debido a ciberoperaciones hostiles. A la luz de la especial importancia del sector sanitario en la mitigación del sufrimiento en todas las épocas y, en especial, durante los conflictos armados y las crisis sanitarias, el CICR ha hecho un llamamiento a todos los Estados para que respeten y protejan contra los ataques cibernéticos de todo tipo a los servicios de salud y las instalaciones sanitarias, sea en tiempo de paz o en situaciones de conflicto, y para que ratifiquen y renueven su compromiso con las normas internacionales que prohíben esos ataques[30]. Además de reflejar las obligaciones del DIH aplicables a las ciberoperaciones durante los conflictos armados[31], el llamamiento ratificaría, o incluso fortalecería, las prohibiciones del derecho internacional público que se aplican en todo momento[32].

Las ciberoperaciones contra otros tipos de infraestructura civil crítica, como las redes de electricidad, agua y saneamiento, también pueden causar daños considerables a los humanos[33]. A menudo, estos tipos de infraestructura funcionan con sistemas de control industrial (SCI). Un ataque cibernético contra

28 L. Gisel y L. Olejnik (eds.), nota 11 *supra*, pp. 18-22.

29 V. Aaron F. Brantly, "The cybersecurity of health", *Council on Foreign Relations Blog*, 8 de abril de 2020, disponible en https://tinyurl.com/yxc4oc9j.

30 V. "Call by global leaders: Work together now to stop cyberattacks on the healthcare sector", *Humanitarian Law and Policy Blog*, 26 de mayo de 2020, disponible en https://blogs.icrc.org/law-and-policy/2020/05/26/call-global-leaders-stop-cyberattacks-healthcare/. En el marco específico del GTCA, el CICR propuso que los Estados podrían adoptar una norma por la cual se comprometieran a "no conducir o apoyar deliberadamente ciberoperaciones que podrían dañar servicios médicos o establecimientos sanitarios, y a tomar medidas para proteger los servicios médicos contra los daños". Esta recomendación combina un elemento "negativo", es decir, que los Estados no deben conducir o apoyar deliberadamente actividades cibernéticas que podrían ser dañinas para los servicios médicos o los establecimientos sanitarios, y un elemento "positivo", en concreto, que los Estados deben tomar medidas para proteger los servicios médicos contra el daño. V. CICR, "Norms for responsible state behavior on cyber operations should build on international law", 11 de febrero de 2020, disponible en www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

31 V., más adelante, el apartado "Normas del DIH que confieren protección a los bienes indispensables para la supervivencia de la población civil, los servicios sanitarios y las operaciones de socorro humanitario".

32 Para profundizar en cómo se aplica el derecho internacional a esas operaciones, v. Kubo Mačák, Laurent Gisel y Tilman Rodenhäuser, "Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections?", *Just Security*, 27 de marzo de 2020, disponible en www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-lawprotections/. V. también *Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector*, mayo de 2020 (Declaración de Oxford), disponible en https://www.elac.ox.ac.uk/the-oxford-process/the-oxford-statement-on-ransomware-operations/#/.

33 L. Gisel y L. Olejnik (eds.), nota 11 *supra*, pp. 23-28. V. también Aron Heller, "Israeli cyber chief: Major attack on water systems thwarted", *ABC News*, 28 de mayo de 2020, disponible en https://abcnews.go.com/International/wireStory/israeli-cyber-chief-major-attack-water-systems-thwarted-70920855.

un SCI requiere una complejidad y un conocimiento específico y, con frecuencia, un software malicioso diseñado específicamente para ese ataque. Si bien los ataques a SCI no son tan frecuentes como otros tipos de ciberoperaciones, aparentemente, su frecuencia está en aumento y la gravedad de la amenaza ha evolucionado más rápidamente que lo que se preveía hace solo algunos años[34]. Los especialistas en ciberseguridad han señalado que "dada la posibilidad de que los ataques ciberfísicos tengan efectos cinéticos y causen víctimas, es de suma urgencia e importancia que la comunidad internacional de expertos en informática, los gobiernos y los letrados humanitarios inicien conversaciones sobre cómo regular el despliegue de los ataques ciberfísicos"[35].

Tal como se analizará más adelante, en un conflicto armado, el DIH confiere una protección integral al sector sanitario y prohíbe los ataques a la infraestructura civil, salvo que esta se haya convertido en un objetivo militar.

Más allá del impacto de las ciberoperaciones en determinada infraestructura, hay al menos tres de sus características que generan inquietud[36].

En primer lugar, si bien no es imposible atribuir un ciberataque a un Estado o a un actor no estatal, la tarea no es fácil[37]. Esto dificulta la posibilidad de identificar a los actores que violan el DIH en el ciberespacio y de hacerlos responsables, que es una forma de garantizar el cumplimiento del DIH. La posibilidad de negar la autoría de los ataques y la esperanza de que no se descubra también pueden alterar los cálculos políticos que requiere la ejecución de un ataque cibernético y la ejecución de esos ataques en infracción del derecho internacional.

En segundo lugar, como ha observado China, por ejemplo, "la proliferación de herramientas y tecnología cibernéticas [está] en aumento"[38]. Dadas sus características únicas, las herramientas y los métodos cibernéticos pueden proliferar de manera tal que resultan difíciles de controlar. Hoy en día, los ciberataques complejos solo los ejecutan los actores con más conocimiento y mejores recursos. Sin embargo, cuando se utiliza, se roba, se filtra o se obtiene de alguna otra manera un software malicioso, actores que no son los que lo desarrollaron podrían encontrarlo en línea, aplicarle ingeniería inversa y usarlo para sus propios fines.

En tercer lugar, las ciberoperaciones conllevan el riesgo de causar reacciones exageradas por parte de los Estados que sufren el ataque, con la consiguiente

34 Ibíd., p. 25.

35 Marina Krotofil, "Casualties caused through computer network attacks: The potential human costs of cyber warfare", 42.ª Mesa Redonda sobre cuestiones actuales relativas al derecho internacional humanitario, 2019, disponible en http://iihl.org/wp-content/uploads/2019/11/Krotofil1.pdf.

36 V. también CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, Ginebra, 2019 (Informe del CICR de 2019 sobre los desafíos de los conflictos armados contemporáneos), p. 27, disponible en https://www.icrc.org/es/publication/el-derecho-internacional-humanitario-y-los-desafios-de-los-conflictos-armados; L. Gisel y L. Olejnik (eds.), nota 11 *supra*, p. 7.

37 Para un análisis más pormenorizado en relación con la atribución, con referencia a las normas jurídicas internacionales pertinentes, v., más adelante, el apartado "La cuestión de la atribución".

38 Declaración del consejero de la delegación china, Sun Lei, en el Debate Temático sobre información y ciberseguridad en la Primera Comisión del 72.ª período de sesiones de la Asamblea General de la ONU, 23 de octubre de 2017, disponible en www.china-un.org/eng/chinaandun/disarmament_armscontrol/unga/t1505683.htm.

escalada de la violencia. Al objetivo del ciberataque, por lo general, le resulta difícil saber si el atacante tiene fines espionaje o de causar otros daños, posiblemente, físicos. La finalidad de una operación cibernética solo puede conocerse con certeza una vez que se logra el efecto o el objetivo final. En consecuencia, existe el riesgo de que el objetivo de una operación anticipe el peor impacto posible y reaccione con mayor contundencia que si supiera que el atacante solo tiene fines de espionaje.

En el momento de la redacción de este artículo, las ciberoperaciones no causan daños humanos importantes, pero sí daños económicos considerables[39]. En cuanto a los posibles costos humanos de las ciberoperaciones, no se sabe mucho acerca de la evolución tecnológica, las capacidades y las herramientas desarrolladas por los actores más avanzados –incluidos los militares– ni en qué medida el uso de ciberoperaciones durante los conflictos armados podría ser diferente de las tendencias observadas hasta ahora. Dicho de otro modo, si bien el riesgo de que se produzcan costos humanos no parece extremadamente alto sobre la base de las observaciones actuales, en especial, si se considera la destrucción y el sufrimiento que siempre causan los conflictos, la evolución de las ciberoperaciones requiere que se les preste atención, dada la incertidumbre que generan y la velocidad a la que evolucionan.

## La aplicabilidad del DIH a las ciberoperaciones durante los conflictos armados

Desde el punto de vista jurídico, el principal régimen que impone limitaciones al uso de ciberoperaciones durante los conflictos armados y protege a las poblaciones civiles de los posibles daños es el derecho internacional humanitario.

El DIH no contiene una definición de ciberoperaciones, ciberguerra o guerra cibernética y otras ramas del derecho internacional tampoco dan una definición de estos términos. En algunos Estados, se han empleado distintas definiciones en documentos militares y de otro tipo[40]. En otros Estados, se hace referencia a guerra informática o guerra digital, y la definición de este concepto incluye, al menos, algunos aspectos de lo que normalmente se entiende por

39 El costo general solo de los delitos informáticos es del orden de los billones de dólares. En 2015, la cifra fue de tres billones de dólares en todo el mundo, y las previsiones indican que se duplicará hacia 2021 (Steve Morgan, "Hackerpocalypse: A cybercrime revelation", Herjavec Group, 17 de agosto de 2016, disponible en www.herjavecgroup.com/hackerpocalypse-cybercrime-report/). Se calcula que el impacto económico de NotPetya fue de más de mil millones de dólares, y hay quienes estiman que superó los diez mil millones de dólares (Fred O'Connor, "NotPetya still roils company's finances, costing organizations $1.2 billion in revenue", *Cybereason*, 9 de noviembre de 2017, disponible en www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue; A. Greenberg, nota 5 *supra*). Con frecuencia, el sistema financiero también se ve afectado por los ataques cibernéticos; v., p. ej., Choe Sang-Hun, "Computer networks in South Korea are paralyzed in cyberattacks", *New York Times*, 20 de marzo de 2013, disponible en www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.

40 V., p. ej., Departamento de Defensa de Estados Unidos, *DOD Dictionary of Military and Associated Terms*.

ciberguerra[41]. Independientemente de cuál sea la definición de ciberoperaciones, ciberguerra o guerra informática que propongan los Estados y otros actores, la determinación de si el DIH se aplica a esas operaciones debe basarse en la naturaleza, las consecuencias y las circunstancias de las operaciones mismas.

El CICR entiende por "ciberoperaciones durante los conflictos armados" las operaciones contra una red o sistema informáticos, u otro dispositivo conectado, a través de un flujo de datos, cuando se usa como medio o método de guerra en el contexto de un conflicto armado[42].

Aunque el debate sobre la cuestión de si el DIH se aplica a las ciberoperaciones durante los conflictos armados y, en consecuencia, les impone limitaciones no está zanjado, el CICR ha adoptado desde el principio una posición clara y afirmativa[43]. A juicio del CICR, no existen dudas de que las ciberoperaciones durante los conflictos armados, o ciberguerra, se rigen por el DIH, al igual que cualquier arma, medio o método de guerra utilizado por un beligerante en un conflicto, sea este nuevo o antiguo. El hecho de que las ciberoperaciones se valen de una tecnología nueva que evoluciona continuamente no impide la aplicación del DIH al uso de esas tecnologías como medio o método de guerra. Esto es cierto sea que se considere al ciberespacio un nuevo dominio de la guerra comparable al aire, la tierra, el mar o el espacio ultraterrestre, que se lo considere un tipo de dominio diferente porque es artificial, mientras que los anteriores son naturales, o que no se lo considere un dominio de la guerra.

En nuestra opinión, se observa un claro apoyo a esta posición en los tratados de DIH, en la jurisprudencia de la Corte Internacional de Justicia (CIJ) y en las opiniones expresadas por algunos Estados y organizaciones internacionales.

El objeto y fin del DIH es regular conflictos futuros, es decir, los que tengan lugar tras la aprobación de un tratado de DIH. Siempre que se aprueba un tratado de DIH, los Estados incorporan normas que prevén el desarrollo de medios y métodos de guerra nuevos y suponen que el DIH se aplicará a ellos. Ya en 1868, la Declaración de San Petersburgo proponía que debían mantenerse los principios establecidos sobre "los perfeccionamientos que puedan producirse, que la ciencia

41 En el Acuerdo OCS, nota 17 *supra*, se define "guerra informática" como "una confrontación entre dos o más Estados en el espacio informático con el objeto de causar daño a sistemas, procesos y recursos informáticos de importancia crítica, así como a otras estructuras, con lo que se socavan sistemas políticos, económicos y sociales, se manipula psicológicamente a la población a fin de desestabilizar la sociedad y el Estado, y se obliga al Estado a tomar decisiones en favor de la parte adversaria". Las Fuerzas Armadas de la Federación de Rusia definen guerra informática de la misma manera y afirman que "las Fuerzas Armadas de la Federación de Rusia se rigen por […] el derecho internacional humanitario" durante las actividades militares en el espacio informático mundial (Ministerio de Defensa de la Federación de Rusia, *Russian Federation Armed Forces' Information Space Activities Concept*, 2011, apartado 2.1, disponible en https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle).

42 V. CICR, nota 1 *supra*.

43 V. CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, Ginebra, 2011 (Informe del CICR de 2011 sobre los desafíos de los conflictos armados contemporáneos), pp. 40-43, disponible en https://www.icrc.org/es/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-es.pdf; K. Dörmann, nota 12 *supra*.

pudiera introducir en el armamento de las tropas"[44]. Una importante norma del DIH más reciente al respecto se encuentra en el artículo 36 del Protocolo adicional I de 1977 (PA I)[45], que establece:

> 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.

No caben dudas de que esta obligación se basa en el supuesto de que el DIH se aplica a esas armas, medios y métodos de guerra nuevos; de lo contrario, no sería necesario revisar su licitud de conformidad con el derecho en vigor. Quedan incluidas las armas, medios y métodos de guerra que se basan en la tecnología digital.

La conclusión de que el DIH se aplica a las ciberoperaciones durante los conflictos armados se fundamenta también en las opiniones expresadas por la CIJ. En su Opinión consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares, la Corte destacó que los principios y las normas establecidos del derecho humanitario aplicables a los conflictos armados son válidos para "todas las formas de guerra y todos los tipos de armas", incluso "las del futuro"[46]. Aquí también quedan incluidas las ciberoperaciones. Esta opinión ha encontrado un amplio consenso entre los expertos[47].

El reconocimiento de los Estados de que el derecho internacional se aplica en el ciberespacio y, en especial, de que el DIH se aplica a las ciberoperaciones durante los conflictos armados y, por lo tanto, les impone limitaciones es cada vez mayor. Como se ha observado, en los informes del GEG de la ONU de 2013 y 2015, los expertos arribaron a la conclusión de que "el derecho internacional, en particular

44 Declaración de San Petersburgo de 1868 con el objeto de prohibir el uso de determinados proyectiles en tiempo de guerra, San Petersburgo, 29 de noviembre - 11 de diciembre de 1868.

45 Protocolo adicional (I) a los Convenios de Ginebra del 12 de agosto de 1949 relativos a la protección de las víctimas de los conflictos armados internacionales, 1125 UNTS 3, 8 de junio de 1977 (en vigor desde el 7 de diciembre de 1978).

46 CIJ, *Legalidad de la amenaza o el empleo de armas nucleares*, Opinión consultiva, 8 de julio de 1996, párr. 86.

47 V. Manual de Tallin 2.0, nota 13 *supra*, norma 80; Declaración de Oxford, nota 32 *supra*, punto 5. V. también el artículo de Zhixiong Huang y Yaohui Ying publicado en este número de la *International Review*; y v. Ma Xinmin, que en ese momento era subdirector general del Departamento de Tratados y Derecho del Ministerio de Asuntos Exteriores de la República Popular China, que escribió a título personal: "[E] l alcance de la aplicabilidad de las normas del DIH se ha extendido. […] [A]simismo, se ha ampliado al ciberespacio. El GEG sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional en sus informes de 2013 y 2015 asegura que el derecho internacional, en particular, la Carta de la ONU, es aplicable en el ciberespacio. Así pues, el DIH debería, en principio, ser aplicable a los ataques cibernéticos, pero cómo aplicarlo es aún tema de debate" (traducción informal no oficial). Ma Xinmin, "International humanitarian law in flux: Development and new agendas – In commemoration of the 40th anniversary of the 1977 Protocols to the Geneva Conventions", *Chinese Review of International Law*, vol. 30, n.º 4, 2017, p. 8.

la Carta de las Naciones Unidas, es aplicable" en el entorno de las tecnologías de la información y las comunicaciones[48], conclusión que ha sido acogida primero con beneplácito[49] y, posteriormente, confirmada[50] por la Asamblea General de la ONU. El informe de 2015 también señalaba la existencia de "principios jurídicos internacionales establecidos, incluidos, si procede, los principios de humanidad, necesidad, proporcionalidad y distinción"[51]. Si bien en esta enumeración de principios no se hace mención expresa del DIH, los expertos han señalado que estos son "principios fundamentales del DIH"[52].

En consonancia con esa conclusión, un número cada vez mayor de Estados y organizaciones internacionales han afirmado públicamente que el DIH se aplica a las ciberoperaciones durante los conflictos armados; entre otros, la UE[53] y la OTAN[54]. Asimismo, el Llamamiento de París para la confianza y la seguridad en el ciberespacio (que contaba con el apoyo de setenta y ocho Estados en abril de 2020) ha reivindicado la aplicabilidad del DIH a las ciberoperaciones durante los conflictos armados[55]; los jefes de gobierno de cincuenta y cuatro Estados de la Mancomunidad de Naciones se han "[c]ompromet[ido] a avanzar en el debate sobre cómo […] se aplica el derecho internacional humanitario aplicable al ciberespacio en todos sus aspectos"[56]; y las respuestas de los Estados a un cuestionario preparado por el Comité Jurídico Interamericano de la OEA ha "reflej[ado] apoyo a la aplicabilidad del derecho internacional humanitario" en el ciberespacio[57].

A la vez, en el contexto de los debates sobre la aplicabilidad del DIH a las ciberoperaciones durante los conflictos armados, algunos Estados han expresado su oposición a la militarización del ciberespacio o a una carrera armamentista

48 Asamblea General de la ONU, "Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional: Nota del Secretario General", doc. ONU A/68/98, 24 de junio de 2013, párr. 19, y doc. ONU A/70/174, 22 de julio de 2015, párr. 24.

49 Asamblea General de la ONU, res. 70/237, "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional", doc. ONU A/RES/70/237, 30 de diciembre de 2015, párr. 16 del preámbulo.

