International Review of the Red Cross, N.° 910
Guerra y memoria

Guerra conectada 3.0: protección de la población civil durante las operaciones cibernéticas

Michael N. Schmitt*

El doctor Michael N. Schmitt es miembro del Comité Editorial de la *International Review of the Red Cross*. Es profesor de Derecho Internacional Público en la Universidad de Exeter y profesor Howard S. Levie del Colegio de Guerra Naval de EE. UU. Asimismo, es académico distinguido Francis Lieber de la Academia Militar de EE. UU. en West Point y editor general del *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

Resumen

En términos generales, el derecho internacional humanitario ha de proporcionar el marco jurídico para las operaciones cibernéticas durante un conflicto armado. Sin embargo, hay dos debates al respecto que no han concluido aún y cuya resolución determinará el nivel de protección exacto que ha de conferirse a la población civil durante las operaciones cibernéticas. El primero de esos debates gira en torno al significado del término "ataque" en distintas normas sobre la conducción de las hostilidades, mientras que el segundo pretende responder el interrogante de si la información puede considerarse un objeto de modo que las operaciones que la destruyan o la alteren estén sujetas a la prohibición de atacar bienes de carácter civil y sus consecuencias deban evaluarse al considerar los principios de proporcionalidad y precauciones en el ataque. Incluso si se llegaran a resolver esos debates, la población civil seguiría afrontando los riesgos inherentes a las capacidades particulares de las operaciones cibernéticas.

* Las opiniones vertidas en este artículo son exclusivas del autor. El autor agradece al teniente coronel Jeffrey Biller (Fuerza Aérea de EE. UU.) por sus valiosos comentarios.

En este artículo, se proponen dos políticas que las partes en conflicto deberían pensar en adoptar a fin de reducir esos riesgos. Ambas se basan en la premisa de que las operaciones militares deben reflejar un equilibrio entre las consideraciones militares y el interés de los Estados en imponerse en el conflicto.

Palabras clave: operaciones cibernéticas, ataques, datos, objetos civiles, proporcionalidad, precauciones en el ataque, necesidad militar

***

La negativa de Rusia, de China y de otros países durante las negociaciones del Grupo de Expertos Gubernamentales de la ONU sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional (GEG ONU) que tuvieron lugar entre 2016 y 2017 para que se reconociera expresamente la aplicabilidad del derecho internacional humanitario (DIH) a las operaciones cibernéticas fue un revés en los esfuerzos por esclarecer las obligaciones que impone a esas operaciones el derecho internacional[1]. La negativa fue llamativa en vista de que dos años antes, el GEG ONU previo, que estaba integrado por Rusia y China, había caracterizado "los principios de humanidad, necesidad, proporcionalidad y distinción" como "principios jurídicos internacionales establecidos"[2], aseveración que solo puede interpretarse como un acuerdo de que el DIH rige la conducción de las hostilidades cibernéticas durante los conflictos armados.

Desde el punto de vista jurídico, la negativa es desconcertante. Existe un amplio consenso en cuanto a la aplicabilidad del DIH a las operaciones cibernéticas durante un conflicto armado. Esa es la posición de países clave con capacidades cibernéticas, como Estados Unidos[3], organizaciones internacionales como la

1 Michael N. Schmitt y Liis Vihul, "International cyber law politicized: The UN GGE's failure to advance cyber norms", *Just Security*, 30 de junio de 2017, disponible en línea en www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

2 GEG ONU, Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, doc. ONU A/70/174, 22 de julio de 2015, párr. 28(d).

3 Brian J. Egan, asesor jurídico, Departamento de Estado de EE. UU. "Remarks on international law and stability in cyberspace", 10 de noviembre de 2016, disponible en línea en https://perma.cc/B6TH-232L. V. también "Applicability of international law to conflicts in cyberspace", *Digest of United States Practice in International Law*, 2014, cap. 18, sección A(3)(b), p. 737; Harold Koh, asesor jurídico, Departamento de Estado de EE. UU., "International law in cyberspace", comentarios en la Conferencia Jurídica Interinstitucional del Comando Cibernético de EE. UU. 18 de septiembre de 2012. Sobre las declaraciones de Koh, v. Michael N. Schmitt, "International law in cyberspace: The Koh speech and Tallinn Manual juxtaposed", *Harvard Journal of International Law Online*, vol. 54, 2012.

OTAN y la Unión Europea[4], el Comité Internacional de la Cruz Roja (CICR)[5] y la mayor parte de la comunidad académica[6]. El consenso se basa, en parte, en la práctica de los Estados, que reconoce desde hace mucho tiempo que los nuevos medios y métodos de la guerra están sujetos a las prohibiciones, las restricciones y los requisitos que se encuentran en las disposiciones sobre armas y las normas que rigen la conducción de las hostilidades en el DIH[7]. En su Opinión consultiva sobre las armas nucleares, por ejemplo, la Corte Internacional de Justicia confirmó la aplicabilidad del DIH a las nuevas armas[8]. Asimismo, el artículo 36 del Protocolo adicional I a los Convenios de Ginebra (PA I) dispone que cuando una parte, "estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, […] determinar[á] 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"[9]. Hasta los Estados que no son parte del PA I reconocen la necesidad de garantizar que las nuevas armas, incluidas las armas cibernéticas, cumplan los requisitos de las normas existentes del DIH[10]. Por último, la lógica indica que el DIH ha de aplicarse a las nuevas formas de conducción de las hostilidades, ya que casi todos los conflictos traen consigo armas, tácticas y formas operacionales nuevas. Sería absurdo afirmar que solo los medios y los métodos de guerra anteriores a la aprobación de un tratado o a la materialización de una norma de derecho consuetudinario están sujetos a los principios y las normas previstas en ellos[11].

Así pues, no se trata de si el DIH se aplica a las operaciones cibernéticas que se ejecutan durante un conflicto armado, sino de cómo se aplica. En la mayoría de los casos, la aplicación es directa. Lejos está de ser una epifanía jurisprudencial concluir, por ejemplo, que una operación cibernética letal, nociva o destructiva

4 Consejo del Atlántico Norte, Declaración de la Cumbre de Gales, 5 de septiembre de 2014, párr. 72, disponible en línea en www.nato.int/cps/ic/natohq/official_texts_112964.htm. V. también Comisión Europea, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 de febrero de 2013, p. 72.

5 CICR, "Cyberwarfare and international humanitarian law: The ICRC's position", junio de 2013, p. 2, disponible en línea en www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf.

6 V., p. ej., Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013, norma 20; Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Manual de Tallinn 2.0), norma 80.

7 William H. Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, pp. 340-341; CICR, *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos*, enero de 2006, pp. 3-4.

8 Corte Internacional de Justicia (CIJ), *Legalidad de la amenaza o el empleo de armas nucleares*, Opinión consultiva, 8 de julio de 1996, *ICJ Reports 1996*, párrs. 85-86.

9 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 (PA I), art. 36.

10 Oficina del Consejo General, Departamento de Defensa de EE. UU., *Law of War Manual*, ed. revisada, diciembre de 2016 (Manual de derecho de la guerra de EE. UU.), párr. 16.6; Fuerza Aérea de EE. UU., *Legal Review of Weapons and Cyber Capabilities*, AF Instruction 51-402, 27 de julio de 2011.

11 Para un excelente estudio integral sobre las cuestiones de DIH que plantean las operaciones cibernéticas, v. 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.

dirigida contra personas civiles no solo es violatoria del DIH[12], sino que también constituye un crimen de guerra en situación de conflicto tanto internacional como no internacional[13]. Del mismo modo, los ataques cibernéticos están claramente limitados por los principios de proporcionalidad[14] y de precauciones en el ataque[15].

No obstante, quedan numerosas cuestiones por resolver. En el centro de esta zona gris se desarrollan dos debates persistentes, cuya resolución tendrá consecuencias significativas para la población civil. Ambos se relacionan con criterios de definición. El primero tiene que ver con el alcance del término "ataque". Es una cuestión determinante respecto de las operaciones cibernéticas porque numerosas prohibiciones, restricciones y requisitos del DIH se aplican solo a las comprendidas dentro de la definición de ataque[16]. El segundo gira en torno al significado del término "objeto". Tiene relevancia para las operaciones cibernéticas porque plantea la cuestión de si una operación cibernética que destruye o altera datos civiles, pero no se manifiesta físicamente, constituye un ataque prohibido a un bien de carácter civil[17].

Me he ocupado de estos temas en dos artículos anteriores de la *International Review*: "La guerra de la información" y "Rewired Warfare"[18]. En el presente artículo, voy más allá del derecho propiamente dicho en busca de soluciones

12 PA I, art. 51(2); Jean-Marie Henckaerts y Louise Doswald-Beck (eds.), *El derecho internacional humanitario consuetudinario, Vol. 1: Normas*, CICR, Buenos Aires, 2007 (Estudio del CICR sobre derecho consuetudinario), norma 1; 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 (PA II), art. 4(i). V. también Manual de Tallinn 2.0, nota 6 *supra*, norma 94.

13 V., p. ej., Estatuto de Roma de la Corte Penal Internacional, 2187 UNTS 90, 17 de julio de 1998 (Estatuto de Roma), arts. 8(2)(b)(i), 8(2)(c)(i).

14 PA I, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 14; Manual de Tallinn 2.0, nota 6 *supra*, norma 113.

15 PA I, art. 57; Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, cap. 5; Manual de Tallinn 2.0, nota 6 *supra*, normas 114-120. V. también Eric Jensen, "Cyber attacks: Proportionality and precautions in attack", *International Law Studies*, vol. 89, 2012.

16 V., en general, PA I, título IV, sección I. Algunos académicos extenderían la aplicación de estas normas más allá de los ataques, a pesar del uso del término en las normas propiamente dichas. V., p. ej., Nils Melzer, *Cyberwarfare and International Law*, UNIDIR, artículo de recursos, 2011, p. 27, disponible en línea en https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (donde se sostiene que la aplicabilidad depende de si las operaciones cibernéticas constituyen "hostilidades"); Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, pp. 196-202 (sobre la referencia a las operaciones militares del art. 48 del PA I).