50 Asamblea General de la ONU, res. 73/27, nota 15 *supra*, párr. 17 del preámbulo; Asamblea General de la ONU, res. 73/266, nota 15 *supra*, párr. 12 del preámbulo.

51 Doc. ONU A/70/174, nota 48 *supra*, párr. 28(d).

52 Michael N. Schmitt, "France speaks out on IHL and cyber operations: Part I", *EJIL: Talk!*, 30 de septiembre de 2019, disponible en www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-i/.

53 Conclusiones del Consejo Europeo, nota 20 *supra*.

54 Declaración de Gales, nota 21 *supra*, párr. 72.

55 V. "Llamamiento de París para la confianza y la seguridad en el ciberespacio", 12 de noviembre de 2018, *Francia Diplomacia*, disponible en https://www.diplomatie.gouv.fr/es/politica-exterior/francia-en-naciones-unidas/alianza-por-el-multilateralismo/article/llamamiento-de-paris-para-la-confianza-y-la-seguridad-en-el-ciberespacio.

56 Declaración sobre el ciberespacio de la Mancomunidad de Naciones, nota 19 *supra*, p. 4, párr. 4.

57 V. OEA, nota 22 *supra*, párr. 43 (donde se hace mención a Bolivia, Chile, Estados Unidos, Guyana y Perú); la respuesta de Ecuador parece indicar su apoyo (v. también párrs. 19-21, 25). Otros Estados miembros de la OEA expresaron su posición en el contexto del GTCA. V. comentarios de Brasil, Colombia y Uruguay en el primer anteproyecto del informe del GTCA, disponible en www.un.org/disarmament/open-ended-working-group/. V., en cambio, las opiniones de Cuba, Nicaragua y Venezuela, que observan, entre otras cuestiones, que aún no existe consenso en cuanto a la aplicabilidad del DIH en el ciberespacio y que la referencia directa al DIH en el informe puede validar o determinar la licitud de la militarización del ciberespacio.

en ese ámbito. Los Estados también expresaron su preocupación respecto de la posible legitimación del uso de ciberoperaciones militares[58], llamaron a emplear la prudencia en los debates sobre la aplicabilidad del DIH[59] y observaron que el DIH "debe aplicarse teniendo en cuenta las peculiaridades de la guerra cibernética"[60]. Estas consideraciones son importantes, pero no deberá entenderse como incompatibles con la aplicación del DIH a las ciberoperaciones durante los conflictos armados.

A nuestro juicio, sin embargo, asegurar que el DIH se aplica a las ciberoperaciones durante los conflictos armados no es un estímulo para militarizar el ciberespacio y no debería entenderse, de ninguna manera, como una legitimización de la guerra cibernética[61]. Cualquier recurso a la fuerza, sea de naturaleza cibernética o cinética, por parte de los Estados, se rige siempre por la Carta de la ONU y el derecho internacional consuetudinario, en particular, respecto de la prohibición del uso de la fuerza[62]. Las disputas internacionales deben resolverse por

58 V., más recientemente, las propuestas de China, Cuba, Irán, Nicaragua y Rusia, entre otras, relativas al primer anteproyecto del informe del GTCA, disponible en www.un.org/disarmament/open-ended-working-group/. V. también, p. ej., República Popular China, documento de posición de la República Popular China para el 73.º período de sesiones de la Asamblea General de las Naciones Unidas, 2018, p. 10, disponible en https://tinyurl.com/y4qquywp; "Declaración de Miguel Rodríguez, representante de Cuba, en la sesión final del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional", 23 de junio de 2017, p. 2; Ministerio de Asuntos Exteriores de la Federación de Rusia, "Response of the Special Representative of the President of the Russian Federation for international cooperation on information security Andrey Krutskikh to TASS' question concerning the state of international dialogue in this sphere", 29 de junio de 2017.

59 "La aplicabilidad del derecho de los conflictos armados y el *jus ad bellum* requiere prudencia. La licitud de la guerra cibernética no debería estar reconocida bajo ninguna circunstancia. Los Estados no deberán convertir el ciberespacio en un nuevo campo de batalla": "China's submissions to the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security", septiembre de 2019, p. 6, disponible en https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf. "Deberíamos ser extremadamente cautos respecto de cualquier intento de introducir el uso de la fuerza en cualquiera de sus formas en el ciberespacio, hacer una evaluación seria de los posibles conflictos y confrontaciones que surgieran de la aplicación indiscriminada del derecho de los conflictos armados en el ciberespacio y abstenernos de enviar mensajes equivocados al mundo": "China's contribution to the initial pre-draft of OEWG report", abril de 2020, p. 5, disponible en https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf. "[S]in la práctica de los Estados, debemos ser prudentes en el debate sobre la aplicación del derecho humanitario en las denominadas 'ciberguerras'. La razón es muy simple, pero no por ello menos fundamental: en primer lugar, las ciberguerras no deberían estar permitidas y, en segundo lugar, la ciberguerra será una forma completamente novedosa de guerra tecnológica": Declaración de China durante la 58.ª sesión anual de AALCO, en AALCO, *Verbatim Record of Discussions: Fifty-Eighth Annual Session*, doc. n.º AALCO/58/DAR ES SALAAM/2019/VR, 2019, p. 176, disponible en www.aalco.int/Verbatim%20(FINAL)%2020200311.pdf.

60 China ha afirmado en una reunión del Grupo de Trabajo de AALCO sobre derecho internacional en el ciberespacio que "los regímenes de *jus ad bellum* y *jus in bello* deben aplicarse tomando en consideración las peculiaridades de la guerra cibernética". AALCO, *Summary Report of the Fourth Meeting of the Open-ended Working Group on International Law in Cyberspace*, 3 de septiembre de 2019, disponible en www.aalco.int/Summary%20Report%20as%20Adopted.pdf.

61 Esta opinión también ha sido expresada en las propuestas de Australia, Brasil, Chile, Dinamarca y Reino Unido, entre otras, sobre el primer anteproyecto del informe del GTCA, disponible en www.un.org/disarmament/open-ended-working-group/.

62 Carta de la ONU, art. 2(4).

medios pacíficos. Este principio se aplica en el ciberespacio y en todos los demás dominios. Además de los requisitos de la Carta de la ONU, e independientemente de ellos, el DIH impone límites a la conducción de las hostilidades cuando los Estados o las partes no estatales deciden recurrir a ciberoperaciones durante los conflictos armados. En concreto, el DIH confiere protección a los civiles y los bienes de carácter civil contra los efectos de las hostilidades al restringir la elección de los medios y métodos de guerra por los beligerantes, independientemente de si el uso de la fuerza es lícito o no. Esto quiere decir que, en lugar de legitimar las ciberoperaciones (o cualquier otra operación militar) durante un conflicto armado, el DIH –el *jus in bello*– proporciona límites además de los que se encuentran en la Carta de la ONU y el derecho internacional consuetudinario, el *jus ad bellum*. Más aun, el DIH impone, de hecho, algunos límites a la militarización del ciberespacio. Por ejemplo, prohíbe el desarrollo de capacidades cibernéticas que se considerarían armas y que, por su naturaleza, tendrían efectos indiscriminados o causarían daños superfluos o sufrimientos innecesarios[63].

Si se acepta que el DIH se aplica a las ciberoperaciones durante los conflictos armados en general, la siguiente pregunta es si se aplican todas o solo algunas de las normas del DIH. En este sentido, el alcance de la aplicación de las normas del DIH que rigen los medios y métodos de la guerra puede dividirse, en líneas generales, en normas que se aplican a todas las armas, medios y métodos de guerra, dondequiera que se usen (como los principios de distinción, proporcionalidad y precaución), y normas específicas para algunas armas en particular (como los tratados de armas) o determinados dominios (como las normas que rigen específicamente la guerra marítima). Todos los principios y normas consuetudinarios fundamentales que rigen la conducción de las hostilidades pertenecen a la primera categoría y se aplican a las ciberoperaciones durante los conflictos armados[64]. En cambio, es necesario hacer un análisis más minucioso para la aplicabilidad de las normas del DIH específicas para algunas armas en particular o determinados dominios.

El hecho de que se aplique el DIH no impide que los Estados continúen desarrollando el derecho internacional, acuerden sobre normas de carácter voluntario o traten de llegar a un consenso sobre la interpretación común de las normas en vigor. Por ejemplo, cuando se estableció un GTCA de la ONU en 2018, la mayoría de Estados de la Asamblea General de la ONU "acog[ió] con beneplácito" un conjunto de "normas, reglas y principios de comportamiento responsable de los Estados" basados en las normas elaboradas a lo largo de los años por los GEG de la ONU[65]. Otro ejemplo de posibles normas nuevas en el campo de la seguridad de la información se encuentra en el Código Internacional de Conducta para la seguridad

63 V. Jean-Marie Henckaerts y Louise Doswald-Beck (eds.), *El derecho internacional humanitario consuetudinario. Volumen I: Normas*, CICR, Buenos Aires, 2007 (Estudio del CICR sobre derecho internacional consuetudinario), normas 70, 71, disponible en https://www.icrc.org/es/doc/assets/files/other/icrc_003_pcustom.pdf.

64 Los principios y las normas que rigen la conducción de las hostilidades se presentan más adelante, en el apartado "Los límites que impone el DIH al uso de las capacidades cibernéticas durante los conflictos armados".

65 Asamblea General de la ONU, res. 73/27, nota 15 *supra*.

de la información, presentada en 2011 ante la ONU por los Estados miembros de la OCS. En virtud del Código, los Estados deberían comprometerse, entre otras cosas, a "evitar la proliferación de las armas informáticas y las tecnologías relacionadas"[66]. Asimismo, existen propuestas académicas, incluso respecto de sumar restricciones jurídicas o de políticas a las ciberoperaciones durante los conflictos armados[67].

En resumen, si bien existen razones jurídicas convincentes y un creciente apoyo internacional para concluir que el DIH se aplica a las ciberoperaciones durante los conflictos armados, esta cuestión aún no goza de acuerdo universal. Como se ha mostrado en este apartado, sin embargo, un examen minucioso de los distintos argumentos esgrimidos en debates multilaterales muestra que reivindicar la aplicabilidad del DIH no legitima ni la militarización del ciberespacio ni el uso de ciberoperaciones maliciosas. Tampoco anula la posibilidad de desarrollar nuevas normas, sino que proporciona un marco jurídico fundamental que podría –y debería– servir de base para su posible desarrollo.

## ¿Las ciberoperaciones puede por sí solas atravesar "el umbral"? Precisar la diferencia entre los umbrales relevantes del DIH y la Carta de la ONU

En vista de las numerosas ciberoperaciones que se conocen a diario, es importante recordar que el DIH solo se aplica a ciberoperaciones que forman parte de un conflicto armado en el que, por lo demás, se emplean armas convencionales o, en menor medida, ciberoperaciones que por sí solas no constituyen un conflicto armado en ausencia de armas cinéticas. Como se ha destacado en el apartado anterior, la cuestión de si el DIH se aplica a las ciberoperaciones durante los conflictos armados debe analizarse aparte de si ha habido una violación de las normas que rigen el uso de la fuerza de conformidad con la Carta de la ONU. En el contexto de la aplicación del DIH y la Carta de la ONU, un tema fundamental

66 La propuesta de Código Internacional de Conducta para la seguridad de la información está disponible en http://nz.chineseembassy.org/eng/zgyw/t858978.htm. Fue presentada por China, la Federación de Rusia, Tayikistán y Uzbekistán en 2011, y fue copatrocinada por Kazajistán y Kirguistán en 2013 (v. doc. ONU A/68/98, nota 48 *supra*, p. 8, párr. 18). En 2011, el Ministerio de Asuntos Exteriores de la Federación de Rusia presentó también un proyecto de Convenio sobre seguridad internacional de la información (22 de septiembre de 2011, disponible en www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666) donde, entre las principales medidas enumeradas para prevenir los conflictos militares en el espacio de la información, figura que los Estados deberán "tomar medidas destinadas a limitar la proliferación de 'armas informáticas' y de la tecnología para su creación" (art. 6(10)). El art. 7(2), también prevé que "[e]n cualquier conflicto internacional, el derecho de los Estados Partes involucrados en el conflicto de elegir los medios de 'guerra digital' está limitado por las normas del derecho internacional humanitario aplicables".

67 Entre muchos otros autores, Pascucci, por ejemplo, ha propuesto que la negociación de un Protocolo adicional IV podría abordar las cuestiones que plantea la aplicación de los principios de distinción y proporcionalidad en el ciberespacio: Peter Pascucci, "Distinction and proportionality in cyberwar: Virtual problems with a real solution", *Minnesota Journal of International Law*, vol. 26, n.º 2, 2017. Schmitt, en tanto, presentó propuestas en términos de políticas que podrían adoptar los Estados: Michael N. Schmitt, "Wired warfare 3.0: Protecting the civilian population during cyber operations", *International Review of the Red Cross*, vol. 101, n.º 910, 2019 [trad. esp. "Guerra conectada 3.0: protección de la población civil durante las operaciones cibernéticas", disponible en https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-07/910-schmitt_OK.pdf].

es la atribución de las ciberoperaciones a los Estados. Esos tres aspectos –qué ciberoperaciones se rigen por el DIH[68], la relación entre el DIH y la Carta de la ONU y la cuestión de la atribución– se analizan en este apartado.

## Ciberoperaciones regidas por el DIH

Cuando las ciberoperaciones se ejecutan en el contexto de un conflicto armado internacional o no internacional en curso que se desarrolla con medios cinéticos –y tienen un nexo con dicho conflicto–, las normas del DIH pertinentes se aplican a todas las partes en conflicto y regulan su comportamiento[69]. Las ciberoperaciones realizadas en conjunto con operaciones cinéticas o en apoyo de estas durante un conflicto armado son el único tipo de operaciones que los Estados han reconocido y considerado que están regidas por el DIH[70].

Otra cuestión independiente es si las ciberoperaciones por sí solas –en ausencia de operaciones cinéticas– pueden regirse por el DIH. Dicho de otro modo, ¿una operación cibernética puede ser el primer ataque, y posiblemente el único, en un conflicto armado tal como lo define el DIH? Es necesario evaluar esta cuestión a la luz de los artículos 2 y 3 comunes a los cuatro Convenios de Ginebra de 1949[71] para conflictos armados internacionales y no internacionales, respectivamente[72]. Esos dos tipos de conflicto armado difieren en cuanto a la naturaleza de las partes que participan en ellos, la intensidad de la violencia que desencadena la aplicabilidad del DIH y algunas de las normas del DIH aplicables.

Con respecto a los conflictos internacionales, el artículo común 2 prevé que "el presente Convenio se aplicará en caso de guerra declarada o de cualquier otro conflicto armado que surja entre dos o varias de las Altas Partes Contratantes, aunque una de ellas no haya reconocido el estado de guerra". En la actualidad, hay consenso en cuanto a que "un conflicto armado existe siempre que haya 'un recurso

68 Para un ejemplo de estos debates, v. "Scenario 13: Cyber operations as a trigger of the law of armed conflict", en Kubo Mačák, Tomáš Minárik y Taťána Jančárková (eds.), *Cyber Law Toolkit*, disponible en https://cyberlaw.ccdcoe.org/.

69 V. CICR, *Comentario del Primer Convenio de Ginebra: Convenio (I) para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña*, Ginebra, 2021 (Comentario del CICR del CG I), párr. 254; Manual de Tallin 2.0, nota 13 *supra*, norma 80.

70 V. referencias en nota 2 *supra*.

71 Convenio de Ginebra (I) del 12 de agosto de 1949 para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña, 75 UNTS 31 (en vigor desde el 21 de octubre de 1950) (CG I); Convenio de Ginebra (II) del 12 de agosto de 1949 para aliviar la suerte que corren los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar, 75 UNTS 85 (en vigor desde el 21 de octubre de 1950) (CG II); Convenio de Ginebra (III) del 12 de agosto de 1949 relativo al trato debido a los prisioneros de guerra, 75 UNTS 135 (en vigor desde el 21 de octubre de 1950) (CG III); Convenio de Ginebra (IV) del 12 de agosto de 1949 relativo a la protección debida a las personas civiles en tiempo de guerra, 75 UNTS 287 (en vigor desde el 21 de octubre de 1950) (CG IV).

72 Art. 2(1) común: "[E]l presente Convenio se aplicará en caso de guerra declarada o de cualquier otro conflicto armado que surja entre dos o varias de las Altas Partes Contratantes, aunque una de ellas no haya reconocido el estado de guerra". Art. 3(1) común: "En caso de conflicto armado que no sea de índole internacional y que surja en el territorio de una de las Altas Partes Contratantes".

a la fuerza armada entre Estados'"[73]. Con respecto a la cuestión de si existe un umbral de intensidad para los conflictos armados internacionales, algunas prácticas de los Estados y determinados argumentos humanitarios y conceptuales de peso indican que el DIH se aplica en cuanto se emplea la fuerza armada entre Estados, independientemente de la intensidad de la violencia. El DIH guarda relación principalmente con la protección de las personas afectadas por los conflictos armados. Así pues, en cuanto usan la fuerza armada, los Estados deben dirigir sus ataques contra objetivos militares y no contra civiles o bienes de carácter civil, y deben procurar constantemente evitar atacar a estos últimos. No se trata de si hay uno o más civiles que necesitan protección contra los ataques[74]. Al menos cuando el uso de ciberoperaciones entre Estados tiene consecuencias similares a las de los medios y métodos de guerra más tradicionales, se aplica el DIH.

En general, los expertos coinciden en que las ciberoperaciones, por sí solas, tienen el potencial de cruzar el umbral de un conflicto armado internacional de conformidad con el DIH[75]. El CICR es de la misma opinión[76]. En una inusual expresión de la posición de un Estado al respecto, Francia ha afirmado que "[l]as ciberoperaciones que constituyen hostilidades entre dos o más Estados pueden determinar la existencia de un conflicto armado internacional"[77].

La pregunta de dónde se ubica exactamente ese umbral aún no tiene respuesta[78]. A criterio del CICR, no existen motivos para tratar una o más ciberoperaciones cuya consecuencia sea la destrucción de bienes civiles o militares, o la muerte o las lesiones de soldados o civiles, de manera distinta de la que se tratan ataques equivalentes ejecutados con medios y métodos de guerra más tradicionales. Las ciberoperaciones, sin embargo, podrían dejar inutilizados algunos objetos sin dañarlos físicamente. Queda por ver en qué condiciones, si cabe, los Estados podrían considerar que esas operaciones equivalen a un recurso a la fuerza armada

73 Tribunal Penal Internacional para ex Yugoslavia (TPIY), *The Prosecutor v. Duško Tadić*, caso n.º IT-94-1, decisión sobre la petición de la defensa de interponer recurso interlocutorio sobre la jurisdicción, 2 de octubre de 1995, párr. 70; Comentario del CICR del CG I, nota 69 *supra*, párr. 218.

74 De manera análoga, si el recurso a la fuerza armada tiene como consecuencia lesiones o la captura de un miembro de las fuerzas armadas de otro Estado, rigen las normas del DIH sobre la protección de los heridos y los enfermos o el estatuto y el trato debido a los prisioneros de guerra, haya uno o más prisioneros o uno o más heridos a los que se deba asistir. V. Comentario del CICR del CG I, nota 69 *supra*, párrs. 236-244.

75 Manual de Tallin 2.0, nota 13 *supra*, norma 82, párr. 16.

76 Comentario del CICR del CG I, nota 69 *supra*, párrs. 253-256.

77 Ministerio de los Ejércitos de Francia, *International Law Applied to Operations in Cyberspace*, 2019, p. 12, disponible en www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf. En el documento, se especifica que "[s]i bien en principio no puede desestimarse al existencia de un conflicto armado en el que se ejecutan exclusivamente acciones digitales, dicha existencia se basa en la capacidad de las ciberoperaciones autónomas de alcanzar el umbral de violencia requerido".

78 Manual de Tallin 2.0, nota 13 *supra*, norma 82, párrs. 11-16; como se deduce de los párrs. 12-13, la cuestión tampoco está zanjada para las operaciones cinéticas, y esa incertidumbre impregna el debate acerca de si las operaciones cibernéticas por sí solas pueden cruzar el umbral de un conflicto armado internacional más allá de las cuestiones específicas del ámbito cibernético.

de conformidad con el DIH y que, por lo tanto, han de regirse por este cuerpo jurídico[79].

En cuanto a los conflictos armados de índole no internacional, las situaciones de violencia interna pueden catalogarse de conflictos armados no internacionales si existe "violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados o entre dichos grupos dentro de un Estado"[80]. Los dos criterios que se desprenden de esta definición –la organización de las partes en conflicto y la intensidad de la violencia– plantean distintos interrogantes respecto de las ciberoperaciones. En primer lugar, mientras que las fuerzas armadas estatales satisfacen el criterio referido a la organización, determinar el nivel de organización de un grupo armado requiere una evaluación más compleja que se centra en hechos específicos; la cuestión es aún más complicada –aunque no imposible de resolver– cuando ese grupo cuenta con una organización exclusivamente virtual[81]. En segundo lugar, a diferencia del DIH aplicable a los conflictos armados internacionales, que rige todo recurso a la fuerza armada entre Estados sin que sea relevante la intensidad[82], un conflicto armado no internacional solo existe si la violencia entre dos o más partes organizadas alcanza la intensidad suficiente. Nuevamente, si bien se podría sostener que no es imposible en circunstancias excepcionales, es improbable que las ciberoperaciones por sí solas alcancen el grado de intensidad requerido para constituir un conflicto armado no internacional[83]. Si bien ha expresado la opinión de que las ciberoperaciones prolongadas pueden, en principio y según las circunstancias, constituir un conflicto armado no internacional, Francia sostuvo que dado el estado actual de la tecnología habría que descartar la posibilidad por el momento[84].

Se ha señalado, con justa razón, que el derecho de los conflictos armados "no rige las ciberoperaciones que no se ejecutan en el contexto de un conflicto armado"[85]. No obstante, no todas las opiniones coinciden en cuanto a si deberían aplicarse algunos de sus principios, como materia de política, a las ciberoperaciones en todo momento.

Recientemente, Estados Unidos declaró que "aunque el derecho de la guerra no sea técnicamente aplicable porque las operaciones militares cibernéticas

79 Comentario del CICR del CG I, nota 69 *supra*, párr. 255; Manual de Tallin 2.0, nota 13 *supra*, norma 82, párr. 11.

80 TPIY, *The Prosecutor v. Duško Tadić*, nota 73 *supra*, párr. 70.

81 Comentario del CICR del CG I, nota 69 *supra*, párr. 437; Manual de Tallin 2.0, nota 13 *supra*, norma 83, párrs. 13-15. Para un análisis pormenorizado de esta cuestión, v. Tilman Rodenhäuser, *Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law*, Oxford University Press, Oxford, 2018, pp. 104-108.

82 Comentario del CICR del CG I, nota 69 *supra*, párrs. 236-244.

83 Ibíd., párr. 437. Para un análisis más profundo, v. Manual de Tallin 2.0, nota 13 *supra*, norma 83, párrs. 7-10; Cordula Droege, "Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross*, vol. 94, n.º 886, 2012, p. 551; Michael N. Schmitt, "Classification of cyber conflict", *Journal of Conflict and Security Law*, vol. 17, n.º 2, 2012, p. 260.

84 Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 12.

85 Fuerza de Defensa de Nueva Zelanda, *Manual of Armed Forces Law*, vol. 4: *Law of Armed Conflict* (Manual Militar de Nueva Zelanda), segunda edición, DM 69, 2017, párr. 5.2.23, disponible en https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/DM-69-2ed-vol4.pdf.

propuestas no tendrían lugar en el contexto de un conflicto armado, de todos modos, [el Departamento de Defensa] aplica los principios del derecho de la guerra"[86] al igual que en el resto de sus operaciones[87]. Por el contrario, la Federación de Rusia ha advertido contra "los intentos […] potencialmente peligrosos de imponer el principio de aplicabilidad plena y automática del DIH al entorno de las TIC en tiempo de paz"[88].

Si bien es probable que los debates sobre políticas en esta materia continúen, desde el punto de vista jurídico, es incuestionable que el DIH no se aplica fuera del contexto de un conflicto armado. Es cierto que algunas normas del DIH, como la protección de las personas que no participan o han dejado de participar en las hostilidades, consagrada en el artículo 3 común, o la firme protección de los establecimientos sanitarios o los bienes indispensables para la supervivencia de la población civil, podrían tener consecuencias positivas si se aplicaran en todo momento. Por el contrario, otras normas del DIH podrían ser más difíciles de aplicar fuera del contexto de un conflicto armado, en particular, las que derivan de los principios de distinción y proporcionalidad. Esas normas se basan en la premisa de que los ataques contra objetivos militares son lícitos de conformidad con el DIH durante los conflictos armados. Sin embargo, fuera del contexto de un conflicto armado, la noción de "objetivos militares" que pueden ser objeto de ataques lícitos no existe; incluso los ataques a las fuerzas armadas de otro Estado están prohibidos. Si bien el principio de proporcionalidad también existe fuera de los conflictos armados, tiene un significado distinto en otros cuerpos jurídicos y, por lo tanto, funciona de manera diferente durante los conflictos armados y fuera de estos[89]. En contextos distintos de un conflicto armado, las disputas entre Estados y el uso de la fuerza están regulados solo por otras ramas del derecho internacional, como la Carta de la ONU y el derecho de los derechos humanos, según corresponda.

## La relación entre el DIH y la Carta de la ONU

Un Estado que esté considerando dirigir una operación cibernética contra otro Estado debe analizar la licitud de dicha operación conforme al *jus ad bellum*

86 Paul C. Ney Jr., Consejo General del Departamento de Defensa de EE. UU., "DOD General Remarks at U.S. Cyber Command Legal Conference", 2 de marzo de 2020, disponible en www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

87 V. Departamento de Defensa (DoD, por su sigla en inglés) de Estados Unidos, directiva 2311.01E, "DoD law of war program", 2006 (modificado en 2011), párrs. 4-4.1: "La política del DoD determina que […] [l]os miembros de los Componentes del DoD cumplen el derecho de la guerra durante todos los conflictos armados, independientemente de la caracterización de dichos conflictos, *así como en todas las demás operaciones militares*" (cursiva añadida). V. también DoD, *Law of War Manual* (Manual de derecho de la guerra del DoD), 2015, párr. 3.1.1.2, disponible en https://tinyurl.com/y6f7chxo.

88 Federación de Rusia, "Commentary of the Russian Federation on the initial 'pre-draft' of the final report of the United Nations Open-ended Working Group on developments in the field of information and telecommunications in the context of international security", abril de 2020, disponible en https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf.

89 Para un análisis somero, v. Informe del CICR de 2019 sobre los desafíos de los conflictos armados contemporáneos, nota 36 *supra*, pp. 18-22.

(fundamentado en la Carta de la ONU y el derecho internacional consuetudinario) y al *jus in bello* (DIH). Aun cuando pertenecen a ramas distintas del derecho internacional, la Carta de la ONU y el DIH son complementarios a la hora de proteger a las personas contra la guerra y sus consecuencias. Sus objetivos son complementarios: mientras que el preámbulo de la Carta de la ONU establece como objetivo "preservar a las generaciones venideras del flagelo de la guerra", el preámbulo del PA I establece el objetivo del DIH: "proteg[er] a las víctimas de los conflictos armados". En concreto, la Carta de la ONU prohíbe el uso de la fuerza, salvo cuando se recurre a ella en defensa propia o cuando lo autoriza el Consejo de Seguridad. La aplicabilidad del DIH no reemplaza ni desplaza las normas fundamentales de la Carta de la ONU, pero si se desata un conflicto armado, el DIH prevé protecciones para quienes no participan (civiles) o han dejado de participar en las hostilidades (soldados heridos, personas detenidas) y limita la elección de los medios y métodos de guerra por parte de los beligerantes. Por ello, mientras que la Carta de la ONU establece la prohibición del uso de la fuerza –sujeta a unas pocas excepciones–, el DIH impone límites a cómo pueden conducirse las hostilidades una vez que se desata el conflicto.

A la vez, el DIH y la Carta de la ONU son instrumentos que pertenecen a distintos campos del derecho internacional, cada uno con sus propios conceptos y terminología. Dado que ambos contienen disposiciones relativas al uso de la fuerza, parte de la terminología que utilizan es similar y, a veces, puede resultar confusa. Es el caso, por ejemplo, de la noción de "recurso a la fuerza armada entre Estados" para clasificar un conflicto de conformidad con el DIH, y de la prohibición de recurrir "a la amenaza o al uso de la fuerza" y el derecho a la defensa personal contra un "ataque armado" según la Carta de la ONU. Si bien los tratados de derecho internacional no proporcionan una definición de esas nociones –ni en general ni en el ámbito del ciberespacio–, algunos elementos básicos pueden inferirse de la jurisprudencia y los comentarios.

Como se ha observado, el DIH se aplica tan pronto como existe un recurso a la fuerza armada entre Estados, sin que sea relevante la intensidad de la violencia.

La Carta de la ONU no proporciona una definición del término "uso de la fuerza" en su artículo 2(4), y la cuestión del tipo de fuerza empleada es materia de debate. Observando la historia de la redacción de la disposición y la práctica posterior de los Estados, es posible concluir que el recurso a la coerción política o económica no está incluido en la noción de uso de la fuerza[90]. Por el contrario, se ha propuesto que la prohibición de usar la fuerza según la Carta de la ONU se "limita a la fuerza armada"[91]. Es importante observar que, respecto de las

90 V. Oliver Dörr y Albrecht Randelzhofer, "Article 2(4)", en Bruno Simma et al. (eds.), *The Charter of the United Nations: A Commentary*, vol. 1, Oxford University Press, Oxford, 2016, párrs. 17-20 del comentario del art. 2(4). En consecuencia, los expertos han llegado a la conclusión de que "ni las ciberoperaciones psicológicas no destructivas destinadas exclusivamente a minar la confianza en un gobierno ni la prohibición por parte de un Estado de realizar transacciones de comercio electrónico con otro Estado con la intención de generar consecuencias económicas negativas califican como usos de la fuerza": Manual de Tallin 2.0, nota 13 *supra*, párr. 3 del comentario de la norma 69.

91 O. Dörr y A. Randelzhofer, nota 90 *supra*, p. 208, párr. 16.

ciberoperaciones, la CIJ ha determinado que el artículo 2(4) prohíbe "cualquier uso de la fuerza, independientemente de las armas empleadas"[92]. Sobre la base de esta observación, algunos Estados han hecho hincapié en que "atravesar el umbral del uso de la fuerza no depende de los medios digitales empleados, sino de los efectos de la ciberoperación" y, en consecuencia, han arribado a la conclusión de que una "ciberoperación ejecutada por un Estado contra otro Estado es violatoria de la prohibición del empleo de la fuerza cuando sus efectos son similares a aquellos que resultan del uso de armas convencionales"[93]. Hay ejemplos del uso de la fuerza en el ciberespacio proporcionados por los Estados que parecen reflejar esta opinión, por ejemplo, realizar ciberoperaciones que causan lesiones o la muerte de personas, o daño o destrucción de bienes[94]; provocar el colapso de una planta nuclear; abrir un dique sobre una zona poblada que cause destrucción; inhabilitar los servicios de control de tráfico aéreo de modo de provocar accidentes aéreos; y destruir los sistemas logísticos de las fuerzas armadas[95]. Algunos Estados parecen interpretar incluso más ampliamente la prohibición del uso de la fuerza, sosteniendo que no puede descartarse que "una ciberoperación sin efectos físicos también pueda caracterizarse como un caso de uso de la fuerza"[96] o que "una operación cibernética con un impacto económico o financiero muy grave pueda equipararse al uso de la fuerza"[97].

Volviendo al derecho a la defensa propia en la Carta de la ONU y en el derecho internacional consuetudinario, ese derecho solo puede ejercerse contra un "ataque armado". De acuerdo con la observación de la CIJ de que solo "las formas más graves del uso de la fuerza" pueden considerarse ataques armados y que dichos ataques deben alcanzar "una magnitud y unos efectos" determinados[98],

92 CIJ, nota 46 *supra*, párr. 39.

93 Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 7. V. también Manual de Tallin 2.0, nota 13 *supra*, párr. 1 del comentario de la norma 69.

94 V. Estonia, "President of the Republic at the opening of CyCon 2019", 29 de mayo de 2019, disponible en www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html. Departamento de Asuntos Exteriores y Comercio de Australia, "Australia's international cyber engagement strategy", 2019, disponible en https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf.

95 Manual de derecho de la guerra del DoD, nota 87 *supra*, párr. 16.3.1.

96 Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 7. Los ejemplos que proporciona Francia de hechos que podrían "considerarse usos de la fuerza" son "la incursión en sistemas militares a fin de afectar las capacidades de defensa de Francia o de financiar o incluso capacitar a individuos para que dirijan ciberataques contra Francia".

97 Ministerio de Asuntos Exteriores de los Países Bajos, "Letter to the Parliament on the international legal order in cyberspace", 5 de julio de 2019, p. 4, disponible en www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legalorder-in-cyberspace; Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 7. Para un panorama general de las posiciones de los Estados en los últimos años, v. Przemysław Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, informe de políticas, Programa de La Haya para las normas cibernéticas, 2020. Para un ejemplo de esos debates, v., p. ej., Kenneth Kraszewski, "Scenario 14: Ransomware campaign", en K. Mačák, T. Minárik y T. Jančárková (eds.), nota 68 *supra*, párrs. L5-L13.

98 CIJ, *Actividades militares en y en contra de Nicaragua* (*Nicaragua v. Estados Unidos de América*), fallo, 27 de junio de 1986, párrs. 191, 195.

es posible concluir que el uso de la fuerza debe alcanzar un nivel de intensidad para ser considerado un "ataque armado"[99]. En este sentido, los expertos sostienen que "algunas ciberoperaciones pueden ser lo bastante graves para que se justifique clasificarlas de 'ataque armado' según entiende el término la Carta de la ONU"[100], en particular, aquellas cuyos efectos son comparables a los de los ataques armados más convencionales. Esta opinión se refleja asimismo en las posiciones públicas de algunos Estados[101].

Los interrogantes sobre cómo interpretar para el ciberespacio los umbrales de un recurso a la fuerza armada al que se aplica el DIH, la prohibición del uso de la fuerza impuesta por la Carta de la ONU y la noción de "ataques armados" que, por su naturaleza, dan derecho a la defensa propia están cambiando. Si bien es posible identificar algunos indicadores con base en la jurisprudencia de la CIJ, la jurisprudencia de los tribunales y las cortes penales internacionales, la práctica de los Estados y las opiniones de los expertos, por el momento, quedan muchos interrogantes sin resolver.

No obstante, es importante destacar que esas tres nociones y conceptos provienen de distintos cuerpos del derecho internacional y tienen distintos significados. Como se ha mencionado, a juicio del CICR, una operación cibernética equiparable al recurso de la fuerza armada entre Estados conforme al DIH se rige por ese cuerpo del derecho incluso en ausencia de un conflicto armado preexistente. En la práctica, una operación de ese tipo también puede constituir un uso de la fuerza prohibido por la Carta de la ONU. Sin embargo, las dos conclusiones requieren análisis jurídicos independientes: llegar a la conclusión de que se ha alcanzado el umbral conforme a un cuerpo del derecho no necesariamente impide llegar a una conclusión diferente según otro cuerpo del derecho. Esto tiene especial importancia al diferenciar la aplicabilidad del DIH del derecho a la defensa propia de conformidad con la Carta de la ONU. En vista de la posición de que solo las formas más graves del uso de la fuerza –es decir, las que alcanzan determinada magnitud y producen determinados efectos– pueden ser clasificadas como ataques armados, queda claro que no todo recurso a la fuerza armada a la que se aplica el DIH puede considerarse un ataque armado de conformidad con la Carta de la ONU, lo que habilita el ejercicio del derecho a la defensa propia[102]. Esas diferencias tienen importantes consecuencias jurídicas y prácticas. Por eso, cualquier análisis de una situación en la que un Estado dirige ciberoperaciones contra otro Estado ha de distinguir las distintas nociones y no combinarlas en un único "umbral" inespecífico.

99 No obstante, no todos los Estados comparten esta opinión. Estados Unidos, p. ej., considera que cualquier uso de la fuerza constituye un ataque armado.

100 Manual de Tallin 2.0, nota 13 *supra*, párr. 4 del comentario de la norma 71.

101 Ministerio de Asuntos Exteriores de los Países Bajos, nota 97 *supra*, p. 4; Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 7.