17 PA I, art. 52(1); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 7; Manual de Tallinn 2.0, nota 6 *supra*, norma 99.

18 Michael N. Schmitt, "La guerra de la información: los ataques por vía informática y el *jus in bello*", *International Review of the Red Cross*, vol. 84, n.º 846, 2002, disponible en línea en https://www.icrc.org/es/doc/resources/documents/misc/5tecg3.htm; Michael N. Schmitt, "Rewired Warfare: Rethinking the law of cyber attack", *International Review of the Red Cross*, vol. 96, n.º 893, 2014. V. también Knut Dörmann, "Applicability of the Additional Protocol to computer network attack", en Karin Bystrom (ed.), *Proceedings of the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004*, Escuela de Defensa Nacional de Suecia, 2005, disponible en línea en www.icrc.org/en/doc/resources/documents/misc/68lg92.htm. V. también 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.), *Proceedings of the 4th International Conference on Cyber Conflict*, OTAN Centro Cooperativo de Defensa Cibernética de Excelencia, 2012.

parciales a estos dilemas. Para ello, hago una breve revisión de esos debates. Así, en la primera sección de este artículo, hago un resumen de las distintas opiniones respecto de dónde se encuentra el umbral de un "ataque", y en la segunda, describo las discrepancias actuales acerca de si los datos son objetos. No es mi intención discutir aquí las distintas posiciones; por el contrario, reseño los debates en torno a esas dos cuestiones simplemente para ilustrar que el derecho no da respuestas al respecto, con lo que o bien pone a los civiles en riesgo, o bien no aborda las operaciones cibernéticas que, en la actualidad, son legítimas, pero podrían resultar altamente perjudiciales para la población civil.

Dado que es improbable que la situación se resuelva en el corto plazo en el ámbito jurídico, en la tercera sección de este artículo, propongo dos políticas que podrían contribuir a corregir las deficiencias en materia de protección civil respecto de las operaciones cibernéticas. Esas políticas serían aplicadas por el Estado que ejecuta una operación cibernética cuando llega a la conclusión de que la operación no se considera un ataque o no está sujeta a la prohibición de atacar bienes de carácter civil, porque el objetivo son datos y, desde el punto de vista del Estado, los datos no son objetos. Si bien las políticas propuestas tienen la finalidad de mejorar la protección de la población civil, están supeditadas a la necesidad de que los Estados ejecuten sus operaciones de guerra de manera eficaz. Por lo tanto, las propuestas están pensadas para reflejar el equilibrio entre las consideraciones humanitarias y la necesidad militar que da sustento al DIH y a otras normas aplicables a la guerra[19].

Es necesario tener en cuenta que no afirmo que las dos propuestas representen la *lex lata*; no es así en mi opinión, si bien entiendo que haya quienes no estén de acuerdo conmigo. Propongo, en cambio, una red de seguridad humanitaria basada en políticas y realista desde el punto de vista militar que los Estados pueden adoptar en situaciones en las que llegan a la conclusión de que una determinada operación durante un conflicto armado queda fuera de los preceptos del DIH. Con el tiempo, las cuestiones jurídicas que se describen a continuación pueden resolverse, fortaleciendo así la influencia del DIH en las operaciones cibernéticas. Pero mientras tanto, la comunidad internacional necesita una solución práctica que se centre en esas zonas grises del derecho respecto de los objetivos de los ataques cibernéticos.

Primera cuestión: el significado de "ataque"

Tal como se ha mencionado, las prohibiciones, las restricciones y los requisitos fundamentales del DIH previstos en el derecho convencional y en el derecho consuetudinario, o en ambos, están formulados en términos de "ataques"[20]. Por ejemplo, está prohibido atacar directamente a personas o bienes

19 Jean Pictet, *Development and Principles of International Humanitarian Law*, Martinus Nijhoff, Dordrecht y Boston, Massachusetts, 1985, pp. 61-63. Sobre mi formulación de este equilibrio, v. Michael N. Schmitt, "Military necessity and humanity in international humanitarian law: Preserving the delicate balance", *Virginia Journal of International Law*, vol. 50, n.º 4, 2010.

20 Los ataques, en el contexto del DIH, no deben confundirse con el término "ataque armado" del *jus ad bellum* que figura en el art. 51 de la Carta de la ONU. El análisis que se expone en este artículo se limita a los primeros.

civiles[21], realizar ataques indiscriminados[22] o recurrir a la perfidia en el ataque[23]; o atacar, con algunas excepciones y matices, a personas o bienes específicos que gozan de protección especial (por ejemplo, establecimientos sanitarios[24], bienes indispensables para la supervivencia de la población civil[25], el medio ambiente[26], las obras o instalaciones que contienen fuerzas peligrosas, a saber, las presas, los diques y las centrales nucleares[27], las localidades no defendidas[28], y a los combatientes que están fuera de combate[29]). Los ataques están sujetos al principio de proporcionalidad, que prohíbe "los ataques, cuando sea de prever que causarán incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista"[30]. Asimismo, la parte en conflicto que prepara un ataque debe hacer todo lo que sea factible para reducir todo lo posible el daño a la población civil[31].

La interpretación y el carácter consuetudinario de algunas de esas normas, en especial, con respecto a las operaciones cibernéticas, son objeto de controversia. La cuestión, sin embargo, es si su aplicación en el contexto cibernético depende del alcance del término "ataque"[32]. Si una operación cibernética no se considera un ataque, las normas no son aplicables, aunque todas las otras normas del DIH prohíban o restrinjan la operación cibernética[33].

El artículo 49(1) del PA I entiende por ataques los "actos de violencia contra el adversario, sean ofensivos o defensivos". Está ampliamente aceptado que un acto de violencia contra personas civiles o bienes de carácter civil también constituye un ataque[34]. Tomando esta definición, los expertos que elaboraron el *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Manual de Tallinn 2.0) llegaron a la conclusión de que un ataque cibernético incluye toda

21 PA I, arts. 51(2), 52(1). Sobre su carácter consuetudinario, v. Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, normas 1, 7.

22 PA I, art. 51(4); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 11.

23 PA I, art. 37(1); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 65. Sobre el empleo del término respecto del uso inapropiado de los emblemas nacionales del enemigo, v. PA I, art. 39(2); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 62.

24 PA I, nota 9 *supra*, art. 12(1); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 28. Sobre el empleo del término con respecto a atacar aeronaves sanitarias, v. PA I, arts. 27(2), 31(2).

25 PA I, art. 54(2); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 54.

26 PA I, art. 55(2). El carácter consuetudinario de esta norma no está claro.

27 PA I, art. 56(1). El carácter consuetudinario de esta norma no está claro.

28 PA I, art. 59(1); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 37.

29 PA I, art. 41(1); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, norma 47. Sobre la prohibición de atacar personas que se lancen en paracaídas de una aeronave en peligro, v. PA I, art. 42.

30 PA I, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b); Estudio del CICR sobre derecho consuetudinario, nota 12 *supra*, normas 14, 19.

31 PA I, art. 57; Estudio del CICR sobre derecho consuetudinario nota 12 *supra*, norma 15.

32 Para un excelente resumen de la cuestión de los ataques cibernéticos, v. William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012.

33 V., p. ej., Manual del derecho de la guerra de EE. UU., nota 10 *supra*, párr. 16.5.2.

34 Nils Melzer, *Guía para interpretar la noción de participación directa en las hostilidades según el derecho internacional humanitario,* CICR, Ginebra, 2010 (Guía del CICR para interpretar la noción de participación directa), p. 49.

"operación cibernética, sea ofensiva o defensiva, de la que cabe esperar que cause lesiones o la muerte de personas, o daño o destrucción de bienes"[35]. Esto es así independientemente de si el daño se causa al objetivo del ataque o si es colateral[36]. Parecería no haber motivos de peso para oponerse a que las operaciones cibernéticas que tienen ese tipo de consecuencias fueran catalogadas como ataques.

Lo que se suele pasar por alto es que los expertos no restringen el concepto de "ataque cibernético" a las operaciones que causan destrucción o daño físico. La mayoría de ellos coincide en que "una interferencia en la funcionalidad se considera daño si restablecerla requiere la sustitución de componentes físicos"[37]. Por lo tanto, una operación cibernética que implique la pérdida de funcionalidad de la infraestructura constituiría un ciberataque.

En ese punto, deja de haber consenso entre los expertos, que adoptan distintas posiciones respecto del significado de la frase "pérdida de funcionalidad". Mientras que algunos limitan la pérdida de funcionalidad a las situaciones en las que es necesario reparar o reemplazar componentes físicos de la infraestructura cibernética objetivo, otros piensan que habría que ampliar la noción a aquellas situaciones en las que, para recuperar la funcionalidad, se debe volver a instalar el sistema operativo o los datos particulares requeridos por el sistema para ejecutar sus funciones. Algunos hasta llegan a argumentar que es irrelevante la forma en que sucede la pérdida de funcionalidad, pues el mero hecho de que el sistema no funcione como se espera ya es suficiente[38].

Otra zona gris del derecho tiene que ver con las operaciones cibernéticas que, si bien no causan daños de ese tipo, tienen consecuencias adversas para la población civil, como "la interrupción de la comunicación por correo electrónico en todo el territorio nacional"[39]. La mayoría de los expertos del Manual de Tallin 2.0, a pesar de reconocer en qué medida las operaciones cibernéticas de este tipo podrían alterar la vida civil, es de la opinión de que no hay una base jurídica para considerar que esas operaciones constituyen ataques[40]. Todos los expertos coinciden en que las operaciones cibernéticas que solo causan inconveniencia o molestia no alcanzan el nivel de un ciberataque[41].