102 H. Durham, nota 25 *supra*.

## La cuestión de la atribución

En la guerra en general, y en el ciberespacio en particular, en ocasiones los Estados recurren a actores no estatales, como grupos armados no estatales o empresas militares y de seguridad privadas, para realizar ciertas acciones, incluidas las ciberoperaciones. Las características específicas del ciberespacio, entre ellas, la variedad de posibilidades para que los actores se oculten o falseen su identidad, dificultan la atribución de la conducta a individuos específicos y a partes en conflictos armados[103]. Surgen, entonces, importantes dificultades a la hora de determinar la aplicabilidad del DIH en una situación particular. Si no es posible identificar al autor de una operación dada –y, por lo tanto, no puede establecerse el nexo entre la operación y un conflicto armado–, es sumamente difícil determinar incluso si el DIH es aplicable a la operación[104]. En primer lugar, como se ha comentado, los distintos umbrales de violencia son relevantes para clasificar como conflicto armado un ciberataque por parte de un Estado o de un actor no estatal. Por ello, si se desconoce el origen estatal o no estatal de una operación cibernética independiente de un conflicto armado existente, no está claro qué umbral corresponde considerar. En segundo lugar, incluso cuando hay un conflicto armado en curso, los ataques cibernéticos que no tienen un nexo con el conflicto (por ejemplo, los actos criminales no relacionados con el conflicto) no se rigen por el DIH, y la imposibilidad de identificar al autor de una operación cibernética podría dificultar la determinación de si existe un nexo con el conflicto. Esos ejemplos revelan que establecer quién es el autor de una operación cibernética y si la operación puede atribuirse a un Estado o a una parte no estatal en conflicto tienen importantes implicaciones jurídicas.

La atribución de ciberoperaciones también es importante para garantizar que los actores que violan el derecho internacional, incluido el DIH, rindan cuentas. La percepción de que será más fácil negar la responsabilidad de un ataque ilícito también puede contribuir a derribar el tabú contra ese tipo de operaciones y hacer que los actores se tornen más inescrupulosos a la hora de conducir operaciones violatorias del derecho internacional[105].

Dicho esto, la atribución no es un problema desde la perspectiva de los actores que conducen, dirigen o controlan las ciberoperaciones: todos tienen la información disponible para determinar dentro de qué marco jurídico internacional operan y qué obligaciones deben respetar[106].

103 Para un análisis de las dificultades técnicas de atribuir los ataques cibernéticos a actores específicos, v. Vitaly Kamluk, "Know your enemy and know yourself: Attribution in the cyber domain", *Humanitarian Law and Policy Blog*, 3 de junio de 2019, disponible en https://blogs.icrc.org/law-and-policy/2019/06/03/know-your-enemy-know-yourself-cyber-domain-attribution/.

104 Informe del CICR de 2011 sobre los desafíos de los conflictos armados contemporáneos, nota 43 *supra*, p. 42.

105 CICR, nota 1 *supra*, p. 10.

106 Ibíd.

Según el derecho internacional, un Estado es responsable de los comportamientos atribuibles a él, incluidas las posibles violaciones del DIH. Por ejemplo:

(a) violaciones cometidas por órganos estatales, incluidas sus fuerzas armadas;
(b) violaciones cometidas por personas físicas o jurídicas, incluidas entidades facultadas por el Estado para ejercer elementos de la autoridad gubernamental;
(c) violaciones cometidas por personas o grupos que procedan según instrucciones del Estado o bien bajo su dirección o control; y
(d) violaciones cometidas por personas o grupos privados que el Estado reconoce y acepta como propias[107].

Estos principios se aplican independientemente de si el comportamiento se ejerce por medios cibernéticos o de otra índole[108].

## Los límites que impone el DIH al uso de las capacidades cibernéticas durante los conflictos armados

Reconocer que el DIH se aplica a las ciberoperaciones que tienen un nexo con un conflicto armado es solo el primer paso. Las características específicas de esta nueva tecnología plantean numerosas dificultades a la interpretación de las normas del DIH, incluso las relativas a la conducción de las hostilidades.

La naturaleza parcialmente no física (es decir, digital) del ciberespacio y la interconexión de las redes militares y civiles suponen dificultades prácticas y jurídicas para la aplicación de las normas del DIH que confieren protección a los civiles y a los bienes de carácter civil contra las ciberoperaciones, en especial, las que se consideran ataques en el sentido del DIH. Se ha propuesto, incluso, que, en ocasiones, podría ser imposible aplicar los principios básicos del DIH al ciberespacio. Como se observará más adelante, esta dificultad podría ser exagerada. No obstante, surgen cuestiones fundamentales respecto de la protección de la infraestructura cibernética civil clave contra los ataques militares. Como muchas de las normas del DIH que rigen la conducción de las hostilidades solo se aplican a las operaciones militares que constituyen "ataques" según la definición del DIH, en este apartado, se analizan distintas cuestiones relativas a las ciberoperaciones que son consideradas ataques, incluida la cuestión primordial de *qué* operaciones

107 V. Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 149. V. también Comisión de Derecho Internacional, *Responsabilidad del Estado por hechos internacionalmente ilícitos*, 2001, en especial, arts. 4-11.

108 CICR, nota 1 *supra*, p. 11; Manual de Tallin 2.0, nota 13 *supra*, normas 15-17. Para una opinión diferente, v. la propuesta de China sobre el anteproyecto inicial del informe del GTCA, que prevé que respecto de la "responsabilidad del Estado, para la que, a diferencia del derecho de los conflictos armados o los derechos humanos, aún no se ha alcanzado consenso internacional, no hay una base jurídica para el debate sobre su aplicación en el ciberespacio". Comentarios de China sobre el anteproyecto inicial del informe del GTCA, disponible en www.un.org/disarmament/open-ended-working-group/.

constituyen ataques de conformidad con el DIH. En segundo lugar, se examinan las obligaciones de las partes en un conflicto armado en las operaciones militares que no constituyen "ataques". En tercer lugar, en este apartado, se analizan algunas dificultades relativas al examen jurídico de las capacidades cibernéticas.

## Ciberoperaciones que constituyen ataques según el DIH

El DIH establece normas fundamentales que restringen las ciberoperaciones que constituyen "ataques" según la definición del DIH. En este apartado, se examinan las normas y principios pertinentes que han sido materia de muy intensos debates. Se analiza, primero, si desde el punto de vista tecnológico, los ataques cibernéticos pueden dirigirse a objetivos militares específicos tal como requiere el principio de distinción. En la segunda parte, se analiza cómo debería interpretarse la noción de ataque en el ciberespacio según el DIH. En la tercera parte, se analiza el debate de una cuestión íntimamente relacionada: si los datos civiles deben gozar de la misma protección que los "objetos" civiles a los efectos del DIH. En la última parte, se trata el debate actual sobre cómo se aplican las normas del DIH relativas a la conducción de las hostilidades a los objetos que se utilizan simultáneamente para fines civiles y militares (denominados habitualmente "objetos de uso dual"), que son los que predominan en el ciberespacio.

### *Desde el punto de vista técnico, los ataques cibernéticos pueden dirigirse a objetivos militares específicos*

La implementación de los principios de distinción y proporcionalidad, y la prohibición de lanzar ataques indiscriminados requieren que un ataque pueda dirigirse y que, en efecto, se dirija a un objetivo militar y que no cause daños incidentales excesivos a las personas civiles o a los bienes de carácter civil. Contrariamente al supuesto de que esos principios podrían tornarse irrelevantes en el ciberespacio debido a la interconectividad que lo caracteriza, un análisis minucioso de las ciberoperaciones indica que dichas operaciones no son intrínsecamente indiscriminadas. Por ejemplo, si una ciberoperación está ejecutada por operadores que acceden a su objetivo y dirigen una operación contra él, los operadores sabrán dónde se encuentran y qué hacen. Del mismo modo, el análisis de las herramientas informáticas muestra que estas no son necesariamente indiscriminadas. Sin embargo, para programar un software malicioso que discrimine entre objetos civiles y militares, y conducir ciberoperaciones sin causar daños incidentales excesivos, se requieren capacidades y pruebas complejas.

Quienes desarrollan software malicioso o planifican ataques cibernéticos pueden diseñar sus herramientas sin funciones de autopropagación. En ese caso, el software en cuestión no puede propagarse sin intervención humana adicional. Incluso aunque el software se autopropague, los ataques ocurridos a lo largo de los años han demostrado que es posible desarrollar software malicioso para atacar solamente a hardware o software específicos. Esto quiere decir que, incluso si el

software malicioso está programado para propagarse ampliamente, puede diseñarse para que cause daño solo a un objetivo específico o a un grupo de objetivos específicos. En concreto, los ataques cibernéticos que se lanzan para causar daño físico a sistemas de control industrial pueden requerir herramientas informáticas diseñadas para ese objetivo y propósito específicos. En muchos casos, la necesidad de esas herramientas personalizadas efectivamente afectaría –desde el punto de vista técnico– la capacidad de conducir un ataque cibernético a gran escala o de forma indiscriminada. El hecho de que los ataques cibernéticos puedan dirigirse con precisión en los aspectos técnicos, eso no significa que sean necesariamente lícitos si se ejecutan durante un conflicto. Sin embargo, las características observadas en numerosas ciberoperaciones indican que pueden personalizarse con gran precisión para causar efectos solo en objetivos específicos y que esas operaciones son, por lo tanto, capaces de cumplir los principios y las normas del DIH.

El hecho de que algunas de las herramientas cibernéticas conocidas hayan sido diseñadas para autopropagarse y causar daño a sistemas informáticos de uso civil generalizado no justifica el argumento de que la naturaleza interconectada del ciberespacio dificulta, si no imposibilita, la implementación de las normas básicas del DIH. Por el contrario, durante los conflictos armados, el uso de herramientas cibernéticas estaría prohibido por el DIH[109]. El DIH prohíbe los ataques que emplean medios y métodos de guerra, incluidos los medios y métodos cibernéticos, que no puedan dirigirse a objetivos militares específicos o de los que quepa esperar que escaparán al control del usuario[110] o que –cuando se dirijan a un objetivo militar– causarán daños civiles incidentales excesivos en relación con la ventaja militar concreta y directa prevista[111].

### *La noción de "ataque" en el DIH y su aplicación a las ciberoperaciones*

La cuestión de si una operación es un "ataque" según la definición del DIH es fundamental para la aplicación de numerosas normas que tienen origen en los principios de distinción, proporcionalidad y precaución, que confieren una importante protección a los civiles y a los bienes de carácter civil. En concreto, normas como la prohibición de los *ataques* contra los civiles y los bienes de carácter

109 Del mismo modo, el Manual de derecho de la guerra del DoD, nota 87 *supra*, párr. 16.6, concluye: "Por ejemplo, un virus informático destructivo programado para propagarse y destruir sin control sistemas de internet para uso civil estaría prohibido por ser un arma de efectos intrínsecamente indiscriminados".

110 Yves Sandoz, Christophe Swinarski y Bruno Zimmerman (eds.), *Comentario del Protocolo del 8 de junio de 1977 adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I)* (Comentario del CICR del PA I), Bogotá, CICR y Plaza y Janés Editores Colombia, 1998, párr. 1963.

111 Protocolo adicional (I) a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales, 1125 UNTS 3, 8 de junio de 1977 (en vigor desde el 7 de diciembre de 1978) (PA I), art. 51(4)-(5); Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, normas 11, 14.

civil[112], la prohibición de los *ataques*[113] indiscriminados[114] y desproporcionados, y la obligación de tomar todas precauciones factibles para evitar o, al menos, reducir los daños incidentales a los civiles y los daños a los bienes de carácter civil cuando se ejecuta un *ataque*[115] se aplican a las operaciones que son consideradas "ataques" según la definición del DIH. La cuestión de cuán amplia o estricta es la interpretación de la noción de "ataque" en relación con las ciberoperaciones es, por lo tanto, esencial para la aplicabilidad de normas fundamentales –así como para la protección que confieren a los civiles y a la infraestructura civil– a las ciberoperaciones.

El artículo 49 del PA I entiende por ataques "los actos de violencia contra el adversario, sean ofensivos o defensivos". Es sabido que la noción de violencia en esa definición puede hacer referencia a los medios de la guerra o a sus efectos, es decir que una operación que tiene efectos violentos puede ser un ataque incluso si los medios utilizados para causar esos efectos no son, en sí, violentos[116]. Sobre la base de esta interpretación, el Manual de Tallin 2.0 propone la siguiente definición de ataque cibernético: "Un ataque cibernético es una operación cibernética, sea de índole ofensiva o defensiva, de la que es razonable esperar que causará lesiones o la muerte a personas o el daño o la destrucción a objetos"[117].

Los Estados que han adoptado una posición respecto de esta cuestión, el CICR y los expertos aceptan, en general, que las ciberoperaciones que se podría prever que causen muertes, heridas o daños físicos constituyen ataques según el DIH[118]. Algunos Estados incluyen expresamente los daños asociados con los

112 V. PA I, art. 52; Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, normas 7-10.

113 V. PA I, art. 51(5)(b); Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 14.

114 V. PA I, art. 54(c); Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 11.

115 V. PA I, art. 57(1); Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 15.

116 V. C. Droege, nota 83 *supra*, p. 557; William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012, p. 384. Como señala Droege, "no hay controversia respecto de que el uso de agentes biológicos, químicos o radiológicos constituye un ataque, aunque con dicho ataque no se aplique la fuerza física".

117 Manual de Tallin 2.0, nota 13 *supra*, norma 92.

118 V. CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, Ginebra, 2015 (Informe del CICR de 2015 sobre los desafíos de los conflictos armados contemporáneos), pp. 54-55, disponible en https://www.icrc.org/es/document/el-derecho-internacional-humanitario-y-los-desafios-de-los-conflictos-armados; Manual de Tallin 2.0, nota 13 *supra*, norma 92. Para Estados que han adoptado una posición sobre cómo se aplica la noción de ataque en el sentido del DIH a las ciberoperaciones, v., en especial, Departamento de Asuntos Exteriores y Comercio de Australia, nota 94 *supra*, anexo A; Ministerio de Defensa de Dinamarca, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, (Manual Militar de Dinamarca), 2016, pp. 290-291, disponible en https://www.forsvaret.dk/globalassets/fko---forsvaret/dokumenter/publikationer/-military-manual-updated-2020-2.pdf; Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 13; Noruega, *Manual i krigens folkerett* (Manual Militar de Noruega), 2013, párr. 9.54, disponible en https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/194213/manual_krigens_folkerett.pdf?sequence=1&isAllowed=y; Manual Militar de Nueva Zelanda, nota 85 *supra*, párr. 8.10.17; Manual de derecho de la guerra del DoD, nota 87 *supra*, párr. 16.5.1.

efectos indirectos (o secundarios) previsibles de los ataques[119], opinión que también sostiene el CICR[120]. Ese sería el caso, por ejemplo, de los pacientes que se encuentran en la unidad de cuidados intensivos de un hospital y que fallecen como consecuencia de una ciberoperación dirigida contra la red de electricidad que deja al hospital sin suministro de energía.

Más allá de ese consenso básico, existen opiniones diversas sobre si una ciberoperación que altera un objeto sin ocasionar daños físicos constituye un ataque en el sentido del DIH[121]. Se ha debatido extensamente sobre esta cuestión en el proceso de redacción del Manual de Tallin. La mayoría de los expertos sostuvo que una ciberoperación puede equipararse a un ataque si se prevé que interferirá en la funcionalidad y si para restablecer esa funcionalidad es necesario reemplazar componentes físicos. Según algunos expertos, una ciberoperación también será considerada un ataque cuando para restablecer la funcionalidad sea necesario reinstalar el sistema operativo o datos particulares.

El CICR ha adoptado la posición de que una operación dirigida a malograr una computadora o una red informática durante un conflicto armado constituye un ataque según la definición del DIH, tanto si el objeto queda inhabilitado porque se lo ha destruido o por otra causa como si no[122].

La posición del CICR se fundamenta en dos razones principales. La primera proviene de una interpretación de la noción de ataque en su contexto[123]. Puesto que la definición de objetivo militar que figura en el artículo 52(2) del PA I hace referencia no solo a la destrucción o a la captura sino también a la "neutralización" como posible resultado de un ataque, debe interpretarse que, en virtud del artículo 49 del PA I, la noción de "ataque" abarca operaciones destinadas a afectar el funcionamiento de los objetos (esto es, a neutralizarlos) sin causar daño físico ni destrucción. De hecho, se ha observado que, si fuera de otro modo, la mención explícita de la neutralización en el artículo 52(2) sería superflua[124]. En segundo lugar, una interpretación excesivamente estricta de la noción de ataque sería difícil de conciliar con el objeto y fin de las normas relativas a la conducción de las hostilidades, que han de garantizar la protección de la población civil y de los bienes de carácter civil contra los efectos de las hostilidades. De hecho, con una interpretación excesivamente estricta, se consideraría que una ciberoperación destinada a alterar el funcionamiento de una red de uso civil (electricidad, sistema

119 Manual Militar de Dinamarca, nota 118 *supra*, p. 677 (análisis de los ataques a las redes informáticas); Manual Militar de Nueva Zelanda, nota 85 *supra*, párr. 8.10.22; Manual Militar de Noruega, nota 118 *supra*, párr. 9.54.

120 CICR, nota 1 *supra*, p. 9.

121 V., p. ej., Manual de Tallin 2.0, nota 13 *supra*, comentario de la norma 92, párrs. 10-12.

122 V. Informe del CICR de 2015 sobre los desafíos de los conflictos armados contemporáneos, nota 118 *supra*, pp. 54-55. V. también Manual de Tallin 2.0, nota 13 *supra*, párr. 12 del comentario de la norma 92.

123 Convención de Viena sobre el derecho de los tratados, art. 31(1).

124 Knut Dörmann, "Applicability of the Additional Protocols to computer network attacks", 2004, p. 4, disponible en www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf; C. Droege, nota 83 *supra*, p. 559. Para una opinión diferente, v. Michael N. Schmitt, "Cyber operations and the *jus in bello*: Key issues", *International Law Studies*, vol. 87, 2011, pp. 95-96; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 198.

bancario y comunicaciones, entre otras redes) o que pudiera causar esa alteración de manera incidental podría no estar cubierta por normas fundamentales del DIH que confieren protección a la población civil y a los bienes de carácter civil[125].