El CICR trató esta cuestión en sus informes sobre *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos* de 2011 y 2015

35 Manual de Tallinn 2.0, nota 6 *supra*, norma 92.
36 Ibíd., p. 419.
37 Ibíd., p. 417. V. también C. Droege, nota 11 *supra*, pp. 560-561.
38 Manual de Tallinn 2.0, nota 6 *supra*, pp. 417-418. Sobre la pérdida de funcionalidad, v. W. Boothby, nota 32 *supra*, pp. 386-387.
39 Manual de Tallinn 2.0, nota 6 *supra*, p. 418.
40 Ibíd.
41 Ibíd. V. también CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, Ginebra, octubre de 2015 (Informe sobre los desafíos de los conflictos armados contemporáneos de 2015), pp. 54-55, disponible en línea en https://www.icrc.org/es/document/el-derecho-internacional-humanitario-y-los-desafios-de-los-conflictos-armados.

(Informe sobre los desafíos de los conflictos armados contemporáneos)[42]. En el informe de 2015, la Institución observó que "la forma en que se define un 'ataque' cibernético conforme a las normas que rigen la conducción de hostilidades […] tendrá una fuerte influencia en la protección que el DIH otorga a la infraestructura civil esencial"[43]. Luego señaló la cuestión decisiva del punto en el que la pérdida de funcionalidad convierte una operación cibernética en un ataque. El CICR llegó a la conclusión de que, en particular, "una operación diseñada para inhabilitar un objeto, por ejemplo, un ordenador o una red de ordenadores, constituye un ataque conforme a las normas sobre la conducción de hostilidades, sea o no que el objeto quede desactivado por medios cinéticos o cibernéticos"[44]. En el Informe sobre los desafíos de los conflictos armados contemporáneos de 2015, se señala, correctamente, que:

> Un entendimiento excesivamente restrictivo de la noción de ataque sería difícil de reconciliar con el objeto y la finalidad de las normas sobre la conducción de hostilidades, que consisten en garantizar la protección de la población civil y de los bienes de carácter civil contra los efectos de las hostilidades[45].

Con perspicacia, el CICR utilizó el informe para llamar la atención sobre la ambigüedad de los conceptos relacionados con la caracterización de un acto como un ataque. Por ejemplo, con respecto a la exclusión de las operaciones cibernéticas que solo causan inconveniencia, el CICR señaló que "lo que abarca la 'inconveniencia' no está definido, y esta terminología no se utiliza en el ámbito del DIH"[46]. Pero al igual que los expertos del Manual de Tallinn 2.0, el CICR reconoce que, en cierta medida, lo que ha de tenerse en cuenta al considerar una operación cibernética como un ataque es la naturaleza de sus consecuencias, y no necesariamente su gravedad. En particular, en el Informe sobre los desafíos de los conflictos armados contemporáneos de 2015, se excluyó el espionaje en sí de la categoría de ataque y se observó que "la interferencia de las transmisiones de radio o televisión no se ha considerado tradicionalmente un ataque en el sentido del DIH"[47].

De acuerdo con esos enfoques establecidos, es posible caracterizar definitivamente a las operaciones cibernéticas nocivas o destructivas como ataques y excluir a aquellas que se ubican en el extremo inferior de la escala por sus efectos. Aun así, es probable que la mayoría de las operaciones cibernéticas no cause destrucción ni daño físico, y muchas no afectarán la funcionalidad de

42 CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, Ginebra, octubre de 2011, p. 42, disponible en línea 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; Informe sobre los desafíos de los conflictos armados contemporáneos de 2015, nota 41 *supra*, pp. 54-55.

43 Informe sobre los desafíos de los conflictos armados contemporáneos de 2015, nota 41 *supra*, p. 54.

44 Ibíd.

45 Ibíd.

46 Ibíd., p. 55.

47 Ibíd., pp. 54-55.

la infraestructura cibernética atacada de modo tal que se pueda considerar que alcanzan el umbral establecido para la pérdida de funcionalidad.

Esto es doblemente problemático. Por un lado, muchas operaciones cibernéticas que podrían dirigirse contra la infraestructura civil o tener de alguna manera consecuencias adversas graves para la población civil podrían no considerarse ciberataques y, en consecuencia, quedarían fuera del alcance de las normas del DIH relativas a los ataques. En segundo lugar, la incertidumbre respecto del umbral para la pérdida de funcionalidad coloca en el terreno de la ambigüedad la caracterización jurídica de algunas operaciones cibernéticas dirigidas contra la población civil o que afectan a la población civil. Una parte en conflicto podría aprovechar esa incertidumbre para evitar la condena generalizada de las operaciones cibernéticas dirigidas contra la infraestructura cibernética civil o que, de alguna manera, afectan la infraestructura cibernética civil por ilícitas. Desde una perspectiva humanitaria, esa situación es indefendible.

Segunda cuestión: los datos como objetos

Un segundo dilema que implica un riesgo considerable para la población civil está asociado con la cuestión de si la noción de "objeto" se aplica a los datos, de modo que los datos civiles gozarían de la protección que confiere la prohibición de atacar bienes de carácter civil[48]. Esta cuestión es independiente de la definición de ataque, porque si los datos son objetos, su eliminación o alteración claramente constituiría el daño necesario para que la operación cibernética fuera considerada un ataque. Y si los datos no son objetos, no corresponde prohibir el ataque[49].

En el debate predominan dos opiniones. La mayoría de los expertos del Manual de Tallinn 2.0 concuerda con que el término "objeto" no debe interpretarse de modo tal de abarcar los datos[50]. Sus conclusiones se basan en el hecho de que los datos no están comprendidos en el "significado corriente"[51] del término "objeto",

48 Es necesario tener en cuenta que el debate no se extiende a las operaciones cibernéticas dirigidas contra datos cuando esa operación tiene efectos nocivos o destructivos en cadena. Por ejemplo, una operación cibernética en la que se eliminan o se manipulan los datos de un sistema de control de tráfico aéreo y así pone en riesgo la seguridad de una aeronave. Está ampliamente aceptado que una operación semejante constituye un ataque. La cuestión de los datos solo es relevante en situaciones en las que una operación cibernética dirigida contra datos no tiene probabilidad de tener consecuencias que, de por sí, la harían equivalente a un ataque.

49 Las operaciones dirigidas contra determinados datos están prohibidas en otras normas del DIH. V., p. ej., Manual de Tallinn 2.0, nota 6 *supra*, norma 132 y su interpretación de la p. 515 (datos médicos), y norma 142 y su interpretación de las pp. 535-536 (algunos expertos extienden la protección a la propiedad cultural en forma de datos).

50 Ibíd., p. 437.

51 Convención de Viena sobre el derecho de los tratados, 1155 UNTS 331, 23 de mayo de 1969 (en vigor a partir del 27 de enero de 1980), art. 31(1).

pues son intangibles, y tampoco "quedan alcanzados por la explicación que se proporciona en el comentario de 1987 del CICR a los Protocolos adicionales"[52].

Los otros expertos replican que adoptar ese enfoque:

> implicaría que incluso la eliminación de conjuntos de datos esenciales como los de la seguridad social, las declaraciones impositivas y las cuentas bancarias podría no quedar alcanzada por el marco regulatorio del derecho de los conflictos armados, con lo que no se respetaría el principio de protección general de la población civil contra los efectos de las hostilidades.

Los expertos se centran en el objeto y el propósito de la prohibición de atacar bienes de carácter civil y llegan a la conclusión de que el factor fundamental es la "gravedad de las consecuencias de la operación, y no la naturaleza del daño". Para ellos, "los datos civiles que son 'esenciales' para el bienestar de la población civil están comprendidos en la noción de bienes de carácter civil y, como tales, gozan de protección"[53].

En el Informe sobre los desafíos de los conflictos armados contemporáneos de 2015, el CICR hizo una observación similar. Al señalar que "[l]a eliminación o alteración de [ciertos] datos podría paralizar rápidamente los servicios y los negocios privados y causar más daños a los civiles que la destrucción de objetos físicos"[54], la Institución opinó:

> La conclusión de que este tipo de operación no estaría prohibido por el DIH en el mundo de hoy, cada vez más dependiente de la esfera cibernética –sea porque eliminar o alterar esos datos no constituiría un ataque en el sentido del DIH o porque esos datos no se considerarían objetos respecto de los cuales se aplicaría la prohibición de ataques contra bienes de carácter civil– parece difícil de conciliar con el objetivo y el propósito de este ordenamiento jurídico[55].

En principio, coincido con esta apreciación.

Varios otros enfoques se han propuesto para tratar esta cuestión. Uno de ellos distingue entre datos operacionales y de contenido[56]. Los primeros son datos de los que depende el funcionamiento de la infraestructura cibernética, y

52 Yves Sandoz, Christophe Swinarski y Bruno Zimmerman (eds.), *Commentary on the Additional Protocols*, CICR, Ginebra, 1987 (Comentario del CICR de los PA), párrs. 2007-2008: "La versión inglesa emplea el término 'objects', que significa 'algo situado ante los ojos o presentado ante la vista u otro sentido, una cosa individual que se ve o se percibe o que puede ser vista o percibida; una cosa material'. […] La versión francesa […] emplea el término 'biens', que significa 'cosa tangible, susceptible de apropiación'. Queda claro que, tanto en inglés como en francés, la palabra se refiere a algo que es visible y tangible." Es necesario reconocer que el contexto de la explicación no se aplica directamente, pero, de todos modos, los expertos del Manual de Tallinn la consideraron útil en sus deliberaciones.

53 Manual de Tallinn 2.0, nota 6 *supra*, pp. 437.

54 Informe sobre los desafíos de los conflictos armados contemporáneos de 2015, nota 41 *supra*, p. 56.

55 Ibíd.

56 Heather A. 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.

los segundos simplemente representan información en forma de datos, como los datos de texto que conforman este artículo. Al ocuparse solo de los datos de nivel operacional, este enfoque rechaza el criterio de tangibilidad y, en cambio, se centra en si los datos pueden considerar un objetivo militar[57]. Así, implícitamente adopta una visión inflexible de los datos de nivel operacional como objetos. Uno de los autores que defiende esta postura propone utilizar "medios de interpretación textual, sistemática y teleológica de la definición de objetivos militares que se encuentra en el derecho convencional y en el derecho consuetudinario"[58]. El autor concluye:

> Tanto la vida civil como las operaciones militares dependen cada vez más de información y actividades limitadas al ciberespacio, que tienen pocas ramificaciones, o ninguna, en el mundo físico. Para seguir siendo relevante, el derecho de los conflictos armados debe reflejar este cambio. Es por eso que se considera que […] los datos informáticos son objetos en el sentido del derecho internacional humanitario[59].

Ninguno de los planteos mencionados es totalmente satisfactorio. El enfoque restrictivo que adopta la mayoría de los expertos del Manual de Tallinn 2.0 no es lo suficientemente inclusivo en la práctica, pues deja los datos expuestos a la destrucción o la alteración que podrían tener consecuencias sumamente graves para la población civil, aunque no fueran nocivas ni destructivas. Quienes critican esta postura sostienen que esto sería contrario al objetivo y el propósito del DIH.

Por el contrario, el argumento de que los datos *per se* se consideran objetos (más allá de cómo se lo formule) es demasiado inclusivo. Hace muchos años que los militares ejecutan operaciones vinculadas con la información contra la población enemiga, por ejemplo, para entorpecer el apoyo al gobierno o sus políticas[60]. Esto es especialmente tentador en contextos de contrainsurgencia[61]. Con el advenimiento de las capacidades cibernéticas, esas operaciones se han empezado a realizar con medios cibernéticos[62]. Las operaciones psicológicas cibernéticas, por

57 Ibíd., pp. 41-49.

58 Kubo Mačák, "Military objectives 2.0: The case for interpreting computer data as objects under international humanitarian law", *Israel Law Review*, vol. 58, n.º 1, 2015, p. 55. Mi respuesta a los dos enfoques figura en "The notion of 'objects' during cyber operations: A riposte in defence of interpretive precision", *Israel Law Review*, vol. 48, n.º 1, 2015.

59 K. Mačák, nota 58 *supra*, p. 80.

60 V., en general, p. ej., Estado Mayor Conjunto de EE. UU., *Information Operations*, Publicación conjunta 3-13, con modificaciones incorporadas el 20 de noviembre de 2014.

61 V., p. ej., Ejército de EE. UU., *Counterinsurgency*, Manual de campo 3-24, diciembre de 2006, párrs. 5-19 - 5-34.

62 El ejército de EE. UU. evalúa minuciosamente el uso de esas capacidades. V., p. ej., Liston Wells II, "Cognitive-emotional conflict: Adversary will and social resilience", *Prism*, vol. 7, n.º 2, 2017. *Prism* es una publicación de la Universidad Nacional de Defensa de EE. UU. La atención que se presta a esas operaciones queda clara en el establecimiento del Colegio de Información y Ciberespacio de la Universidad Nacional de Defensa (sitio de internet disponible en http://cic.ndu.edu/).

ejemplo, pueden consistir en la destrucción o la alteración de datos, así como en la interrupción de actividades civiles asociadas con medios de comunicación.

El planteo que hace eje en la gravedad de la operación, promovido por una minoría durante el proceso de redacción del Manual de Tallinn 2.0, así como por el CICR, es el más atractivo a nivel intuitivo. Lamentablemente, en su defensa no se ha proporcionado más justificación que el argumento bastante generalizado del cumplimiento del objetivo y el propósito del DIH. Tampoco se ha presentado una orientación detallada para su implementación. Más aún, este planteo pasa por alto el hecho de que la cuestión relevante aquí es la definición. Así, se plantea el interrogante de la lógica normativa de la caracterización de determinados datos como objetos sobre la base de la gravedad de las consecuencias, pero no de otros datos cuando las consecuencias del daño o la alteración son menos graves. Podría ser útil trazar una línea jurídica transaccional sobre la base de las consecuencias generadas, como se hace con la norma de proporcionalidad, pero el mismo razonamiento no se aplica cuando simplemente se define un término.

El debate no se resolverá en el futuro inmediato, pues adoptar un enfoque por el cual los datos son o no son objetos conduce a resultados insatisfactorios y poco prácticos. Y si bien tener en cuenta la gravedad de las consecuencias para la población civil parece reflejar los objetivos fundacionales del DIH, la falta de una base jurídica clara para adoptar esta posición hace que esta sea materia de *lex ferenda* y no de *lex lata*.

¿Qué se debe hacer?

¿Qué ha de hacerse ante esta situación problemática? Desde mi punto de vista, la respuesta reside en prestar atención al espíritu del DIH –ya que la letra no es suficiente– para decidir qué políticas se adoptarán. Por ello, ofrezco dos recomendaciones de políticas basadas en ese espíritu, que se centran en la gravedad de las consecuencias para la población civil y no en el tipo del daño resultante (daño físico).

El espíritu del DIH está en el delicado equilibrio entre los intereses de los Estados por conducir las operaciones militares con eficacia y el sufrimiento que causan esas operaciones tanto en los combatientes como en la población civil. Este equilibrio ha sido reconocido en numerosas ocasiones en la orientación brindada a los Estados y en tratados clave del DIH. Por ejemplo, el Código Lieber de 1863, que daba instrucciones para el Ejército de la Unión durante la Guerra de Secesión de Estados Unidos, establecía:

> La necesidad militar no admite la crueldad, es decir, causar sufrimiento ni por el mero hecho de causarlo, ni por revancha, ni causar mutilaciones o lesiones, salvo durante el combate, ni torturar para obtener confesiones. Tampoco admite el uso de venenos de ninguna naturaleza ni la devastación gratuita de un distrito. Admite el engaño, pero renuncia a la perfidia y, en general, la necesidad

militar no incluye ningún acto de hostilidad que dificulte innecesariamente la restitución de la paz[63].

Cinco años después, la Declaración de San Petersburgo también subrayaba la necesidad de "fij[ar] […] los límites técnicos en que deben detenerse las necesidades de la guerra ante las exigencias de la humanidad"[64]. La necesidad de equilibrio también inspiró a la Conferencia de Paz de La Haya de 1907, como se evidencia en la Convención de La Haya (IV), donde se observa que el instrumento, cuyo carácter consuetudinario es reconocido desde entonces[65], "ha sido inspirado por el deseo de disminuir los males de la guerra, en cuanto lo permitan las necesidades militares"[66]. Asimismo, la Convención presentaba la Cláusula de Martens, que reapareció siete décadas después en el PA I:

> Mientras que se forma un Código más completo de las leyes de la guerra las Altas Partes Contratantes juzgan oportuno declarar que en los casos no comprendidos en las disposiciones reglamentarias adoptadas por ellas las poblaciones y los beligerantes permanecen bajo la garantía y el régimen de los principios del Derecho de Gentes preconizados por los usos establecidos entre las naciones civilizadas, por las leyes de la humanidad y por las exigencias de la conciencia pública[67].

Esas declaraciones y disposiciones ilustran la observación de la Corte Internacional de Justicia (CIJ) en *Corfu Channel*, su primer caso, de que el derecho internacional está animado por "consideraciones elementales de humanidad"[68].

Las operaciones cibernéticas cambian las reglas del juego respecto del anhelado equilibrio en el que ha de sustentarse el DIH. El derecho internacional humanitario se creó en el contexto de los medios y los métodos de la guerra, cuyos efectos eran dañar, destruir, lesionar o matar. Si bien la población civil pudo

63 Departamento de Guerra de EE. UU., *Instructions for the Government of Armies of the United States in the Field*, orden general n.º 100, 24 de abril de 1863 (Código Lieber), art. 16.

64 Declaración de San Petersburgo de 1868 con el objeto de prohibir el uso de determinados proyectiles en tiempo de guerra, *Martens Nouveau Recueil*, serie 1, vol. 18, 29 de noviembre de 1868, preámbulo.

65 CIJ, *Consecuencias jurídicas de la construcción de un muro en el territorio palestino ocupado*, Opinión consultiva, 9 de julio de 2004, *ICJ Reports 2004*, p. 172; CIJ, Opinión consultiva sobre las armas nucleares, nota 8 *supra*, p. 257. El Tribunal de Núremberg también consideró que las normas previstas en la Convención de La Haya IV reflejan el derecho consuetudinario: V. *Trial of the Major War Criminals before the International Military Tribunal*, vol. 1, 1947, p. 254.

66 Convención (IV) relativa a las leyes y costumbres de la guerra terrestre, 36 Stat. 2277, 207 Consol. T.S. 277, 18 de octubre de 1907 (Convención de La Haya IV), preámbulo. V. también Convención (II) relativa a las leyes y costumbres de la guerra terrestre, 32 Stat. 1803, *Martens Nouveau Recueil*, serie 2, vol. 26, 29 de julio de 1899, preámbulo. El Reglamento de La Haya de 1907, en el art. 22 del anexo a ambos tratados, también estipula que "[e]l derecho de los beligerantes de adoptar medios de causar daño al enemigo no es ilimitado". Para la expresión moderna de este principio, v. PA I, art 35(1) (que añade la referencia a los "métodos" de la guerra).

67 Convención de La Haya IV, preámbulo; PA I, art. 1(2). La disposición ha sido citada en CIJ, *Nuclear Weapons*, nota 8 *supra*, p. 257.

68 CIJ, *Corfu Channel (United Kingdom v. Albania)*, 9 de abril de 1949, *ICJ Reports 1949*, p. 22.

haber sufrido como consecuencia de operaciones militares que no tuvieron esas consecuencias, la amenaza de daño provenía, en la gran mayoría de los casos, de esos efectos. Por eso, las normas del DIH se fundamentan en la necesidad de proteger a las personas civiles y los bienes de carácter civil contra esos efectos, al menos en la medida de lo posible, sin privar a los Estados de su capacidad de conducir operaciones militares esenciales[69].