De manera análoga, los expertos proponen que es importante "interpretar la disposición [artículo 49 del PA I] tomando en consideración los desarrollos tecnológicos recientes y expandir el concepto de 'violencia' de modo de incluir no solo los daños materiales a los objetos, sino también la alteración de infraestructuras sin destruirlas"[126].

Como las ciberoperaciones pueden afectar considerablemente los servicios esenciales sin necesariamente causar daños físicos, esto es uno de los temas de debate más críticos para la protección de los civiles contra los efectos de las ciberoperaciones. Por lo tanto, es fundamental que los Estados expresen su opinión sobre el tema y se esfuercen por alcanzar una interpretación común. Por el momento, las opiniones varían entre los Estados que han expresado públicamente su posición.

Las definiciones de la noción de "ataque" adoptadas en los manuales militares de Noruega y Nueva Zelanda reflejan la del Manual de Tallin 2.0. Sin embargo, no queda claro si en esos manuales la intención era expresar una posición en el debate, porque en el comentario de la norma 92 del Manual de Tallin 2.0 se mencionan distintas opiniones de cómo debe entenderse el "daño" en el contexto cibernético. Australia ha declarado que las ciberoperaciones se consideran ataques si se elevan "hasta el mismo nivel de un 'ataque' cinético 'según el DIH'"[127], pero no queda claro si con esa frase se pretendía fijar una posición en el debate.

Algunos Estados toman en cuenta el daño físico para clasificar como ataque a una ciberoperación. Según un estudio de la OEA, Perú opina que, para considerar ataque a una operación, las personas o los objetos deben haber sufrido "daños físicos"[128]. El Manual Militar de Dinamarca especifica para el término "ataque" que "[e]n lo que atañe al daño a los objetos, el término abarca cualquier daño físico. No obstante, el término no incluye la interrupción temporaria y otras neutralizaciones que no impliquen daño físico (por ejemplo, el 'congelamiento' digital de un sistema de control de comunicaciones)"[129]. En la propuesta de 2014 presentada ante el GEG de la ONU, Estados Unidos observa:

125 En este mismo sentido, v. también M. N. Schmitt, nota 67 *supra*, p. 8.

126 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, p. 181. V. también Dieter Fleck, "Searching for international rules applicable to cyber warfare – A critical first assessment of the new Tallinn Manual", *Journal of Conflict and Security Law*, vol. 18, n.º 2, 2013, p. 341: "Desde luego, no sería del todo convincente insistir en que el término 'ataques' debería limitarse a actos que causen daños directos o destrucción física si ese mismo acto puede, por ejemplo, llevar a la interrupción [sic] de suministros esenciales para los hospitales u otra infraestructura civil importante".

127 Departamento de Asuntos Exteriores y Comercio de Australia, nota 94 *supra*, anexo A.

128 OEA, nota 22 *supra*, párr. 43.

129 Manual Militar de Dinamarca, nota 118 *supra*, p. 290. En el Manual, se especifica respecto de los ataques y operaciones dirigidos a redes informáticas que "[e]sto significa, por ejemplo, que las operaciones dirigidas a redes deben considerarse ataques en virtud del DIH si su consecuencia es que causan daños físicos". Ibíd., p. 291.

> Si se ha de determinar si una actividad cibernética constituye un "ataque" a los fines del *jus in bello*, los Estados deberán considerar, entre otras cuestiones, si esa actividad tiene en las personas civiles, los bienes de carácter civil o la infraestructura cibernética civil efectos tanto cinéticos e irreversibles como no cinéticos reversibles[130].

En el mismo sentido, el Manual de la Guerra del Departamento de Defensa (DoD) da el ejemplo de un "ataque cibernético que destruiría los sistemas informáticos del enemigo" y observa que entre los "[f]actores que indicarían que una ciberoperación no es un 'ataque' se encuentra la consideración de si la operación causa solo efectos reversibles o solo efectos temporarios"[131]. Lamentablemente, esos documentos no aclaran qué se entiende por efectos "reversibles" o "temporarios" ni qué diferencia hay entre las dos nociones, si es que la hay[132]. Tampoco se analiza en ellos si un efecto puede dejar de considerarse temporario –y, de ser así, después de cuánto tiempo– ni cómo clasificar las operaciones reiteradas, cada una de las cuales causa un efecto temporario aunque deliberadamente acumulativo. Tampoco se analiza en ellos si "reversible" hace referencia solo a operaciones en las que el autor puede revertir los efectos del ataque[133] o también a operaciones donde el objetivo debe actuar para restablecer la funcionalidad del sistema que ha sido objeto del ataque o para hacer cesar o revertir los efectos del ataque. Al respecto, cabe recordar que la posibilidad de reparar el daño físico causado por una operación militar (sea cibernética o cinética), por lo general, no se considera condición para descartar que la operación sea un ataque en el sentido del DIH[134]. Es así incluso si con la reparación se revierte el efecto directo de esa operación y se restablece la funcionalidad del objeto en cuestión[135].

Francia ha expresado una interpretación más clara y amplia de la noción de ataque cibernético:

> Una ciberoperación es un ataque en el que los equipos o sistemas a los que se dirige ya no pueden ofrecer el servicio para el que fueron implementados, sea de manera temporaria o permanente, reversible o no. Si los efectos son temporarios

130 United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2014-15, p. 5.

131 V. también Manual de derecho de la guerra del DoD, nota 87 *supra*, párrs. 16.5.1, 16.5.2.

132 Gary Brown y Kurt Sanger, "Cyberspace and the law of war", *The Cyber Defense Review*, 6 de noviembre de 2015, disponible en https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136032/cyberspace-and-the-law-of-war/.

133 P. ej., un ataque distribuido de denegación de servicio en el que la red o el sistema al que se dirige volvieran a funcionar normalmente al finalizar el ataque sin que se produjera ningún otro efecto indirecto durante el tiempo en que la red o el sistema se vieran afectados.

134 Laurent Gisel, "The use of cyber technology in warfare: Which protection does IHL afford and is it sufficient?", en G. Venturini y G. L. Beruto (eds.), nota 7 *supra*.

135 P. ej., Michael Lewis analiza la práctica de bombardear puentes sobre el eje longitudinal, que se llevó a cabo durante la Guerra del Golfo de 1991, y, entre otras cuestiones, comenta que "el daño a los puentes estaría más cerca del punto medio y, por lo tanto, estos serían más fáciles de reparar", sin afirmar que esta condición impediría que la operación fuera considerada un ataque. V. Michael Lewis, "The law of aerial bombardment in the 1991 Gulf War", *American Journal of International Law*, vol. 97, n.º 3, 2003, p. 501.

> y/o reversibles, la caracterización del ataque depende de la acción que el adversario deba realizar para restablecer la infraestructura o el sistema (reparación de los equipos, sustitución de un componente, reinstalación de una red, etc.)[136].

En su análisis de esta posición, Schmitt observa que "[e]sta opinión es muy defendible desde el punto de vista del derecho, pues el significado mismo de daño razonablemente abarca sistemas que no funcionan como se espera que lo hagan y que requieren alguna forma de reparación para recuperar la funcionalidad"[137]. De manera análoga, según el estudio de la OEA antes mencionado, Chile propone que para que una operación sea considerada un ataque, su resultado debe requerir que el Estado afectado "deb[a] realizar acciones para reparar o recuperar la infraestructura o sistema informático afectado, debido a que en aquellos casos las consecuencias del ataque son similares a las descritas anteriormente, en particular daños físicos a la propiedad"[138]. El estudio también indica que Guatemala expresa la opinión de que, entre las ciberoperaciones que pueden considerarse ataques, se encuentran las que "solo producen una pérdida de la funcionalidad", opinión compartida por Ecuador[139]. Bolivia, Ecuador y Guyana añaden que las ciberoperaciones pueden constituir ataques en el sentido del DIH, en especial, cuando inhabilitan infraestructura crítica o interrumpen el suministro de servicios básicos a la población[140].

De todos modos, no todas las ciberoperaciones durante un conflicto armado constituirían "ataques" tal como los define el DIH. En primer lugar, para el DIH la noción de ataque no abarca el espionaje. En segundo lugar, las normas relativas a la conducción de las hostilidades no prohíben todas las operaciones que interfieren con los sistemas de comunicaciones civiles: tradicionalmente, la interferencia de las comunicaciones de radio o televisión no se ha considerado un ataque en el sentido del DIH. Sin embargo, la distinción entre ataque e interferencia de las comunicaciones que no se considera ataque es, probablemente, menos clara en las ciberoperaciones que en las operaciones cinéticas o electromagnéticas más tradicionales[141]. Por último, la noción de "operaciones militares" según el DIH, incluidas las ejecutadas con medios cibernéticos, es más amplia que la de "ataques", como se analizará más adelante.

136 Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 13.

137 M. N. Schmitt, nota 52 *supra*. En el mismo sentido, v. W. H. Boothby, nota 116 *supra*, p. 386

138 OEA, nota 22 *supra*, párr. 43.

139 Ecuador especifica que "[u]na operación cibernética puede considerarse un ataque en caso de dejar sin funcionalidad la infraestructura crítica del Estado u otros que pongan en peligro la seguridad del Estado". Ibíd., párr. 44.

140 Bolivia propone que una ciberoperación "podría ser considerada como un ataque cuando tiene el objetivo de inhabilitar los servicios básicos (agua, luz, telecomunicaciones o el sistema financiero); Guyana propone que "las operaciones cibernéticas que socavan el funcionamiento de los sistemas y la infraestructura informáticos necesarios para el suministro de servicios y recursos a la población civil constituyen un ataque", entre los que incluye "plantas nucleares, hospitales, bancos y sistemas de control del tráfico aéreo". Ibíd., párrs. 44-45.

141 Informe del CICR de 2015 sobre los desafíos de los conflictos armados contemporáneos, nota 118 *supra*, pp. 54-55; C. Droege, nota 83 *supra*, p. 560.

### *La protección de datos como "bienes de carácter civil"*

Además de la pregunta fundamental de qué ciberoperaciones son consideradas "ataques" en el sentido del DIH, la cuestión de si los datos civiles gozan de la misma protección que los bienes de carácter civil ha sido objeto de importantes debates que aún no han concluido. La protección de los bienes de carácter civil contra las ciberoperaciones maliciosas durante los conflictos armados es cada vez más importante debido a que los datos son un componente esencial del dominio digital y un pilar en la vida de muchas sociedades: la información médica personal, la información de la seguridad social, los registros impositivos, las cuentas bancarias, los archivos empresariales de clientes y los padrones electorales son fundamentales para el funcionamiento de muchos aspectos de la vida civil. Como se prevé que, en los próximos años, esta tendencia continuará, o incluso se acelerará, la preocupación sobre la salvaguarda de los datos civiles esenciales va también en aumento.

Respecto de los datos que pertenecen a determinadas categorías de bienes que gozan de protección específica en virtud del DIH, las normas que confieren tal protección son integrales. Como se observa más adelante, debe interpretarse que las obligaciones de respetar y proteger los establecimientos sanitarios y las operaciones de socorro humanitario comprenden los datos médicos pertenecientes a esos establecimientos y los datos de las organizaciones humanitarias que son esenciales para sus actividades[142]. Asimismo, está prohibida la eliminación o la alteración de datos que inutilizan los bienes indispensables para la supervivencia de la población civil, como las instalaciones de agua potable o los sistemas de irrigación[143].

Aun así, es importante aclarar en qué medida los datos civiles quedan protegidos por las normas generales en vigor sobre la conducción de las hostilidades. En concreto, esta cuestión ha suscitado el debate sobre si los datos constituyen bienes de conformidad con el DIH, en cuyo caso las ciberoperaciones contra los datos (por ejemplo, las destinadas a eliminarlos) estarían regidas por los principios de distinción, proporcionalidad y precaución, y habilitarían la protección que dichos principios confieren a los bienes de carácter civil[144].

La cuestión de si los datos constituyen un bien de conformidad con el DIH está íntimamente relacionada con los debates acerca de la noción de "ataque" presentados con anterioridad. En primer lugar, si se eliminan o manipulan los datos con el propósito de causar, directa o indirectamente, lesiones o la muerte a una persona, o daños a un bien físico (incluso, a nuestro juicio, inutilizándolo), la

142 V., más adelante, el análisis del apartado titulado "Normas del DIH que confieren protección a los bienes indispensables para la supervivencia de la población civil, los servicios sanitarios y las operaciones de socorro humanitario".

143 PA I, art. 54; Protocolo adicional (II) a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional, 1125 UNTS 609, 8 de junio de 1977 (en vigor desde el 7 de diciembre de 1978) (PA II), art. 14; Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 54.

144 V. Manual de Tallin 2.0, nota 13 *supra*, párrs. 6-7 del comentario de la norma 100. Para un debate académico, v. *Israel Law Review*, vol. 48, n.º 1, pp. 39-132; M. N. Schmitt, nota 67 *supra*.

operación constituye un ataque, independientemente de si los datos en sí mismos constituyen bienes a los fines del DIH. Esto es así porque las consecuencias de una operación dirigida contra los datos pueden hacer que la operación sea considerada un ataque en el sentido del DIH y, por ende, esté sujeta a las normas del DIH pertinente. Para esos ataques, no es importante si los datos son considerados un bien en virtud del DIH o no.

No obstante, la cuestión de si los datos son bienes según el DIH es crítica para operaciones que no están destinadas a tener esas consecuencias o de las que no se prevé que tengan. A grandes rasgos, se pueden tener en cuenta dos enfoques generales. De acuerdo con el primero, que considera que los datos son bienes en virtud del DIH, una operación ideada para eliminar o manipular datos o de la que se prevé que los elimine o manipule sería un ataque para el que rigen todas las normas pertinentes del DIH, porque equivaldría a destruir o dañar un bien (los datos). Lo mismo valdría si no se previera que esa eliminación o manipulación causara la muerte o lesiones a una persona ni que dañara o inutilizara un objeto físico. Aun con esta interpretación, sin embargo, una operación ideada exclusivamente para acceder a los datos (posiblemente confidenciales) sin eliminarlos ni manipularlos –por ejemplo, con fines de espionaje– no constituiría un ataque.

Por el contrario, si los datos no se consideran bienes en el sentido del DIH, una operación ideada para eliminarlos o manipularlos sin causar la muerte o lesiones a una persona ni daño a un bien, no se regiría por las normas aplicables a los ataques ni por algunas de las normas más generales que confieren protección a los bienes de carácter civil (por ejemplo, la obligación de realizar las operaciones con el cuidado constante de preservar a los civiles y los bienes de carácter civil, como se analizará más adelante en el apartado "Normas que rigen las operaciones militares que no constituyen ataques"). Sin embargo, las operaciones podrían regirse por otros regímenes de protección de conformidad con el DIH, cuestión que se analizará más adelante en el apartado "Normas del DIH que confieren protección a los bienes indispensables para la supervivencia de la población civil, los servicios sanitarios y las operaciones de socorro humanitario". Aun así, habría un vacío en materia de protección de los datos civiles esenciales que no se benefician de ningún régimen de protección específica, lo que da lugar a interrogantes.

Los expertos tienen opiniones diferentes sobre si los datos pueden ser considerados objetos a los fines de las normas del DIH sobre la conducción de las hostilidades[145]. Una de esas opiniones, la que sostienen la mayoría de los expertos que participaron en el proceso de redacción del Manual de Tallin, es que no cabe interpretar que el significado corriente del término "bien", tal como se analiza en el Comentario del CICR del PA I, de 1998, incluye los datos, porque los bienes son

145 Para un ejemplo de este debate, v. "Scenario 12: Cyber operations against computer data", en K. Mačák, T. Minárik y T. Jančárková (eds.), nota 68 *supra*.

objetos materiales, visibles y tangibles[146]. Sin embargo, la explicación que se ofrece en el Comentario del CICR tiene por finalidad distinguir objeto de conceptos como "propósito" o "fin" y no diferenciar entre objetos o bienes tangibles e intangibles y, por lo tanto, no puede ser determinante en el debate sobre los datos[147]. Por el contrario, otros han propuesto que todos o algunos tipos de datos serían considerados bienes según el DIH. Una opinión es que el "significado moderno" de la noción de bienes en la sociedad actual, y una interpretación del término a la luz de su objeto y fin, debe llevar a concluir que "los datos son 'bienes' para los fines de las normas del DIH sobre la determinación de objetivos"[148]. Esta opinión se apoya en la interpretación convencional de la noción de "bien" conforme al DIH, que es más amplia que el significado corriente del término y abarca también lugares y animales. Otra propuesta consiste en diferenciar entre "datos operativos", o "código", y "datos de contenido"[149]. En este modelo, se ha propuesto que, en especial, los datos de nivel operativo pueden considerarse un objetivo militar, lo que significa que ese tipo de datos podría, asimismo, considerarse un bien de carácter civil[150]. Si bien considerar los datos operativos como bienes estaría en consonancia con la opinión analizada con anterioridad en el sentido de que inutilizar un bien equivale a un ataque, esa interpretación no parece proporcionar protección adicional. En este debate, se ha argumentado que ninguna de las conclusiones propuestas es totalmente satisfactoria, pues todas ellas fallan por exceso o por defecto[151].

Por su parte, el CICR ha subrayado la necesidad de salvaguardar los datos civiles esenciales y ha hecho hincapié en que, en el ciberespacio, la eliminación o la alteración de esos datos podría paralizar rápidamente los servicios públicos y los

146 Según la definición del *Oxford Dictionary* un "bien" es "un objeto material visible y tangible". Sobre la base del significado corriente del término "bien", el Comentario del CICR del PA I, de 1998, describe un bien como "algo visible y tangible". Comentario del CICR del PA I, nota 110 *supra*, párr. 2008. V. también Manual de Tallin 2.0, nota 13 *supra*, párr. 6 del comentario de la norma 100. Es interesante observar que, actualmente, el *Oxford Dictionary* contiene una definición específica de bienes informáticos: "Un constructo de datos que proporciona una descripción de cualquier cosa administrada por una computadora (p. ej., un procesador o un código) y define su método de funcionamiento".

147 V. también Grupo de Trabajo sobre la conducción de las hostilidades en el siglo xxi de la Asociación de Derecho Internacional (ADI), "The conduct of hostilities and international humanitarian law: Challenges of 21st century warfare" (Informe ADI), *International Law Studies*, vol. 93, 2017, pp. 338-339.