A diferencia de los medios y los métodos cinéticos de la guerra, las operaciones cibernéticas pueden alterar profundamente la vida civil sin necesidad de incumplir las normas basadas en los efectos físicos. Por eso, debido a que la gran mayoría de esas operaciones no son dañinas ni nocivas, no encajan del todo en la arquitectura normativa existente destinada a proteger a la población civil. Esta dificultad no puede resolverse simplemente considerando que los datos civiles constituyen un bien de carácter civil protegido, pues hacerlo sería, como mínimo, controvertido desde el punto de vista jurídico, como ya se ha explicado, y es muy probable que resulte inaceptable para muchos Estados.

El primer paso para remediar la situación es reconocer que, como se ha señalado anteriormente, por lo general, la comunidad internacional acepta el principio de que el sufrimiento que inflige la guerra en la población civil debe reducirse al mínimo, en la medida de lo posible y dentro de las circunstancias. No hay motivos para limitar la aplicación de este principio humanitario en el terreno del derecho vinculante. Por el contrario, la mayoría de las normas del DIH se han adoptado en forma de tratados o se han consagrado en el derecho consuetudinario solo después de que la comunidad internacional considerara los actos a los que se aplican inaceptables o inapropiados dentro de las circunstancias. Las políticas y las perspectivas humanitarias fueron incorporadas al derecho con el tiempo.

En consecuencia, propongo que los Estados adopten dos normas de políticas humanitarias para resolver las lagunas y la incertidumbre descritas anteriormente. Algunos Estados pueden opinar que los elementos de esas normas ya reflejan el DIH. No obstante, a falta de consenso, es necesario que adopten la forma de mandatos de políticas.

69 Este paradigma cognitivo del daño físico se manifiesta, por ejemplo, en el principio general de que la "población civil y las personas civiles gozarán de protección general contra los *peligros* procedentes de operaciones militares" (PA I, art. 51(1), cursiva añadida); la referencia a la *violencia* en la definición de ataque (art. 49(1), cursiva añadida); la limitación en la aplicación del principio de proporcionalidad y algunas precauciones en el ataque, cuando sea de prever que "causarán incidentalmente *muertos y heridos entre la población civil, o daños* a bienes de carácter civil" (arts. 51 (5)(b), 57(2)(a)(ii), 51(2)(a)(iii), 51(2)(b), cursiva añadida); y la prohibición de "los actos o amenazas de *violencia* cuya finalidad principal sea aterrorizar a la población civil" (art. 51(2), cursiva añadida). De hecho, al esclarecer el principio de distinción, que requiere que las partes en conflicto "[hagan] distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirij[an] sus operaciones únicamente contra objetivos militares (art. 48), en el Comentario del CICR de los Protocolos adicionales se define a las operaciones militares como aquellas "durante las cuales se emplea la *violencia*" (Comentario del CICR sobre los PA, nota 52 *supra*, párr. 1875, cursiva añadida).

Primera política: funciones civiles esenciales

La primera propuesta consiste en *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 ellas*. He planteado esa idea en un artículo de 2014[70], en el que proponía que, con el paso del tiempo, los Estados podrían "simplemente comenzar a considerar que las operaciones dirigidas contra datos y servicios civiles esenciales son ataques, absteniéndose de ejecutarlas y condenando a quienes las ejecutan, con lo que generarían la práctica de los Estados sobre la que podría desarrollarse [en parte] la evolución del significado"[71]. Esa propuesta era errónea en el sentido de que confundía la adaptación del significado de un término –"ataque"– con lo que efectivamente es una protección especial. Por ende, reformulo aquí la idea en forma de una protección especial basada en políticas que han de adoptar los Estados que aún no la consideran un requisito jurídico[72].

Es necesario observar que la propuesta tiene la finalidad de salvaguardar funciones y servicios, y no categorías específicas de datos o infraestructuras cibernéticas civiles (es decir que no se pueden considerar objetivos militares). Esto es así para evitar discrepancias acerca de si una infraestructura o un conjunto de datos en particular quedan comprendidos dentro de la categoría protegida. Al centrarse en las funciones o los servicios, la protección se extiende a todas las infraestructuras o datos que puedan perjudicarlos, independientemente de la naturaleza o la categoría de las infraestructuras o los datos en cuestión. Esta formulación tiene antecedentes en el DIH; por ejemplo, en la prohibición de interferir por medios cibernéticos en las funciones sanitarias[73] o, en algunas

70 Michael N. Schmitt, "The law of cyber warfare: Quo vadis?", *Stanford Law and Policy Review*, vol. 25, n.º 2, 2014.

71 Ibíd., p. 296.

72 Para una propuesta anterior en este mismo sentido, v. Adam Segal, "Cyber space governance: The next step", Council on Foreign Relations, memorando de innovación de políticas n.º 2, 14 de noviembre de 2011, p. 3, disponible en línea en www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397. Muchos autores se han mostrado escépticos con respecto a las posibilidades de esta propuesta: v. C. Droege, nota 11 *supra*, p. 577; Robin Geiss y Henning Lahmann, "Cyber warfare: Applying the principle of distinction in an interconnected space", *Israel Law Review*, vol. 45, n.º 3, 2012, p. 394. No soy tan pesimista como estos autores en cuanto a las expectativas relativas a los Estados que suscriban declaraciones o adopten políticas sobre los así llamados "refugios digitales seguros", pero pienso que la propuesta, que abarca cuestiones tanto de *jus ad bellum* como de *jus in bello*, requiere una mayor minuciosidad jurídica.

73 Manual de Tallinn 2.0, nota 6 *supra*, norma 131 (la obligación de "respetar" se "incumple por actos que impiden o previenen que el personal sanitario o religioso, el personal, las unidades o los transportes sanitarios desempeñen sus funciones sanitarias o religiosas"; ibíd., p. 514). Para las obligaciones en general, v. I Convenio de Ginebra del 12 de agosto de 1949 para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña (CG I), 75 UNTS 31 (en vigor a partir del 21 de octubre de 1950), arts. 19, 24, 25, 35-36; II Convenio de Ginebra 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 (CG II), 75 UNTS 85 (en vigor a partir del 21 de octubre de 1950), arts. 22, 24, 25, 27, 36-39; III Convenio de Ginebra del 12 de agosto de 1949 relativo al trato debido a los prisioneros de guerra (CG III), 75 UNTS 135 (en vigor a partir del 21 de octubre 1950), art. 33; IV Convenio de Ginebra del 12 de agosto de 1949 relativo a la protección debida a las personas civiles en tiempo de guerra (CG IV), 75 UNTS 287 (en vigor a partir del 21 de octubre de 1950), arts. 18-22; PA I, arts. 12, 15, 21-24, 26; PA II, art. 9.

circunstancias, en la prestación de asistencia humanitaria[74]. Mi propuesta sigue esta línea, aunque desde el punto de vista de las políticas.

En el Informe sobre los desafíos de los conflictos armados contemporáneos de 2015, el CICR destacaba, de modo similar, la necesidad de proteger la infraestructura civil y los datos civiles esenciales, en particular, a la luz de la incertidumbre que se observa en el derecho[75]. En el Informe se señala:

> Con respecto a los datos pertenecientes a determinadas categorías de objetos que gozan de protección específica conforme al DIH, las normas de protección son amplias. Por ejemplo, se debe entender que la obligación de respetar y proteger las instalaciones de salud se extiende a los datos médicos que pertenecen a esos establecimientos. Sin embargo, sería importante aclarar la medida en que los datos civiles que no se benefician de esa protección específica, como los datos de la seguridad social, los registros fiscales, las cuentas bancarias, los archivos de clientes de las empresas o las listas o registros electorales, ya se encuentran protegidos por las normas generales vigentes sobre la conducción de hostilidades[76].

Si bien concuerdo con el CICR, una mayor precisión podría llevar a advertir que el DIH no brinda protección plena a datos clave que afectan a la población civil. La política propuesta reduciría el riesgo, pues si una mayor precisión revelara que los datos no están protegidos por el DIH, estos igual gozarían de la protección que proporciona la política. Asimismo, la política podría aplicarse hasta que se precisara la cuestión de los datos, así como la del umbral de ataque.

El diablo está en los detalles, en este caso, en la identificación de las funciones y los servicios considerados esenciales. Es muy probable que haya discrepancias al respecto, como ya se ha observado en los extensos debates sobre la designación de algunos sistemas como "infraestructura crítica"[77]. Un ejemplo de un posible desacuerdo es cómo el CICR destaca los datos vinculados con cuentas bancarias y registros electorales en la cita anterior tomada del Informe sobre los desafíos de los conflictos armados contemporáneos de 2015. Estimo que muchos Estados no estarían dispuestos a eliminar completamente de la discusión esos datos. Por ejemplo, una operación cibernética en la que se bloquea el acceso a las cuentas bancarias de los amigos de un dictador o de miembros de su partido político bien podría ser una opción interesante durante un conflicto armado, al igual que obstaculizar su reelección manipulando los datos de la votación podría ser atractivo para un Estado enemigo. No menciono esta cuestión para expresar mi desacuerdo,

74 Manual de Tallinn 2.0, nota 6 *supra*, norma 145. Para las obligaciones en general, v. CG IV, arts. 23, 59; PA I, arts. 69-70.

75 Informe del CICR sobre los desafíos de los conflictos armados contemporáneos de 2015, nota 41 *supra*, pp. 55-56.

76 Ibíd., p. 56.

77 V., p. ej., John Moteff, Claudia Copeland y John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?*, Informe del Servicio de Investigación del Congreso de Estados Unidos, 29 de enero de 2003.

sino para destacar que será difícil conseguir un consenso amplio respecto de qué funciones y servicios civiles son esenciales y merecen ser protegidos.

Sin embargo, parecería que algunas funciones encajan claramente dentro de los límites de la categoría; por ejemplo, los servicios sociales para las personas discapacitadas, los jóvenes, los pobres y los ancianos. Lo mismo vale para la educación primaria y secundaria. Entre los indicadores de si es adecuado incluir una función o servicio en la categoría, podría encontrarse el hecho de que interferir en ellos como se ha ejemplificado probablemente generaría una profunda preocupación en la población civil. Por ejemplo, en otro artículo, he propuesto que "la integridad de los datos de instituciones financieras y la disponibilidad de sistemas financieros críticos" deben gozar de protección especial en materia de políticas[78].

Otro indicador podría ser que una operación cibernética que afecta una función particular de un servicio tuviera consecuencias que continuaran mucho después de la finalización de las hostilidades. Un ejemplo pertinente sería el de una operación que impidiera el funcionamiento general del sistema de universidades nacionales, aunque, en ese caso, la protección no se extendería a la infraestructura cibernética individual de una universidad que pudiera considerarse como objetivo miliar, como aquellas que realizan investigaciones sobre armas u otras áreas de interés militar.

Segunda política: equilibrio entre los efectos negativos para los civiles y los beneficios relacionados con el conflicto

La segunda política propuesta se aplicaría en situaciones no comprendidas en la primera (o hasta que se alcance un acuerdo respecto de las funciones y los servicios comprendidos en ella). A diferencia del primero, que es de carácter absoluto, este compromiso es relativo en el sentido de que se basa en el equilibrio entre las consideraciones humanitarias y los intereses del Estado relativos al conflicto armado. Según esta segunda opción, 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*

78 Michael N. Schmitt y Tim Maurer, "Protecting financial data in cyberspace: Precedent for further progress on cyber norms?", *Just Security*, 26 de agosto de 2017, disponible en línea en www.justsecurity.org/44411/protecting-financial-data-cyberspace-precedent-progress-cyber-norms/. Esa propuesta no comprende actividades tales como bloquear el acceso a los datos durante un período limitado o acceder a datos confidenciales.

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[79].

Retomando las controversias planteadas anteriormente, la inaplicabilidad del DIH podría ser consecuencia de la conclusión de un Estado de que la operación no constituye un ataque en los términos del DIH o de la adopción de la posición de que los datos no son objetos. Cabe señalar que la perspectiva de la interpretación del derecho aplicable sería la del Estado que realiza la operación. Dicho de otro modo, en virtud de esta propuesta, el Estado estaría de acuerdo en aplicar la política toda vez que llegara a la conclusión de que una operación no se rige por las normas del DIH relativas a la conducción de hostilidades. Otro Estado podría llegar a una conclusión distinta respecto de una operación análoga; en ese caso, respetaría las disposiciones previstas en el derecho.

El compromiso merece un análisis pormenorizado. Para empezar, comprende operaciones que tienen como objetivo infraestructura cibernética y datos que o bien son objetivos militares, o bien son objetos civiles. Una cuestión interesante en este sentido que ha sido señalada en el Informe del CICR sobre los desafíos de los conflictos armados contemporáneos de 2015 tiene que ver con los bienes de "doble uso", es decir, los que se utilizan con propósitos militares y civiles. La posición dominante entre los expertos en DIH es que todo uso militar de un objeto civil, incluida la infraestructura cibernética, convierte al objeto en un objetivo militar, con excepción de los aspectos que son componentes claramente separados y definidos[80]. En el Informe sobre los desafíos de los conflictos armados contemporáneos, se expresa el temor de que ese criterio se aplique en el contexto cibernético:

79 El foco del DIH en el elemento físico plantea cuestiones específicas respecto de las operaciones cibernéticas que, en efecto, *constituyen* un ataque. En particular, el daño colateral que se tiene en cuenta para el análisis de la proporcionalidad y el requisito de tomar todas las precauciones posibles en el ataque se limita textualmente a las lesiones, la muerte o el daño. Si bien puede entenderse razonablemente que el daño incluye la pérdida de funcionalidad (independientemente de dónde se fije el umbral), este no incluye otras formas de daño. Por ejemplo, el análisis de la proporcionalidad de un ataque a una infraestructura de uso dual no necesitaría, desde el punto de vista del derecho, tener en cuenta la interrupción temporaria o la pérdida de servicios civiles que dependen de ella, a menos que la pérdida pusiera en riesgo de daño físico a personas civiles o de daño a bienes de carácter civil. Si bien el caso es el mismo para los ataques cinéticos, como un ataque a una tienda que se emplea para almacenar armas, las redes y otras formas de conectividad incrementan las repercusiones no nocivas o no destructivas en cadena de los ciberataques. Este artículo no aborda esa realidad, pues se limita a las operaciones cibernéticas que están más allá del alcance del DIH, pero es un fenómeno específico de la esfera cibernética que merece una atención particular.

80 Manual de Tallinn 2.0, nota 6 *supra*, norma 101; Programa de Harvard de investigación en políticas humanitarias y conflictos, *HPCR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge University Press, Cambridge, 2013 (Manual de Harvard), p. 119; Nils Melzer, *Derecho internacional humanitario: Una introducción integral*, CICR, Ginebra, 2016, p. 101. Para un análisis del carácter diferenciado de parte de un objetivo establecido, v. Michael N. Schmitt y John J. Merriam, "The tyranny of context: Israeli targeting practices in legal perspective", *University of Pennsylvania Journal of International Law*, vol. 37, n.º 1, 2015, pp. 119-123.

> Una aplicación estricta de este entendimiento podría llevar a concluir que muchos objetos que forman parte de la infraestructura del ciberespacio constituirían objetivos militares y no estarían protegidos contra los ataques (cibernéticos o cinéticos). Esto causaría graves preocupaciones debido al impacto que esa pérdida de protección podría causar en términos de la perturbación del creciente uso civil concomitante del ciberespacio[81].

Comparto la preocupación. La cuestión de si la infraestructura cibernética constituye un objetivo militar trasciende el alcance de este artículo. Adhiero a la opinión dominante. Pero, aunque esta posición cambiara con el transcurso del tiempo y se decidiera que determinada infraestructura cibernética de uso dual es de carácter civil, sería legítimo ejecutar operaciones cibernéticas contra ella, incluidas las operaciones con consecuencias graves para la población civil, siempre y cuando esas operaciones no alcanzaran el nivel de un ataque, en particular, por ser nocivas o destructivas. La política propuesta resolvería, en parte, el dilema.

Algunos términos de la política han sido seleccionados cuidadosamente para enfatizar determinadas cuestiones y, con suerte, servirán como ejes alrededor de los cuales giren los futuros debates. La frase "consecuencias negativas" se emplea en sentido amplio. Incluye todas las consecuencias para la población civil que no impliquen que la operación cibernética constituye un ataque y, por ende, está sujeta a la aplicación de las normas relativas a los ataques. Si bien se limita a las consecuencias para las personas, en cuanto distintas de los objetos, se extiende a todas las consecuencias para los civiles causadas por los efectos de una operación sobre la infraestructura tomada como objetivo. Por ejemplo, un ataque de denegación de servicio al sistema informático de un banco impediría que los clientes retiraran dinero. En este caso, los clientes se verían afectados y, por lo tanto, la política sería aplicable.

Poner el foco en las consecuencias también indica que el tipo de una operación cibernética no influye en la aplicabilidad de la propuesta. Por ejemplo, un ataque de denegación de servicio o una operación que causara el enlentecimiento de un sistema cibernético no estarían menos regidos por la política que una operación que hiciera que el sistema operativo funcionara de forma incorrecta. Por el contrario, el factor clave es que la población civil se vería afectada de una manera que no está contemplada en las normas del DIH, al menos desde el punto de vista del Estado que ejecuta la operación.

Si bien los expertos del Manual de Tallin 2.0 estuvieron de acuerdo en que la inconveniencia no es lo bastante grave para que se alcance el umbral de un ataque, no existe motivo para trazar una línea de esa naturaleza en el caso de la política propuesta. Esto es así porque solo prohibiría una operación cibernética cuando las consecuencias negativas para los civiles fueran excesivas comparadas con los beneficios esperados relacionados con el conflicto. Desde el punto de vista de la política, hay una justificación para excluir la inconveniencia o la molestia de las consecuencias que prohibirían la operación cibernética si la parte que la ejecuta no

81 Informe sobre los desafíos de los conflictos armados contemporáneos de 2015, nota 41 *supra*, p. 56.

puede ofrecer una razón suficiente para que tenga mayor peso que los factores para no prohibirla. Pretender causar inconveniencias o molestias excesivas respecto de los beneficios esperados de la operación cibernética, que probablemente tendrían poca importancia, sería pura malicia. El Departamento de Defensa de EE. UU. parece haber adoptado la encomiable actitud de incorporar este enfoque como parte de sus políticas[82].

En lo que respecta a alcanzar un equilibrio entre las consideraciones humanitarias y los intereses de un Estado relacionados con un conflicto, la política propuesta aplica la prueba del exceso de la norma de proporcionalidad. El *HPCR Manual on the International Law Applicable to Air and Missile Warfare* (Manual de Harvard), redactado por un reconocido grupo de académicos y profesionales del ámbito del derecho internacional, adopta la razonable posición de que el exceso se caracteriza por una situación en la que "hay un desequilibrio considerable entre el beneficio militar esperado, por un lado, y el daño colateral a las personas civiles y los bienes de carácter civil previsto, por otro lado"[83]. Esta consideración está en línea con el principio de necesidad militar, un principio fundacional del DIH. Después de todo, no sería práctico utilizar una prueba estricta de equilibrio "51-49" respecto de dos valores tan disímiles –daño colateral y ventaja militar–, en especial, cuando la consecuencia de un leve desequilibrio percibido en favor del primero sería una prohibición absoluta de atacar un objetivo militar legítimo. La sensibilidad a esta dinámica se refleja asimismo en la aplicación de la norma de proporcionalidad del Estatuto de Roma solo cuando se espera que el daño colateral sea "manifiestamente" excesivo en relación con la ventaja militar "de conjunto" esperada[84].

Dado que las operaciones cibernéticas contempladas en la política incluyen las que se dirigen contra objetivos militares, aunque en situaciones que no alcanzan el nivel de un ataque, no tendría sentido disminuir el umbral de exceso. Si se propusiera un nivel inferior, los Estados albergarían la misma preocupación que animó la decisión de adoptar el criterio del exceso respecto de la proporcionalidad. Ciertamente, el argumento a favor de un umbral más alto es, en realidad, más fuerte respecto de la política porque el daño que, por lo general, no es nocivo ni destructivo, es de carácter menos grave.