148 Kubo Mačák, "Military objectives 2.0: The case for interpreting computer data as objects under international humanitarian law", *Israel Law Review*, vol. 48, n.º 1, 2015, p. 80; Robert McLaughlin, "Data as a military objective", Australian Institute of International Affairs, 20 de septiembre de 2018, disponible en www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/.

149 Según la distinción propuesta, los datos de contenido incluirían datos "tales como el texto del presente artículo, o los contenidos de las bases de datos médicos y los catálogos de bibliotecas, entre otros similares", mientras que los datos operativos definirían "esencialmente 'el alma de la máquina'", es decir, el "tipo de datos que dan funcionalidad al hardware, así como la capacidad de realizar las tareas que necesitamos". Heather Harrison Dinniss, "The nature of objects: Targeting networks and the challenge of defining cyber military objectives", *Israel Law Review*, vol. 48, n.º 1, 2015, p. 41.

150 Ibíd., p. 54.

151 Schmitt sostiene que, como una cuestión de políticas, los Estados deberían, entonces, "conferir protección especial a determinadas 'funciones o servicios civiles esenciales' mediante el compromiso de abstenerse de conducir operaciones cibernéticas contra infraestructuras civiles o datos que interfieran en ella". M. N. Schmitt, nota 67 *supra*, p. 15.

negocios privados y causar más daños a los civiles que la destrucción de objetos físicos. Así pues, según el CICR, la conclusión de que este tipo de operaciones no estaría prohibido por el DIH en el mundo de hoy, cada vez más dependiente de la esfera cibernética, parece difícil de conciliar con el objetivo y el propósito de este ordenamiento jurídico[152]. Lógicamente, el reemplazo de archivos y documentos en papel por datos digitales no debe disminuir la protección que les confiere el DIH[153]. Tal como ha enfatizado el CICR, "[e]xcluir los datos civiles esenciales de la protección otorgada a los bienes de carácter civil dejaría un vacío considerable en materia de protección"[154].

Hasta el momento, pocos Estados han expresado su opinión sobre si debería entenderse que en la noción de "bien" están comprendidos los datos a efectos de las normas que se aplican a la conducción de las hostilidades. Por ejemplo, en el Manual Militar de Dinamarca se considera que "por lo general, los datos (digitales) no constituyen un objeto"[155]. Por el contrario, en el Manual Militar de Noruega, se afirma que los datos serán considerados bienes y solo pueden atacarse directamente si cumplen las condiciones para ser calificados de objetivo legítimo[156]. Francia ha adoptado una posición intermedia al afirmar que "[d]ada la situación actual de dependencia digital, los datos de contenido (por ejemplo, datos civiles, bancarios, médicos, etc.) están protegidos en virtud del principio de distinción"[157]. La descripción de la posición de Perú en el informe de la OEA *Mejora de la transparencia* parece reflejar una posición similar: si bien Perú no adopta expresamente una posición sobre si los datos constituyen bienes, en la descripción de su posición se afirma que el país analiza las operaciones dirigidas a los datos según la noción de "objetivo militar", lo que indica que algunos sistemas de datos no pueden atacarse, porque hacerlo "no generaría una ventaja militar legítima"[158]. Como la definición de "objetivos militares" según el artículo 52(2) del PA I se aplica "en lo que respecta a los bienes", este razonamiento parece implicar que los datos constituyen bienes. Chile propone evaluar las repercusiones de un ataque dirigido a los datos y concluye que "el principio de distinción debe, por lo tanto, ser tenido en consideración en el contexto de las operaciones cibernéticas, por lo cual un Estado debería abstenerse de atacar datos en caso de que esto pudiese afectar a la población civil". Según consta, Chile ha señalado que "un ataque

152 Informe del CICR de 2015 sobre los desafíos de los conflictos armados contemporáneos, nota 118 *supra*, pp. 56-57.

153 Informe del CICR de 2019 sobre los desafíos de los conflictos armados contemporáneos, nota 36 *supra*, p. 28.

154 CICR, nota 1 *supra*, p. 10. V. también P. Pascucci, nota 67 *supra*, que observa que la posición adoptada por la mayoría de los expertos en el Manual de Tallin respecto de los datos crea un "vacío en expansión en lo que respecta a qué constituye un bien", y luego afirma que "[n]o es realista en la era de la información que los datos queden excluidos del ámbito de los bienes, de modo de no gozar de la protección que confiere el DIH sobre la base de los principios de distinción y proporcionalidad".

155 Manual Militar de Dinamarca, nota 118 *supra*, p. 292.

156 Manual Militar de Noruega, nota 118 *supra*, párr. 9.58.

157 Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 14.

158 OEA, nota 22 *supra*, párr. 49, nota 115.

dirigido exclusivamente en contra de datos informáticos podría perfectamente generar consecuencias adversas que afecten a la población civil"[159].

En un mundo cada vez más dependiente de los datos informáticos, la cuestión de cómo interpretan los Estados las normas para proteger los datos esenciales contra la destrucción, la eliminación o la alteración será una forma definitiva de medir la adecuación de las normas humanitarias en vigor.

### *La protección de la infraestructura cibernética que se utiliza, a la vez, con fines militares y civiles*

Con el objeto de proteger la infraestructura civil crítica que depende del ciberespacio, es asimismo esencial proteger la infraestructura del propio ciberespacio. Sin embargo, el problema radica en la interconexión de las redes civiles y las redes militares. La mayoría de las redes militares dependen de la infraestructura informática civil, por ejemplo, los cables de fibra óptica submarinos, los satélites, los enrutadores o los nodos. Los vehículos civiles o el control de tráfico aéreo y marítimo están equipados, cada vez con mayor frecuencia, con dispositivos de navegación que dependen del sistema global de navegación por satélite (GNSS, por su sigla en inglés), como los satélites BeiDou, GLONASS, GPS y Galileo, que también pueden utilizar las fuerzas armadas. Las cadenas logísticas de suministro (de alimentos o de insumos médicos), entre otros sectores, usan la misma red de internet y de comunicaciones por la que se transmite parte de las comunicaciones militares. Salvo algunas redes que son de exclusivo uso militar, es prácticamente imposible diferenciar entre infraestructuras puramente civiles e infraestructuras puramente militares.

Según el DIH, los ataques deben ceñirse estrictamente a objetivos militares. En lo que respecta a los bienes, los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida. Todos los objetos que no son objetivos militares de acuerdo con esta definición son bienes de carácter civil en virtud del DIH y no deben ser objeto de ataques ni represalias. En caso de duda sobre si un objeto que normalmente sirve para fines civiles se utiliza para contribuir eficazmente a la acción militar, debe considerarse que continúa gozando de la protección que se otorga a los bienes de carácter civil[160].

Tradicionalmente, se considera que un objeto puede convertirse en un objetivo militar cuando su uso con fines militares es tal que satisface la definición de objetivo militar, aunque se use simultáneamente con fines civiles. Una interpretación amplia de esa norma llevaría a concluir que muchos objetos que forman parte de la infraestructura del ciberespacio constituirían objetivos militares y, por lo tanto, no estarían protegidos contra los ataques, sean estos cibernéticos o cinéticos. Esa situación produciría una gran inquietud, debido a la creciente dependencia civil del ciberespacio.

159 Ibíd., párr. 48.
160 V. PA I, art. 52. Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, normas 7-10.

No obstante, esa conclusión estaría incompleta. En primer lugar, el análisis de en qué momento un bien de carácter civil se convierte en un objetivo militar no puede realizarse para el ciberespacio o para internet en general. En cambio, los beligerantes deben identificar qué computadora, nodo, enrutador o red podría haberse convertido en un objetivo militar. En este sentido, los componentes de una red, una computadora específica u otro hardware que pueda separarse de una red o sistema deben analizarse de forma individual. Los medios y métodos empleados deben permitir dirigir el ataque a los objetivos militares específicos que puedan haberse identificado, y deben adoptarse todas las precauciones factibles para evitar, o al menos reducir todo lo posible, los daños que pudieran afectar incidentalmente al resto de los bienes de carácter civil o de los componentes de la red[161]. También se ha afirmado que está prohibido tratar como un único objetivo a un número evidentemente discreto de objetivos militares cibernéticos en infraestructuras cibernéticas que se emplean principalmente con fines civiles si así se dañara a personas o bienes protegidos[162]. En segundo lugar, el ciberespacio está diseñado con un alto nivel de redundancia, lo que implica que una de sus características es la capacidad de redirigir inmediatamente el tráfico de datos. Esa resiliencia intrínseca ha de tenerse en cuenta cuando se analiza si la destrucción o la neutralización del objetivo daría una ventaja militar definida como requiere la definición de objetivo militar. De no ser así, el bien seguiría considerándose civil y no puede ser objeto de ataque. Y, en tercer lugar, todos los ataques están regidos por la prohibición de realizar ataques indiscriminados y por los principios de proporcionalidad y precaución en el ataque. Hacer cesar o alterar el uso civil de un bien de manera violatoria de una de esas normas transformaría en ilícito el ataque, aunque el bien se hubiera convertido en un objetivo militar[163].

En comparación con las operaciones militares cinéticas, dependiendo de las circunstancias, el uso de ciberoperaciones puede permitir el logro de un efecto particular causando una menor destrucción (del objetivo o, incidentalmente, de otros bienes o sistemas) o causando daños que pueden repararse más fácilmente. Esta consideración es de particular importancia para el uso de objetos de uso dual, como se ilustra en la situación de un beligerante que trata de neutralizar un búnker subterráneo de mando interrumpiendo el suministro de electricidad de una red que alimenta también a la infraestructura civil. Una ciberoperación puede habilitar

161 V. PA I, arts. 51(4), 57(2)(a)(ii); Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, normas 12-17.

162 V. Manual de Tallin 2.0, nota 13 *supra*, norma 112, que surge de la prohibición de los ataques por bombardeo que determinan el art. 51(5)(a) del PA I y el DIH consuetudinario (v. Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 13).

163 Aunque reconoce la existencia de la otra opinión, el Grupo de Trabajo sobre la conducción de hostilidades de la ADI pensó que esta es "la mejor opinión" basándose en la práctica de los Estados, la doctrina y los documentos oficiales: v. Informe ADI, nota 147 *supra*, pp. 336-337. V. también CICR, *International Expert Meeting Report: The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law*, Ginebra, 2018, p. 39, disponible en www.icrc.org/en/document/international-expert-meeting-reportprinciple-proportionality; Helen Durham, discurso de apertura, en Edoardo Greppi (ed.), *Conduct of Hostilities: The Practice, the Law and the Future*, XXXVII Mesa Redonda sobre problemas actuales del derecho internacional humanitario, San Remo, 2015, p. 31.

al operador a elegir qué componentes de la red afectar de manera remota[164]. De esta forma, se podría permitir que la parte que ataca alcanzara el efecto deseado evitando, o al menos reduciendo todo lo posible, los efectos adversos en el suministro de electricidad a los civiles. En ese caso, y siempre y cuando la decisión de utilizar una ciberoperación en lugar de una operación cinética sea *factible*, el principio de precaución indicaría que se debe elegir la ciberoperación. De hecho, la obligación de tomar todas las precauciones factibles en la elección de los medios y métodos de ataque para evitar o, al menos, reducir todo lo posible los daños civiles incidentales[165] es tecnológicamente neutral: también se aplica a los medios y métodos basados en las nuevas tecnologías, e incluso puede exigir su uso[166]. Si eso es factible en una instancia concreta, dependerá de las circunstancias imperantes en el momento, incluidas las consideraciones humanitarias y militares[167].

## Limitaciones a las ciberoperaciones que no están consideradas "ataques", incluida la protección específica a determinadas personas y bienes

Si bien muchas normas generales relativas a la conducción de las hostilidades se limitan a actos que se consideran ataques en virtud del DIH, algunas normas de este ordenamiento jurídico relativas a la conducción de las hostilidades se aplican a un conjunto más amplio de operaciones. En primer lugar, unas pocas normas se aplican a todas las "operaciones militares" y, en segundo lugar, la protección específica de la que gozan determinadas categorías de personas y bienes trasciende la protección contra los ataques.

### *Normas que rigen las operaciones militares que no constituyen ataques*

Identificar y, en lo posible, elucidar el significado de las normas que confieren protección general a la población civil y a los bienes de carácter civil contra los efectos de las ciberoperaciones que no constituyen ataques es una cuestión que merece una mayor atención, más aún si se adopta la postura de que solo se consideran ataques las operaciones que causan daños físicos. En ese caso, habría una categoría bastante amplia de ciberoperaciones a las que solo se aplica un conjunto limitado de normas del DIH. Esa conclusión generaría verdaderas dificultades en lo que atañe a la protección de los civiles y de la infraestructura civil.

164 Se ha señalado que en las ciberoperaciones de 2015 contra la red eléctrica de Ucrania se lanzó una ciberoperación de este tipo. V. Kim Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid", *Wired*, 3 de marzo de 2016, disponible en www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

165 PA I, art. 57(2)(a)(ii); Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 17.

166 V. Informe ADI, nota 147 *supra*, p. 384.

167 Si bien las consideraciones militares podrían incluir la "fragilidad" de los medios y métodos cibernéticos, ese no es el único factor relevante para determinar la factibilidad. No es posible descartar que es factible —y que, por lo tanto, se debe— recurrir a ciberoperaciones para evitar o reducir todo lo posible los daños civiles incidentales con el único criterio de que los medios y métodos cibernéticos utilizados son "frágiles", sin prestar atención a la situación en su conjunto, incluidas todas las consideraciones humanitarias pertinentes.

La noción de "operación militar" aparece en numerosos artículos de los Convenios de Ginebra de 1949 y en sus Protocolos adicionales de 1977[168]. De mayor interés a los fines del presente artículo son las normas que regulan la conducción de las operaciones militares, incluidas las que se realizan por medios cibernéticos. Entre ellas, la norma básica de que "las Partes en conflicto […] dirigirán sus operaciones únicamente contra objetivos militares" (PA I, artículo 48), el principio de que "[l]a población civil y las personas civiles gozarán de protección general contra los peligros procedentes de operaciones militares" (PA I, artículo 51(1))[169] y la obligación de que las operaciones militares se realicen "con un cuidado constante de preservar a la población civil, a las personas civiles y a los bienes de carácter civil" (PA I, artículo 57(1))[170].

El significado corriente del término "operaciones militares" y la interpretación sistemática de esos artículos lleva a concluir que esta noción es distinta de la de "ataque" según la definición del artículo 49 del PA I[171]. Mientras que el Comentario del CICR del artículo 48 del PA I señala que la noción hace referencia a las operaciones militares en las que se usa la violencia, y no a campañas ideológicas, políticas o religiosas, aclara que se trata una noción más amplia que la de "ataque". El Comentario define "operaciones militares" a los efectos de esos artículos como "cualquier movimiento, maniobra y otra actividad realizada por las fuerzas armadas con miras a combatir" o "relacionada con las hostilidades", una interpretación que está ampliamente aceptada[172].

168 V. CG III, art. 23; CG IV, art. 28; PA I, arts. 3, 39, 44, 51, 56-60; PA II, art. 13.

169 V. también PA I, art. 58; PA II, art. 13(1).

170 V. también Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 15; Manual de Tallin 2.0, nota 13 *supra*, norma 114.

171 Una interpretación que asimilara las nociones de "operación" y "ataque" privaría de contenido valioso a las normas aplicables a las operaciones y las tornaría superfluas. V. C. Droege, nota 83 *supra*, p. 556.

172 Comentario del CICR del PA I, nota 110 *supra*, párrs. 2191, 1936, 1875. En este misma línea, v. Michael Bothe, Karl Josef Partsch y Waldemar A. Solf, *New Rules for Victims of Armed Conflict: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Leiden, 2013, párr. 2.2.3 sobre el art. 48, párr. 2.8.2 sobre el art. 57; Ministerio de Defensa del Reino Unido, *The Joint Service Manual of the Law of Armed Conflict* (Manual Militar del Reino Unido), Joint Service Publication 383, 2004, párr. 5.32, nota 187; Informe ADI, nota 147, p. 380. El *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Programa de investigación de políticas humanitarias y conflictos, Universidad de Harvard, 2009) establece la obligación de tener cuidado constante en las "operaciones de combate aéreo o con misiles" (norma 34), una noción más amplia que la de "ataque" que incluye, entre otras cosas, el abastecimiento de combustible, la interferencia de los radares del enemigo, el uso de sistemas de alerta aerotransportados y el lanzamiento de fuerzas aerotransportadas (comentario de la norma 1(c), párr. 3). V. también Noam Neuman, "A precautionary tale: The theory and practice of precautions in attack", *Israel Yearbook on Human Rights*, vol. 48, 2018, p. 28; Jean-François Quéguiner, "Precautions under the Law Governing the Conduct of Hostilities", *International Review of the Red Cross*, vol. 88, n.º 864, 2006, p. 797 [trad. esp. "Precauciones previstas por el derecho relativo a la conducción de las hostilidades", p. 5, disponible en https://www.icrc.org/es/doc/assets/files/other/irrc_864_queguiner.pdf]; Chris Jenks y Rain Liivoja, "Machine autonomy and the constant care obligation", *Humanitarian Law and Policy*, 11 de diciembre de 2018, disponible en https://blogs.icrc.org/law-and-policy/2018/12/11/machine-autonomy-constant-care-obligation/. Específicamente sobre las ciberoperaciones, v. Manual de Tallin 2.0, nota 13 *supra*, párr. 2 del comentario de la norma 114 (donde se observa que la noción de hostilidades, a la que se aplica la obligación de cuidado constante, es más amplia que la de ataque); H. Harrison Dinniss, nota 124 *supra*, p. 199. Para una opinión distinta, al menos con respecto al principio de distinción, v. M. Roscini, nota 126 *supra*, p. 178.

El análisis de esa noción se centra principalmente en la obligación que establecen el derecho convencional y el derecho consuetudinario de realizar las operaciones militares con un cuidado constante para preservar a la población civil, a las personas civiles y a los bienes de carácter civil. Francia ha expresado que esa obligación se aplica también en el ciberespacio[173]. Esta obligación exige que todos los que participan en operaciones militares tengan siempre presentes las consecuencias de las operaciones militares para la población civil, las personas civiles y los bienes de carácter civil, adopten medidas para reducir todo lo posible esas consecuencias y traten de prevenir los efectos innecesarios[174]. Se la ha definido como una obligación positiva y continua que tiene por finalidad a mitigar los riesgos y prevenir los daños que impone exigencias que aumentan a medida que aumenta el riesgo para los civiles[175]. A este respecto, el Manual de Tallin explica:

> [e]l derecho no admite situaciones, o momentos, en que las personas que participan en los procesos de planificación y ejecución no tengan en cuenta las consecuencias de sus operaciones para los civiles o los bienes de carácter civil. En el ámbito cibernético, esto requiere un conocimiento constante de la situación, no solo durante la etapa de preparación de una operación[176].