La expresión "beneficio concreto relacionado con el conflicto" en la política propuesta debe distinguirse de la frase "ventaja militar concreta y directa" que figura en el principio de proporcionalidad en el ataque. Todos los adjetivos reflejan el componente de necesidad militar del equilibrio que sostengo que debe servir de base a la hora de adoptar las decisiones militares que afectan a la población civil. Sin embargo, como se explicará más adelante, la omisión de la palabra "directa" se

82 V. Manual de derecho de la guerra de EE. UU., nota 10 *supra*, párr. 16.5.2: "Por ejemplo, aunque una operación cibernética no constituya un 'ataque' o no cause daños o perjuicios graves que deban ser considerados a la luz del principio de proporcionalidad en el ataque, esa operación cibernética no deberá ejecutarse de forma de causar inconveniencias innecesarias a las personas civiles o neutrales".

83 Manual de Harvard, nota 80 *supra*, p. 92; Nils Melzer, *Targeted Killings in International Law*, Oxford University Press, Oxford, 2008, pp. 344, 360.

84 Estatuto de Roma, nota 13 *supra*, art. 8(2)(b)(iv).

debe a la intención de ampliar el alcance de la política más allá del que se aplica en el caso de la proporcionalidad.

Según el Comentario del CICR de los Protocolos adicionales, "la expresión 'concreta y directa' pretendía mostrar que la ventaja en cuestión debe ser sustancial y relativamente cercana, y que las ventajas que son apenas perceptibles y las que solo se obtendrían en el largo plazo no deben ser atendidas"[85]. El término también se explicaba en el comentario no oficial, aunque reconocido (en vista de la participación de los autores en la Conferencia Diplomática que redactó los Protocolos adicionales), de Bothe, Partsch y Solf. Allí, se señala que "concreta" significa "específica, no general; percibida por los sentidos", y se equipara el término a "definida" en la definición de objetivo miliar, que denota una ventaja que no es hipotética ni especulativa[86]. En cambio, continúan los autores, el adjetivo "directa" significa "sin intervención de la condición de agencia"[87].

No hay un fundamento lógico para sostener que los beneficios que han de tenerse en cuenta al aplicar la política propuesta no necesariamente tienen que ser concretos. Señalar que los beneficios especulativos relacionados con el conflicto podrían llegar a bastar para justificar las consecuencias negativas reales previstas para la población civil equivaldría a ignorar por completo las consideraciones humanitarias. Sin embargo, la misma lógica no se aplica al adjetivo "directa". Los Estados probablemente objetarían el requisito de nexo causal directo entre la operación y el beneficio que exige la proporcionalidad en los ataques cibernéticos u otras formas de ataque. Por ejemplo, en el caso de operaciones destinadas a debilitar el apoyo civil a la participación en un conflicto. Esas campañas normalmente consisten en una cadena de causalidad de más de un eslabón. La operación de información puede diseñarse para modificar la actitud de la población civil hacia el gobierno y el conflicto con el tiempo, tal vez alentando la participación de la sociedad civil o los medios de comunicación. Siempre que exista un nexo causal que no se atenúe hasta convertirse en especulativo, según la propuesta, sería adecuado tenerlo en cuenta en el proceso destinado a lograr el equilibrio.

Precisamente en la misma lógica, aunque invertida, se sustenta la limitación de las consecuencias negativas para la población civil a las concretas. Indicar que una parte en conflicto debe renunciar a llevar adelante una operación que probablemente tendría beneficios válidos relacionados con el conflicto sobre la base de la especulación respecto de las posibles consecuencias negativas para la población civil implicaría empujar indebidamente el equilibrio deseado en la dirección opuesta.

La otra diferencia significativa entre la política propuesta y la norma de proporcionalidad es la sustitución del término "ventaja militar" por la frase

85 Comentario del CICR de los PA, nota 52 *supra*, párr. 2209.

86 Michael Bothe, Karl Josef Partsch y Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, segunda edición, Martinus Nijhoff, Leiden y Boston, Massachusetts, 2013, p. 407. V. también Ministerio de Defensa del Reino Unido, *The Manual of the Law of Armed Conflict*, 2004 (Manual del derecho de la guerra del Reino Unido), párr. 5.33.3.

87 M. Bothe, K. J. Partsch y W. A. Solf, nota 86 *supra*, p. 407.

"beneficio relacionado con el conflicto". La ventaja militar es un concepto que el DIH interpreta en sentido estricto. Por ejemplo, en el Manual de Harvard se señala:

> La ventaja militar hace referencia solo a la que está directamente relacionada con las operaciones militares y no con otras formas de ventaja que puedan, de algún modo, relacionarse con el conflicto de manera más general. La ventaja militar no hace referencia a la ventaja de naturaleza exclusivamente política, psicológica, económica, financiera, social o moral. Así pues, obligar al enemigo a cambiar su posición en las negociaciones solo afectando la moral de la población civil no equivaldría a una ventaja militar[88].

La política no limitaría la ventaja obtenida en las operaciones cibernéticas a lo puramente militar. Tomando el ejemplo anterior, sería aceptable considerar la conducción de operaciones cibernéticas destinadas a alterar la posición de negociación del enemigo, incluso afectando la moral de la población civil. Los Estados ya planifican operaciones cibernéticas que no constituyen ataques, incluidas las que alteran o eliminan datos, que tienen efectos que no son exclusivamente militares. En vista de la resistencia esperable de estos Estados a imponer una norma que requiera un beneficio militar, en la propuesta no se emplea el término "militar"[89].

Es necesario destacar que el término "ventaja" normalmente hace referencia a una ganancia militar para la parte que comete el ataque en los planos táctico u operacional de la guerra, pero no en el plano estratégico, es decir, político[90]. Dicho de otro modo, la ventaja debe tener un impacto no demasiado mitigado en el campo de batalla o en la campaña militar en cuestión[91]. Por ejemplo, la ventaja de conseguir que los líderes militares del enemigo reconsideren su participación en el conflicto, como en el caso de ataques contra sus bienes o inversiones personales, no convertiría esos objetivos en objetivos militares ni justificaría el daño colateral causado cuando se realiza una evaluación de proporcionalidad.

88 Manual de Harvard, nota 80 *supra*, p. 36.

89 Como se señala en la declaración de la ratificación del PA I por el Reino Unido, "la ventaja militar prevista para un ataque hace referencia a la ventaja prevista del ataque en su conjunto y no solo de partes aisladas o particulares del ataque". Declaración de ratificación del Protocolo adicional del Reino Unido, párr. (i), disponible en línea en https://tinyurl.com/yct795zh.

90 "Nivel táctico de la guerra: Nivel de la guerra en el que las batallas y combates se planifican y ejecutan para alcanzar objetivos militares asignados a unidades tácticas o destacamentos especiales", Departamento de Defensa de EE. UU., *Dictionary of Military and Associated Terms*, versión de marzo de 2018, p. 226; "Nivel operacional de la guerra: Nivel de la guerra en el que se planifican, conducen o sustentan las campañas y las grandes operaciones militares a fin de alcanzar objetivos en teatros de operaciones u otras zonas operacionales", ibíd., p. 173; "Nivel estratégico de la guerra: Nivel de la guerra en el que una nación, con frecuencia, en cuanto miembro de un grupo de naciones, determina objetivos y orientación estratégicos en materia de seguridad nacional o multinacional (alianza o coalición), y desarrolla y emplea recursos nacionales para alcanzar dichos objetivos", ibíd., p. 219.

91 Manual del derecho de la guerra del Reino Unido, nota 86 *supra*, párr. 5.33.5; Manual de Harvard, nota 80 *supra*, pp. 36-37; Manual de Tallinn 2.0, nota 6 *supra*, p. 442. V., también Ian Henderson, *The Contemporary Law of Targeting*, Martinus Nijhoff, Boston, Massachusetts, 2009, pp. 199-202, que proporciona un análisis pormenorizado de las razones por las cuales la ventaja militar puede medirse en el plano operacional en contraposición con el plano táctico y de por qué, por lo general, es inadecuado medir la ventaja militar en el plano estratégico.

No obstante, los Estados aspiran a obtener una ventaja en el nivel estratégico que no esté vinculada con las operaciones en el campo de batalla, y el DIH los habilita a ejecutar operaciones militares que no alcanzan el nivel de un ataque para obtenerla. Por ello, para que sea satisfactoria para los Estados, la política propuesta permite tener en cuenta los beneficios concretos en todos los niveles de la guerra al evaluar si puede lanzarse una operación cibernética. A modo de ejemplo, bloquear la capacidad del enemigo de difundir propaganda relacionada con el conflicto mediante operaciones de denegación de servicio contra instalaciones de medios de comunicación sería un beneficio que podría tenerse en cuenta al evaluar el equilibrio.

A pesar de la ampliación del alcance vinculado a la norma de proporcionalidad, la política limita los beneficios a aquellos en los que existe un nexo claro con el conflicto. Si bien esto puede llevar a argumentar que la condición es demasiado restrictiva, la finalidad de la política es ampliar la protección contra el perjuicio para la población civil durante una situación que probablemente ya sea terrible: el conflicto armado. Las operaciones cibernéticas ejecutadas por malicia o venganza contra personas civiles o contra la población civil deben estar prohibidas.