Más problemática aún es la cuestión de la aplicación del principio de distinción a las operaciones militares que no constituyen ataques. Como se ha comentado, el artículo 48 del PA I exige que las operaciones militares se dirijan exclusivamente a objetivos militares. Si bien los comentarios del CICR y los de Bothe, Partsch y Solf[177] hacen hincapié en el carácter fundamental de este artículo, no aclaran demasiado el significado y el alcance exactos de la obligación, que continúan siendo materia de debate.

El artículo 48 se interpreta en ocasiones como un principio general que se implementa a través de la aplicación de numerosas normas de la sección correspondiente del Protocolo a la que da inicio. Así pues, algunos autores sostienen que las normas específicas que dimanan del principio de distinción se aplican solo a los ataques y no a las operaciones militares que no constituyen ataques[178]. En consonancia con esa opinión, algunos manuales militares establecen expresamente que las ciberoperaciones que no constituyen ataques pueden dirigirse contra civiles

173 Ministerio de los Ejércitos de Francia, nota 77 *supra*, p. 15.

174 Manual Militar del Reino Unido, nota 172 *supra*, párr. 5.32.1; Manual de Tallin 2.0, nota 13 *supra*, párr. 4 del comentario de la norma 114; Dieter Fleck, *The Handbook of International Humanitarian Law*, tercera edición, Oxford University Press, Oxford, 2013, p. 199; N. Neuman, nota 172 *supra*, pp. 28-29.

175 Informe ADI, nota 147 *supra*, p. 381.

176 Manual de Tallin 2.0, nota 13 *supra*, párr. 4 del comentario de la norma 114.

177 M. Bothe, K. J. Partsch y W. A. Solf, nota 172 *supra*.

178 M. Roscini, nota 126 *supra*, p. 178. V. también, expresado en virtud del derecho consuetudinario, Manual de Tallin 2.0, nota 13 *supra*, párr. 5 del comentario de la norma 93; Michael N. Schmitt, "'Attack' as a term of art in international law: The cyber operations context", en Christian Czosseck, Rain Ottis y Katharina Ziolkowski (eds.), *4th International Conference on Cyber Conflict: Proceedings*, NATO CCD COE Publications, Tallin, 2012, pp. 283-293, 289-290.

o contra bienes de carácter civil[179]. Para los Estados Partes en el Protocolo no sería fácil conciliar esa afirmación con el artículo 48, o al menos habría que formularla con mayor precisión. De hecho, los expertos han señalado que "[s]i bien […] existe una distinción entre operaciones militares y ataques, eso no implica que los ataques no violentos a redes informáticas puedan dirigirse a bienes de carácter civil"[180]. Esta conclusión se desprende de las normas de interpretación de los tratados, que requieren que las disposiciones sean interpretadas de modo que su "contenido tenga propósito y no sea superfluo"[181].

Como ya se ha observado, se entiende por "operaciones militares" los movimientos, maniobras y otras actividades realizadas por las fuerzas armadas con miras al combate o las hostilidades[182]. Por ejemplo, establecer un acceso remoto a un sistema o dispositivo podría ser un paso para alcanzar o atacar otro sistema o dispositivo[183]. En el supuesto de que el primer sistema o dispositivo sea de naturaleza civil y el segundo, un objetivo militar, puede surgir la pregunta de si establecer el acceso al sistema o dispositivo civil constituiría una operación militar prohibida. A nuestro juicio, una situación semejante no parece ser violatoria del artículo 48 porque, en última instancia, la operación está dirigida a un objetivo militar[184]. De hecho, esas ciberoperaciones pueden evaluarse de la misma forma que las operaciones militares convencionales; por ejemplo, cuando una unidad militar atraviesa una vivienda para atacar un objetivo militar que se ubica detrás. Aun así, otras obligaciones seguirían siendo pertinentes, por ejemplo, la obligación de tener cuidado constante de preservar los bienes de carácter civil.

En nuestra opinión, debe interpretarse que el artículo 48, por sí mismo o en conjunto con los artículos 51(1) y 57(1) del PA I, prohíbe las ciberoperaciones destinadas exclusivamente a interrumpir el servicio de internet para la población civil, incluso si esas ciberoperaciones no inutilizan bienes ni tienen consecuencias que hagan que se las considere ataques. En la actualidad, el uso civil de internet está tan extendido que cualquier otra interpretación dejaría un vacío importante en la

179 Manual Militar de Noruega, nota 118 *supra*, párr. 9.57. V. también Manual de derecho de la guerra del DoD, nota 87 *supra*, párr. 16.5.2.

180 H. Harrison Dinniss, nota 124 *supra*, p. 199.

181 V. también C. Droege, nota 83 *supra*, p. 556.

182 V., p. ej., DoD de Estados Unidos, *Cyberspace Operations*, Joint Publication 3-12, 8 de junio de 2018, p. xii: "Movimientos y maniobras. Las operaciones del ciberespacio permiten proyectar la fuerza sin la necesidad de establecer una presencia física en territorio extranjero. Las maniobras de la red informática del Departamento de Defensa u otro espacio cibernético azul [amigo] incluyen el posicionamiento de fuerzas, sensores y defensas a fin de reforzar la seguridad en zonas del ciberespacio o participar en acciones defensivas cuando sea necesario. Las maniobras del ciberespacio gris [neutral] y rojo [enemigo] son acciones de explotación del ciberespacio e incluyen actividades tales como acceder a los enlaces y nodos del adversario, enemigo o intermediario y preparar ese ciberespacio a fin de dar soporte a acciones futuras".

183 L. Gisel y L. Olejnik (eds.), nota 11 *supra*, p. 57.

184 Comparar con H. Harrison Dinniss, nota 124 *supra*, p. 201.

protección que el DIH confiere a los civiles contra los efectos de las hostilidades emprendidas con medios cibernéticos[185].

Como se ha observado, algunos autores sostienen que no todas las ciberoperaciones que inutilizan bienes, o que eliminan o alteran datos, constituyen ataques. Como consecuencia de esas interpretaciones, un rango considerablemente más amplio de ciberoperaciones no estaría regido por las normas que se aplican a los ataques, incluidas las operaciones que generarían un riesgo considerable de daños. Por lo tanto, es de suma importancia para la protección de la población civil que todos los que interpretan rigurosamente las nociones de "ataque" y "bienes" aclaren si consideran que las ciberoperaciones que solo inutilizan objetos o eliminan datos constituyen "operaciones militares", y qué significa esto para la aplicación del principio de distinción a dichas operaciones, en especial, lo que implica la exigencia del artículo 48 del PA I de que las partes en conflictos armados "diri[jan] sus operaciones únicamente contra objetivos militares". Por ejemplo, debería conservarse, al menos, determinado nivel de protección si quienes interpretan la noción de "ataque" aceptan estrictamente que una ciberoperación que solo inutiliza bienes es una "operación militar" que, como consecuencia, debe dirigirse solo contra objetivos militares.

Hasta las ciberoperaciones que no están comprendidas en la noción de "operación militar" en virtud del PA I podrían estar reguladas por algunas normas del DIH basadas en el principio de distinción. Por ejemplo, se ha señalado que "dirigir" operaciones psicológicas o propaganda de otro tipo a los civiles no sería violatorio del artículo 48 del PA I, porque esas operaciones no estarían comprendidas en el significado de "operaciones militares" según el artículo 48[186]. Aun así, las operaciones psicológicas no están fuera del alcance de la protección de otras normas del DIH. Por ejemplo, no deben ser actos prohibidos ni amenazas de violencia cuya finalidad principal sea sembrar el terror entre la población civil o incitar a la violación del DIH[187].

Las limitaciones a las ciberoperaciones que no constituyen ataques también pueden derivar del principio de necesidad militar. Sobre la base de la norma consuetudinaria correspondiente del Reglamento de la Haya de 1907, el Manual del derecho de la guerra del DoD establece que "[u]na ciberoperación que no constituye un ataque pero que, de todos modos, expropia o destruye propiedades enemigas ha de estar exigida imperiosamente por las necesidades de la guerra"[188]. El Manual también hace referencia a la necesidad militar en forma más general, y aclara que

185 Los expertos encargados de la redacción del Manual de Tallin debatieron acerca de si la interrupción de todas las comunicaciones de correo electrónico de un país durante un conflicto armado constituía un ataque: una noción más acotada que la de operaciones militares. Si bien una minoría fue de la opinión de que la comunidad internacional, por lo general, consideraría que una operación de ese tipo sería equiparable a un ataque, la mayoría sostuvo que, en ese momento, el DIH no tenía un alcance tan amplio, aunque consideró que era razonable clasificar como ataques a esas operaciones. Manual de Tallin 2.0, nota 13 *supra*, párr. 13 del comentario de la norma 92.

186 C. Droege, nota 83 *supra*, p. 556.

187 Informe del CICR de 2019 sobre los desafíos de los conflictos armados contemporáneos, nota 36 *supra*, pp. 28-29.

188 Manual del derecho de la guerra del DoD, nota 87 *supra*, párr. 16.5.1.

las ciberoperaciones que no constituyen ataques "no deben dirigirse contra civiles enemigos ni contra bienes de carácter civil enemigos, a menos que las operaciones sean exigidas por la necesidad militar"[189]. En la misma línea, Australia observa que "[l]as normas del DIH aplicables también se aplicarán a las ciberoperaciones realizadas durante un conflicto armado que no constituyan ni alcancen el nivel de un 'ataque', incluido el principio de necesidad militar"[190]. Si bien esas referencias a la necesidad militar como principio restrictivo son útiles, se necesita una mayor claridad respecto de qué prescribe exactamente el principio de necesidad militar en la conducción de las ciberoperaciones.

Este breve análisis muestra que las ciberoperaciones que no constituyen ataques no carecen de regulación. Sin embargo, el ordenamiento jurídico que rige dichas operaciones sigue siendo menos completo, preciso y exigente que el que rige las operaciones que constituyen ataques en el sentido del DIH. Para resolver este vacío en la protección, al menos en cierta medida, Schmitt propone que los Estados realicen –en el ámbito de las políticas– una evaluación de proporcionalidad adaptada a las ciberoperaciones que no constituyen ataques[191].

La protección específica que el DIH prevé para determinadas personas y bienes restringe aún más el conjunto de las operaciones militares permitidas.

### *Normas del DIH que confieren protección a los bienes indispensables para la supervivencia de la población civil, los servicios sanitarios y las operaciones de socorro humanitario*

Además de las normas generales que rigen la conducción de las hostilidades, el DIH establece regímenes específicos para determinados bienes y servicios que confieren mayor protección que la que se proporciona a todos los civiles y los bienes de carácter civil.

Por ejemplo, el DIH específicamente considera ilícito "atacar, destruir, sustraer o inutilizar los bienes indispensables para la supervivencia de la población civil"[192]. Esta norma protege, por ejemplo, "los artículos alimenticios", "las zonas agrícolas que los producen" y "las instalaciones y reservas de agua potable y las obras de riego"[193]. Si bien concluyeron de que internet como tal no puede considerarse un bien indispensable para la supervivencia de la población civil, los redactores del Manual de Tallin señalaron, a la vez, que "la infraestructura cibernética indispensable para el funcionamiento de los generadores eléctricos,

189 Ibíd., párr. 16.5.2.

190 Departamento de Asuntos Exteriores y Comercio de Australia, nota 94 *supra*, p. 4.

191 M. N. Schmitt, nota 67 *supra*, p. 18: "Los Estados se comprometerían, como cuestión de política, a abstenerse de ejecutar operaciones cibernéticas a las cuales no se aplican las normas del DIH que rigen los ataques cuando los efectos negativos concretos para las personas civiles o la población civil sean excesivos en comparación con el beneficio concreto relacionado con el conflicto que se espera obtener con dichas operaciones".

192 V. PA I, art. 54(2); PA II, art. 14; Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 54.

193 PA I, art. 54(2).

las obras de riego y las instalaciones de agua potable, y los establecimientos de producción de alimentos podría considerarse, en virtud de las circunstancias, un bien indispensable"[194]. La inclusión del término "inutilizar" indica que el conjunto de operaciones que pueden tener impacto en esos bienes no se limita a los ataques y la destrucción. Como se observa en el Comentario del CICR del artículo 54(2) del PA I, la intención de los redactores era "abarcar todas las posibilidades" de cómo pueden inutilizarse los bienes indispensables para la subsistencia de la población civil[195]. Hoy en día, las ciberoperaciones que están diseñadas para inutilizar, o de las que se espera que inutilicen, bienes indispensables para la población civil están prohibidas, independientemente de si constituyen ataques o no. Por lo tanto, el debate sobre si las operaciones militares dirigidas a esos bienes constituyen ataques (como se ha analizado) es irrelevante para estos bienes.

El DIH también brinda protección específica a los servicios sanitarios. Dada la importancia fundamental de la asistencia de salud para todos los afectados por conflictos armados, los beligerantes deben respetar y proteger los establecimientos y el personal sanitario en todo momento[196]. La obligación de "respetar" las unidades y el personal sanitarios implica no solo la protección contra las operaciones que constituyen ataques, sino que también la prohibición de "causarles daño por cualquier medio. Eso quiere decir, asimismo, que no se deberá interferir en su labor (por ejemplo, impidiendo el transporte de insumos) o anulando la posibilidad de que continúen asistiendo a los heridos y los enfermos que están a su cuidado"[197]. La protección especial de que gozan los establecimientos sanitarios incluye las comunicaciones médicas: si bien, por lo general, interferir las comunicaciones del enemigo se considera permisible, "la interrupción

194 Manual de Tallin 2.0, nota 13 *supra*, párr. 5 del comentario de la norma 141.

195 Comentario del CICR del PA I, nota 110 *supra*, párrs. 2101, 2103.

196 V., p. ej., CG I, art. 19; CG II, art. 12; CG IV, art. 18; PA I, art. 12; PA II, art. 11; Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, normas 25, 28, 29; Manual de Tallin 2.0, nota 13 *supra*, normas 131-132. La protección de las unidades y el personal sanitarios cesará solamente cuando se los utilice, al margen de sus fines humanitarios, con objeto de realizar actos perjudiciales para el enemigo. Sin embargo, la protección puede cesar sólo después de una intimación dando, en todos los casos oportunos, un plazo razonable, y que no haya surtido efectos. V. CG I, art. 21; CG II, art. 34; CG IV, art. 19; PA I, art. 13; PA II, art. 11(2); Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, normas 25, 28, 29; Manual de Tallin 2.0, nota 13 *supra*, norma 134.

197 Comentario del CICR del PA I, nota 110 *supra*, párr. 517. V. también Comentario del CICR del CG I, nota 69 *supra*, párr. 1799; Declaración de Oxford, nota 32 *supra*, punto 5 ("Durante un conflicto armado, el derecho internacional humanitario determina que las unidades, los vehículos y el personal sanitarios sean respetados y protegidos en todo momento. En consecuencia, las partes en un conflicto armado no deben interrumpir el funcionamiento de los establecimientos sanitarios por medio de ciberoperaciones; deben tomar todas las precauciones factibles para facilitar el funcionamiento de las unidades sanitarias y para prevenir los daños incidentales causados por las ciberoperaciones y; deben adoptar todas las medidas que sean factibles para facilitar el funcionamiento de las unidades sanitarias y para prevenir los daños, incluso los causados por ciberoperaciones"); Manual de Tallin 2.0, nota 13 *supra*, párr. 5 del comentario de la norma 131 ("Por ejemplo, esta norma [norma 131, que prevé que "[e]l personal sanitario y religioso, las unidades sanitarias y los vehículos sanitarios deben ser respetados y protegidos y, en especial, no deben ser objeto de ataque"] prohibiría la alteración de datos en el Sistema de Posicionamiento Global de un helicóptero sanitario con el fin de desviarlo, aunque la operación no constituya un ataque a un vehículo sanitario").

intencional de las capacidades de comunicación con fines médicos de las unidades [sanitarias]" puede no estar permitida, incluso si las unidades sanitarias establecen comunicaciones con las fuerzas armadas[198]. Asimismo, la obligación de respetar y proteger los establecimientos sanitarios abarca la prohibición de eliminar, alterar o afectar negativamente los datos médicos[199]. También puede proteger contra las ciberoperaciones que afectan la confidencialidad de los datos médicos, que al menos en algunas circunstancias sería difícil de conciliar con la obligación de proteger y respetar los establecimientos sanitarios[200]. Los datos relevantes en el contexto médico incluyen los "datos necesarios para el uso adecuado de los equipos médicos y para el control del inventario de los insumos médicos", así como "los datos médicos personales necesarios para el tratamiento de los pacientes"[201]. La obligación de "proteger" los establecimientos sanitarios, incluidos sus datos, conlleva obligaciones positivas. Las partes en conflicto deben adoptar activamente medidas para proteger, siempre que sea factible, los establecimientos sanitarios contra los daños, incluso contra los daños causados por las ciberoperaciones[202].

El DIH también prescribe que el personal humanitario y los envíos de socorro deben ser respetados y protegidos[203]. En efecto, esta obligación prohíbe cualquier "ataque" contra las operaciones humanitarias. Al igual que en el caso de la obligación de respetar y proteger al personal y los establecimientos sanitarios, debe entenderse que las normas pertinentes prohíben "otras formas de conductas dañinas fuera de la conducción de hostilidades" contra el personal humanitario o la interferencia indebida en su labor[204]. Más aún, las partes en un conflicto armado deben aceptar, permitir y facilitar las operaciones de socorro humanitario[205]. En consonancia con esto, la norma 145 del Manual de Tallin 2.0 establece que "las ciberoperaciones no estarán diseñadas ni se conducirán para interferir indebidamente en los esfuerzos imparciales para brindar asistencia humanitaria" y especifica que esas operaciones están prohibidas "incluso cuando no alcanzan

198 Comentario del CICR del PA I, nota 110 *supra*, párr. 1804.

199 Informe del CICR de 2015 sobre los desafíos de los conflictos armados contemporáneos, nota 118 *supra*, p. 56.

200 V. L. Gisel y L. Olejnik (eds.), nota 11 *supra*, p. 36, donde se analiza una situación hipotética de interferencia en las historias clínicas y registros administrativos de un establecimiento sanitario con el objetivo de conocer la fecha en que un jefe militar enemigo asistirá a una consulta médica para capturarlo o matarlo en el trayecto. Esto podría interferir en exceso en el funcionamiento del establecimiento sanitario y afectar la capacidad de los profesionales de la salud de observar el principio ético de preservar la confidencialidad de los datos médicos. En el Manual de Tallin 2.0, nota 13 *supra*, párr. 2 del comentario de la norma 132, se proporciona el siguiente ejemplo de una operación que no sería violatoria del DIH: "...un reconocimiento informático que no causa daños para determinar si el establecimiento y los vehículos sanitarios en cuestión (o las computadoras, las redes informáticas y los datos asociados) se utilizan indebidamente para cometer actos dañinos desde una perspectiva militar".

201 Manual de Tallin 2.0, nota 13 *supra*, párr. 3 del comentario de la norma 132.

202 Comentario del CICR del CG I, nota 69 *supra*, párrs. 1805-1808; Manual de Tallin 2.0, nota 13 *supra*, párr. 6 del comentario de la norma 131.

203 PA I, arts. 70(4), 71(2); Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, normas 31, 32.

204 Comentario del CICR del GC I, nota 69 *supra*, párrs. 1358, 1799.

205 V., p. ej., CG IV, art. 59; PA I, arts. 69-70; Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 55.

el nivel de un 'ataque'"[206]. Debe entenderse que la obligación de respetar y proteger al personal y las operaciones de socorro implica la protección de los datos relevantes[207]. Al menos para los Estados Partes en el PA I, la protección de los datos humanitarios debe abarcar los datos del CICR necesarios para que la organización "pueda desempeñar las tareas humanitarias que se le atribuyen en los Convenios [de Ginebra] y en el presente Protocolo a fin de proporcionar protección y asistencia a las víctimas de los conflictos"[208].

Estas protecciones especiales muestran que el DIH prevé normas más estrictas para las operaciones militares contra determinados bienes o servicios esenciales para la supervivencia, la salud y el bienestar de la población civil.

## La importancia de los exámenes jurídicos de los medios y métodos cibernéticos de la guerra para garantizar el respeto del DIH

A la luz de las dificultades específicas que plantean las características del ciberespacio para la interpretación y la aplicación de algunos principios del DIH en la conducción de las hostilidades, las partes en un conflicto armado que deciden desarrollar, adquirir o adoptar armas, medios y métodos de guerra que dependen de tecnologías digitales han de hacerlo con cuidado. En este sentido, los Estados Partes en el PA I que desarrollan o adquieren capacidades de guerra cibernéticas –con propósitos tanto ofensivos como defensivos– tienen la obligación de evaluar si el empleo de un arma, medio o método cibernético estaría prohibido por el derecho internacional en ciertas condiciones o en todas las circunstancias[209]. En un sentido más amplio, los exámenes jurídicos son fundamentales para que todos los Estados garanticen que sus fuerzas armadas respetan el DIH[210], empleando solo armas, medios o métodos de guerra, incluidos los que dependen de la tecnología cibernética, que cumplan las obligaciones que el DIH impone al Estado en cuestión[211]. En esos exámenes, se deberá adoptar un enfoque multidisciplinario que incluya los expertos jurídicos, militares y técnicos pertinentes[212]. Los exámenes jurídicos deben realizarse con anterioridad y en mayor profundidad que la evaluación de la licitud de la utilización de una herramienta en la circunstancia específica de un ataque.

206 Manual de Tallin 2.0, nota 13 *supra*, párr. 4 del comentario de la norma 80.

207 Para un análisis más pormenorizado, v. Tilman Rodenhäuser, "Hacking humanitarians? IHL and the protection of humanitarian organizations against cyber operations", *EJIL: Talk!*, 16 de marzo de 2020, disponible en www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyberoperations/.

208 PA I, art. 81. Esos datos incluyen, entre otros, los necesarios para establecer agencias de búsqueda con el objeto de recopilar datos de personas dadas por desaparecidas en el contexto de un conflicto armado o los que recoge el CICR cuando visita y realiza entrevistas privadas a personas detenidas.

209 PA I, art. 36.

210 V. art. 1 común; Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 139.

211 CICR, *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos: Medidas para aplicar el artículo 36 del Protocolo adicional I de 1977*, Ginebra, 2006, p. 1.

212 Ibíd., p. 21.

En vista de lo novedoso de la tecnología, es fundamental prestar especial atención al examen jurídico de las armas, los medios y los métodos de guerra cibernéticos. La prohibición de las armas cuyos efectos son indiscriminados puede ser especialmente relevante dada la capacidad de autopropagarse de forma autónoma que tienen determinadas herramientas cibernéticas[213]. No obstante, el examen jurídico de las armas, los medios y los métodos cibernéticos puede presentar numerosas dificultades. A continuación, ilustraremos algunas cuestiones, aunque sin pretender ser exhaustivos.

En primer lugar, un Estado que realiza un examen jurídico debe determinar sobre la base de qué normas jurídicas examina una herramienta cibernética. Dicho de otro modo, el Estado deberá conocer las respuestas a algunas de las cuestiones analizadas con anterioridad, por ejemplo, si el uso de una herramienta puede considerarse un ataque y si, en consecuencia, está sujeto a un amplio conjunto de normas del DIH. Para cuestiones en las que el derecho no es claro o no hay una posición establecida, se deberá adoptar un enfoque prudente, a fin de evitar que parezca que el empleo de la herramienta cibernética fue ilícito o debería haber sido calificado de ilícito.

En segundo lugar, el Estado debe determinar qué necesita examinar. Esto no es necesariamente evidente cuando se trata de herramientas o capacidades cibernéticas, como se observa en el uso generalizado de esos términos en lugar de nociones como la de armas cibernéticas. Los expertos han analizado si las herramientas o las capacidades cibernéticas son armas, medios o métodos de guerra y qué implicancias tiene eso para el examen jurídico[214]. De todos modos, como ya se ha observado, los Estados Partes en el PA I deben examinar todas sus herramientas o capacidades cibernéticas que se consideran armas, medios o métodos de guerra. Para los Estados que no son Partes en el PA I, la obligación de que sus fuerzas armadas respeten y hagan respetar el DIH y la novedad del uso de las tecnologías digitales como armas, medios o métodos de guerra harían que fuese prudente incluir la mayor cantidad de elementos posibles en el examen de las capacidades[215].

En tercer lugar, un arma o medio de guerra no debería evaluarse sin considerar la forma en la que se utilizará, es decir que, en el examen jurídico, ha de tenerse en cuenta el uso normal o previsto del arma o medio de guerra. Sin embargo, las capacidades militares cibernéticas están menos normalizadas que las armas cinéticas, en especial, cuando están diseñadas para una operación específica.

213 V. Estudio del CICR sobre derecho internacional consuetudinario, nota 63 *supra*, norma 71. Para un ejemplo de las cuestiones que plantea el examen jurídico de las armas cibernéticas, v. "Scenario 10: Cyber weapons review", en K. Mačák, T. Minárik y T. Jančárková (eds.), nota 68 *supra*.

214 Jeffrey T. Biller y Michael N. Schmitt, "Classification of cyber capabilities and operations as weapons, means, or methods of warfare", *International Law Studies*, vol. 95, 2019, p. 219.

215 P. ej., mientras que el DoD de Estados Unidos adoptó la política de realizar exámenes jurídicos de las armas, incluidas las que incorporan capacidades cibernéticas (Manual de Guerra del DoD, nota 87 *supra*, párr. 16.6), la instrucción correspondiente de la Fuerza Aérea de Estados Unidos determina que deben examinarse las armas y las capacidades cibernéticas: Departamento de la Fuerza Aérea de Estados Unidos, *Legal Reviews of Weapons and Cyber Capabilities*, Air Force Instruction 51-402, 27 de julio de 2011.

Esto implicaría que el examen ha de realizarse teniendo en cuenta el entorno cibernético específico en el que es probable que se use el arma.

En cuarto lugar, y en relación con lo anterior, el Estado deberá realizar un examen jurídico no solo para un arma, medio o método de guerra que piensa adquirir o adoptar por primera vez, sino también cuando modifica un arma, medio o método que ya ha sido aprobado en un examen jurídico anterior. Esto puede ser un problema en el caso de las herramientas cibernéticas que probablemente sean objeto de adaptaciones frecuentes, incluso en respuesta a las actualizaciones de seguridad del software de los posibles objetivos de un ataque. Si bien es necesario seguir precisando la cuestión del tipo y la magnitud del cambio que exigiría un nuevo examen jurídico, este debe realizarse, en especial, cuando el arma, medio o método de guerra se modifica de forma que se altera su función o cuando la modificación podría tener un impacto en si el empleo del arma, medio o método de guerra se haría conforme a derecho[216]. Al respecto, se ha observado, en relación con las armas cibernéticas, que "la evaluación de si un cambio afectará el funcionamiento de un programa debe ser de índole cualitativa y no cuantitativa"[217]. Para que un examen jurídico sea eficaz, los Estados que estudian, desarrollan, adquieren o adoptan nuevas armas, medios o métodos que incorporan nuevas tecnologías deben analizar esas y otras complejidades. Dicho de otro modo, los procedimientos de prueba deben adaptarse a las características peculiares de las tecnologías digitales. A la luz de las complejidades mencionadas, una práctica idónea mediante la cual todos los Estados podrían garantizar el respeto del DIH sería compartir información sobre sus mecanismos de examen jurídico y, siempre que sea factible, sobre los resultados sustanciales de sus exámenes jurídicos[218]. Esto tendría especial importancia si surgieran problemas de compatibilidad de un arma con el DIH, para que los otros Estados no tuvieran que enfrentarse a los mismos problemas y pudieran beneficiarse de las conclusiones del Estado que realiza el examen acerca de si el uso de la herramienta en cuestión está prohibido por el DIH. El intercambio de información sobre los exámenes jurídicos de las armas, medios o métodos de guerra que incorporan nuevas tecnologías también puede ayudar a generar conocimiento y a identificar buenas prácticas, así como ayudar a los Estados que deseen establecer o fortalecer sus propios mecanismos de examen jurídico[219].

216 CICR, nota 211 *supra*, p. 8-9.

217 Gary D. Brown y Andrew O. Metcalf, "Easier said than done: Legal reviews of cyber weapons", *Journal of National Security Law and Policy*, vol. 7, 2014, p. 133.

218 Esta propuesta formó parte de las palabras introductorias de Helen Durham, directora del Departamento de Derecho Internacional y Políticas Humanitarias del CICR, en la audiencia pública que tuvo lugar el 22 de enero de 2019 ante la Comisión Mundial sobre la estabilidad del ciberespacio (declaración en los registros del CICR).

219 Informe del CICR de 2019 sobre los desafíos de los conflictos armados contemporáneos, nota 36 *supra*, p. 35.

## Conclusión

Para proteger a la población civil y la infraestructura civil durante un conflicto armado, es de suma importancia reconocer que las ciberoperaciones realizadas durante los conflictos armados no ocurren en un vacío jurídico, sino que están reguladas por el derecho internacional, en especial, por el DIH. No obstante, como se ha mostrado en el este artículo, el debate no termina con el reconocimiento de la aplicabilidad del DIH. Es necesario continuar el debate –en especial, entre Estados– sobre cómo ha de interpretarse el DIH en el ámbito del ciberespacio. Cada uno de esos debates debe basarse en un conocimiento profundo del desarrollo de las capacidades militares cibernéticas, sus posibles costos humanos y la protección que confiere el derecho en vigor. Con este artículo, se pretende proporcionar una base para esos debates. Si bien el uso de ciberoperaciones durante un conflicto armado, sus posibles costos humanos y las posiciones jurídicas de los Estados respecto de esta cuestión cambian continuamente, el análisis realizado en este artículo ofrece algunas conclusiones.

En primer lugar, las ciberoperaciones que se realizan durante un conflicto armado son una realidad de los conflictos armados contemporáneos, y es probable que su uso aumente en el futuro. Las ciberoperaciones pueden causar daños considerables a la población civil, en especial, si afectan la infraestructura civil crítica, por ejemplo, los establecimientos sanitarios o las redes de electricidad, agua o saneamiento. Si bien, según las observaciones actuales, el riesgo de que causen daños humanos no parece demasiado alto, en particular, en comparación con la destrucción y el sufrimiento que siempre causan los conflictos, la evolución de las ciberoperaciones requiere que se preste la debida atención a las incertidumbres existentes y al ritmo acelerado del cambio.

En segundo lugar, en opinión del CICR no hay dudas de que las ciberoperaciones realizadas durante un conflicto armado están reguladas por el DIH, al igual que cualquier arma, medio o método de guerra, nuevo o convencional, utilizado por un beligerante en un conflicto. Si bien la cuestión (aún) no goza de consenso universal, un análisis minucioso de los distintos argumentos propuestos en los debates multilaterales muestra que reafirmar la aplicabilidad del DIH no legitima la militarización del ciberespacio ni el uso de ciberoperaciones maliciosas. Un Estado que piensa realizar una ciberoperación contra otro Estado debe analizar la licitud de esa operación en virtud de la Carta de la ONU y del DIH. Estos dos ordenamientos jurídicos son complementarios en lo referente a la protección de las personas contra la guerra y sus efectos. Si bien parte de la terminología que emplean ambos es similar, los regímenes son independientes desde el punto de vista jurídico y requieren análisis diferentes, pues la terminología similar tiene (a veces) significados distintos. Por ejemplo, concluir que una ciberoperación desencadena la aplicabilidad del DIH no necesariamente implica que dicha ciberoperación constituya un ataque armado, lo que habilita el derecho a la defensa propia.

En tercer lugar, la naturaleza parcialmente no física –es decir, digital– del ciberespacio y la interconexión de las redes militares y civiles plantean problemas

prácticos y jurídicos para la aplicación de los principios y las normas generales del DIH que protegen a los civiles y a los bienes de carácter civil, sobre todo, en los casos de la noción de "ataque" en el sentido del DIH, la cuestión de si los datos civiles tienen la misma protección que los "bienes de carácter civil" y la protección de la infraestructura cibernética de "uso dual".

La cuestión de si una operación constituye un "ataque" en el sentido del DIH o no es fundamental para la aplicación de varias de las normas que dimanan de los principios de distinción, proporcionalidad y precaución, que confieren una protección decisiva a los civiles y a los bienes de carácter civil. Desde hace muchos años, el CICR sostiene la posición de que una operación destinada a inutilizar una computadora o una red informática durante un conflicto armado constituye un ataque en el sentido del DIH, sea que el objeto quede inutilizado por destrucción o por cualquier otro medio. Esta opinión se refleja asimismo en la posición adoptada por algunos Estados.

Si bien muchas de las normas generales relativas a la conducción de las hostilidades se limitan a actos que se consideran ataques según el DIH, algunas de las normas de este ordenamiento jurídico que rigen la conducción de las hostilidades se aplican a un conjunto más amplio de operaciones. El DIH incluye algunas normas que se aplican a todas las "operaciones militares", por ejemplo, la obligación de tener cuidado constante de preservar a los civiles y a los bienes de carácter civil. Asimismo, el DIH define normas específicas que confieren protección a determinadas categorías de personas y bienes, por ejemplo, a los bienes indispensables para la supervivencia de la población civil, los servicios sanitarios y las operaciones de socorro humanitario. La protección que confieren esas normas trasciende la protección general que se brinda a los civiles y a los bienes de carácter civil.

La protección de los datos contra las operaciones cibernéticas maliciosas durante un conflicto armado está adquiriendo una importancia cada vez mayor, porque los datos son un componente esencial del dominio digital y un pilar de la vida en muchas sociedades. En opinión del CICR, la conclusión de que una ciberoperación ideada para eliminar o manipular datos civiles esenciales o de la que se prevé que los eliminará o manipulará no estaría prohibida por el DIH en el mundo de hoy, cada vez más dependiente de la esfera cibernética, parece difícil de conciliar con el objetivo y el propósito de este ordenamiento jurídico y genera una profunda inquietud.

Con el objeto de proteger la infraestructura civil crítica que depende del ciberespacio, es asimismo esencial proteger la infraestructura del propio ciberespacio. Históricamente, se ha considerado que un bien de carácter civil puede convertirse en un objetivo militar si su uso con fines militares es tal que satisface la definición de objetivo militar, incluso si se utiliza al mismo tiempo con fines civiles. No obstante, una parte en un conflicto que considere dirigir un ataque contra la infraestructura cibernética debe analizar qué partes concretas de esa infraestructura contribuyen efectivamente a la acción militar, y si su destrucción o neutralización ofrecería, en las circunstancias imperantes en ese momento, una ventaja militar

definida. Asimismo, esa parte debe tomar todas las precauciones factibles para impedir, o al menos reducir todo lo posible, los daños civiles incidentales, incluidos los daños por los efectos indirectos o secundarios, y debe abstenerse de realizar el ataque si cabe esperar que los daños sean excesivos.

En cuarto lugar, a la luz de los problemas particulares que plantean las características del ciberespacio para la interpretación y la aplicación de determinados principios del DIH en la conducción de las hostilidades, las partes en conflicto que deciden desarrollar, adquirir o adoptar armas, medios o métodos de guerra que incorporan tecnología cibernética han de hacerlo con cuidado. Si bien los exámenes jurídicos de las nuevas armas, medios y métodos de guerra son obligatorios para los Estados Partes en el PA I, también son fundamentales para que todos los Estados garanticen que sus fuerzas armadas solo utilizan armas, medios o métodos de guerra que permiten al Estado cumplir las obligaciones que le impone el DIH.

En conclusión, reconocer que el DIH se aplica en el ciberespacio y participar en debates sobre cómo permite abordar los diversos problemas que plantean las características específicas de la esfera cibernética y si el derecho en vigor es adecuado y suficiente no excluyen la utilidad o incluso la necesidad de nuevas normas. En nuestra opinión, la respuesta a este interrogante depende especialmente de cómo interpretan los Estados las obligaciones del DIH en vigor. Si se adoptan interpretaciones estrictas, pueden surgir vacíos importantes en el ámbito de la protección de las poblaciones civiles y la infraestructura civil, y podría ser necesario fortalecer el marco jurídico existente. Sin embargo, si se elaboran nuevas normas, en nuestra opinión, es fundamental que se tome como base y se fortalezca el marco jurídico existente, en particular, el DIH.