Este requisito no debe confundirse con la aplicación del principio de necesidad militar. Según algunas interpretaciones de este principio, solo están permitidos "el tipo y el nivel de fuerza, que no estén prohibidos por el derecho de la guerra, requeridos para alcanzar el propósito legítimo del conflicto, es decir, la rendición parcial o total del enemigo lo antes posible y con el menor costo"[92]. La aplicación de este principio no sería suficiente para afrontar el problema en cuestión. En primer lugar, como se ha señalado, el principio de necesidad militar solo se aplica al uso de la fuerza; la política propuesta se centra en operaciones cibernéticas que no pueden ser definidas fácilmente como tales. En segundo lugar, si bien se refiere a la necesidad basada en consideraciones "militares", la frase "relacionado con el conflicto armado" de la política tiene una referencia más amplia. En tercer lugar, y de manera muy significativa, hay cierta oposición a tratar el principio de necesidad militar como una norma fundamental del derecho internacional que funciona independientemente de otras normas fundamentales del derecho internacional. Esa cuestión fue, en parte, responsable de la oposición que suscitó la *Guía para interpretar la noción de participación directa en las hostilidades según el derecho*

92 Manual del derecho de la guerra del Reino Unido, nota 86 *supra*, párr. 2.2.

internacional humanitario del CICR[93], y es vista con recelo por algunos expertos[94]. En mi opinión, la necesidad militar es un principio fundacional del DIH, pero no es una norma fundamental[95]. Sea cual fuere la interpretación correcta, el principio de necesidad militar no puede satisfacer los fines que se pretende alcanzar a través de la adopción de la política propuesta.

Por último, al igual que la norma de proporcionalidad, la prueba propuesta en la política se aplica *ex ante* y no *post factum*, lo cual se evidencia en el uso de términos como "previsto" y "esperado". Así pues, quienes apliquen la política serán juzgados sobre la base de cómo hayan pensado que eran los hechos, dentro de lo razonable, en el momento en que se haya planificado, aprobado y ejecutado la operación cibernética.

Reflexiones finales

El estado actual del DIH que rige las operaciones cibernéticas no es totalmente satisfactorio. La falta de precisión respecto de qué operaciones cibernéticas constituyen ataques, en el mejor de los casos, pone en riesgo a los civiles cuando no debería ser así y, en el peor de los casos, habilita a los Estados a aprovechar la ambigüedad para dirigir operaciones cibernéticas sumamente perjudiciales contra la población civil. Además, algunas operaciones cibernéticas que claramente no constituyen ataques podrían sembrar el caos entre la población civil.

La cuestión de si los datos son objetos complejiza aún más la situación. Por un lado, si lo son, muchas operaciones cibernéticas que ejecutan los Estados estarían prohibidas. Por loables que sean sus intenciones, los defensores de esta posición pecan de ingenuos al creer que su interpretación será aceptada por los Estados con capacidades cibernéticas[96]. Pero, por otro lado, no considerar que

93 La oposición al capítulo IX de la Guía del CICR para interpretar la noción de participación directa, nota 34 *supra*, surgió cuando algunos de los expertos que participaban en el proyecto objetaron lo que consideraban que era un uso del principio como norma fundamental del derecho. V., p. ej., W. Hays Parks, "Part IX of the ICRC 'Direct Participation in Hostilities' study: No mandate, no expertise, and legally incorrect", *New York University Journal of International Law and Politics*, vol. 42, n.º 3, 2010, pp. 802-810. No obstante, v. la respuesta de Nils Melzer, que en ese momento pertenecía a la división jurídica del CICR y que encabezó el proyecto: Nils Melzer, "Keeping the balance between military necessity and humanity: A response to four critiques of the ICRC's interpretive guidance on the notion of direct participation in hostilities", *New York University Journal of International Law and Politics*, vol. 42, n.º 3, 2010, pp. 892-912.

94 Es interesante, en este sentido, consultar el Manual del derecho de la guerra de EE. UU., nota 10 *supra*, párr. 16.5.2. (las operaciones que no se consideran ataques, de todos modos, "no deben dirigirse contra enemigos civiles ni bienes de carácter civil, a menos que las operaciones respondan a la necesidad militar"). Este análisis ha recibido críticas, merecidas, por cierto. V. William H. Boothby y Wolff Heintschel von Heinegg, *The Law of War: A Detailed Assessment of the Department of Defense Law of War Manual*, Cambridge University Press, Cambridge, 2018.

95 M. N. Schmitt, nota 19 *supra*.

96 El teniente coronel Bart van den Bosch (del Ejército de los Países Bajos) está realizando un interesante trabajo sobre esta cuestión en el programa de doctorado de la Universidad de Ámsterdam ("Hacer la guerra sin violencia") con la dirección del profesor Terry Gill y el brigadier general Paul Ducheine.

algunos datos civiles son objetos de carácter civil que están protegidos por el DIH implica subestimar las consideraciones humanitarias en las que se sustenta la prohibición de atacar bienes de carácter civil. Para alcanzar el equilibrio entre las consideraciones humanitarias y la necesidad militar, los argumentos formulados desde ambas posiciones son insuficientes.

Las políticas propuestas han sido pensadas para hacer frente a esas realidades. Al principio, los Estados pueden oponerse. Esto suele ocurrir cuando los académicos y las organizaciones no gubernamentales proponen limitar la discrecionalidad de los Estados en el campo de batalla y, en muchos casos, la reacción está justificada. Sin embargo, en estos casos, los Estados deberán tener en cuenta las consideraciones que se plantean a continuación.

En primer lugar, según mis intercambios con quienes ejecutan operaciones cibernéticas, parecería que algunos elementos de las políticas adoptan la forma de reglas de combate y otros, de orientación o simplemente de práctica aceptada. Es más: el artículo 57(1) del PA I requiere que las partes en conflicto contemplen la posibilidad de que haya consecuencias negativas para la población civil o los bienes de carácter civil durante las operaciones militares, incluidos los ataques, aunque sin limitarse a estos. Pienso que esta disposición refleja el DIH consuetudinario, y los grupos de expertos y manuales militares confirman que el requisito de "cuidado constante" tiene por finalidad imponer un deber positivo, aunque es de carácter general y está insuficientemente definido[97]. Lo único que hacen las políticas propuestas es proporcionar orientación respecto de las medidas que han de adoptarse luego de realizar la evaluación.

En este sentido, se podría proponer que el resultado de las políticas ya se logra mediante la aplicación de la Cláusula de Martens, porque las situaciones destacadas deben estar sujetas a "las leyes de la humanidad" y "las exigencias de la conciencia pública". Aun así, los Estados y los expertos no están de acuerdo en los medios por los que ha de implementarse la cláusula y si esta impone normas vinculantes específicas a las partes en conflicto. Independientemente de la posición que se adopte con respecto a estas cuestiones, la Cláusula de Martens destaca por su vaguedad y por su escasa aplicación en la práctica. Siendo así, las políticas propuestas proporcionan un nivel de claridad práctica y una dirección que pueden funcionar para proporcionar protección real a la población civil.

En segundo lugar, prohibir los ataques a las infraestructuras cibernéticas o los datos que puedan interferir en funciones o servicios civiles esenciales es

97 V. Manual del derecho de la guerra del Reino Unido , nota 86 *supra*, párr. 5.32.1 ("Así, el jefe militar deberá tener en cuenta las consecuencias para la población civil de lo que ha decidido hacer y adoptar medidas para mitigar tales consecuencias en la medida de lo posible"); Manual de Harvard, nota 80 *supra*, p. 142 ("La frase 'cuidado constante' significa que no hay excepciones al deber de respetar a la población civil, las personas civiles y los bienes de carácter civil"); Manual de Tallinn 2.0, nota 6 *supra*, p. 477 (donde se observa el "deber general de 'respetar' a la población civil, es decir, de tener en cuenta los efectos deletéreos de las operaciones militares para los civiles"). Más aún, el Manual de Tallinn 2.0 determina que "el deber de cuidado constante exige a los jefes militares y a todas las personas que participan en las operaciones estar continuamente atentos a los efectos de sus actividades en la población civil y en los bienes de carácter civil, y tratar de evitar todos los efectos innecesarios de dichas operaciones" (p. 477).

congruente con la premisa general de que determinadas actividades, funciones y bienes merecen protección especial contra los efectos perjudiciales de la guerra. Las políticas propuestas simplemente reconocen que el universo existente de dichas actividades, funciones y bienes debe expandirse para responder a los riesgos particulares, y a veces graves, para la población civil vinculados con las operaciones cibernéticas. Más aún, dejan en manos de los Estados la decisión de qué funciones y servicios son esenciales y, por ende, merecen protección especial, al menos en el plano de las políticas.

En tercer lugar, el lector perspicaz habrá advertido que la segunda política, que exige un equilibrio, es más restrictiva respecto de las operaciones que no se consideran ataques contra objetivos militares que respecto de las que sí se consideran ataques. La norma de proporcionalidad aplicable a los ataques cibernéticos solo exige que se contemple el daño (incluida, posiblemente, la pérdida de funcionalidad), las lesiones o la muerte. Por el contrario, la política propuesta comprende todas las consecuencias negativas para la población civil. Esto podría parecer ilógico, pero el resultado se compensa por el hecho de que la política es más permisiva en cuanto a qué puede tener en cuenta la parte que conduce la operación cibernética cuando evalúa un posible equilibrio con las consecuencias negativas. La norma de proporcionalidad se limita a la ventaja militar concreta y directa. Por el contrario, la política propuesta permite que se tengan en cuenta beneficios que no son de naturaleza directa ni militar, y los beneficios pueden corresponder al nivel estratégico de la guerra. Por lo tanto, la política logra un equilibrio justo entre las consideraciones humanitarias y los intereses del Estado. Los Estados pueden encontrar un alivio adicional en el hecho de que la política adopta el criterio del nivel de exceso, que otorga a las partes en conflicto un considerable margen de interpretación al aplicarla.

Las políticas propuestas no son la panacea contra el daño no nocivo y no destructivo a las personas civiles o a las poblaciones civiles causado por las operaciones cibernéticas. Gran parte de ese daño quedaría sin atender, como en el caso de la aplicación de la norma de proporcionalidad a los ataques cibernéticos, dado que la norma solo se aplica al daño colateral, las lesiones o la muerte. No obstante, el tiempo para que los Estados y la comunidad internacional aborden las cuestiones humanitarias siempre es anterior a su manifestación trágica en el campo de batalla. En este caso, el tiempo es hoy.