La aplicación del principio de distinción en el contexto cibernético: una perspectiva china

Zhixiong Huang y Yaohui Ying*

Zhixiong Huang, Joven Académico Sobresaliente del programa Changjiang, es profesor en el Instituto de Derecho Internacional/Instituto de Gobernanza Cibernética de la Universidad de Wuhan. También se desempeña como investigador del Equipo Clave para la Innovación de Shanghái, un grupo dedicado al tema "Investigación sobre los mecanismos jurídicos de salvaguardia para la construcción del Cinturón y la Ruta de la Seda" que pertenece a la Universidad de Ciencias Políticas de China Oriental. Correo electrónico: fxyhzx@whu.edu.cn.

Yaohui Ying es doctorando en la Facultad de Derecho de la Universidad de Wuhan, China. Correo electrónico: yingyaohui@whu.edu.cn.

Resumen

Hasta ahora, el gobierno de China se ha limitado a formular solo observaciones muy generales sobre la aplicación del derecho internacional humanitario al ciberespacio. Por cierto, hay algunos artículos académicos chinos relacionados con este tema, pero el examen del principio de distinción adolece de limitaciones tanto en su extensión como en su profundidad académica. En comparación con Occidente, las investigaciones

* Esta investigación cuenta con el apoyo del Fondo Nacional de Ciencias Sociales de China para Grandes Proyectos (Subvención n.° 20&ZD204). Los autores desean expresar su agradecimiento a todos los editores y revisores por sus útiles sugerencias y a Eric Jensen, Kubo Mačák, Ignacio de la Rasilla del Moral, Jinyuan Su, Nicole Hogg y Nicholas Tsagourias por sus valiosos comentarios sobre versiones anteriores de este artículo. Un borrador del presente artículo fue presentado en el taller "El derecho en los conflictos armados híbridos de hoy", organizado por la Universidad Brigham Young en febrero de 2019, y todas las respuestas y observaciones de los participantes han sido muy apreciadas.

de los estudiosos chinos acerca de esta cuestión siguen en una etapa relativamente preliminar. En la actualidad, no hay deconstrucciones ni aclaraciones específicas sobre la aplicación del principio de distinción en el ciberespacio que hayan sido elaboradas por académicos chinos. Este es el primer informe escrito por académicos chinos que versa específicamente sobre esta cuestión. Por ello, ofrece una perspectiva diferente, presentando las posiciones de los funcionarios chinos y las opiniones de los académicos de ese país. Los autores se proponen discernir si las normas existentes siguen siendo plenamente aplicables en el contexto cibernético y, si es necesario, determinar qué tipo de mejoras y aclaraciones podrían hacerse. Al intervenir en estos debates, argumentamos que, pese a los posibles problemas técnicos y a las incertidumbres, el principio de distinción debería aplicarse en el ciberespacio. Este principio también debería reexaminarse y esclarecerse para prevenir la militarización excesiva y fortalecer la protección de los intereses de las poblaciones civiles. En lo que respecta a los objetivos humanos, los elementos del estatuto del combatiente definidos en el derecho internacional consuetudinario y en los tratados relevantes no resultan adecuados para el campo de batalla digital, pero, aun así, los cibercombatientes están obligados a distinguirse de las personas civiles. Al aplicar el principio de distinción, afirmamos que es más lógico centrarse en los elementos sustantivos que en los elementos formales, tales como llevar las armas a la vista o tener un signo distintivo fijo que sea reconocible a distancia. Al interpretar la "participación directa en las hostilidades", el umbral de daño exige una probabilidad objetiva, no la mera intención subjetiva; el nexo beligerante debería confirmarse y el vínculo causal debería ser directo. La aplicación por analogía del modelo de la "cadena de eliminación cibernética" nos ayuda a comprender todo el proceso de la participación directa en las hostilidades durante la ciberguerra. En cuanto a los objetivos no humanos, todos los objetivos militares deben satisfacer en forma acumulativa tanto el criterio de la "contribución efectiva" como el de la "ventaja militar definida", que son igualmente indispensables. Los mismos requisitos se aplican a los objetos de doble uso. Además, ciertos datos deberían encuadrarse en el ámbito de los bienes de carácter civil.

Palabras clave: China, principio de distinción, ciberespacio, cibercombatiente, objetivo militar, datos.

***

Introducción

Hasta ahora, el gobierno chino no se ha pronunciado con claridad acerca de la aplicación del derecho internacional humanitario (DIH)[1] al ciberespacio. Hubo algunos debates preliminares sobre el DIH en el ciberespacio entre los estudiosos chinos[2], en especial aquellos con antecedentes militares[3], pero el examen

1 Con el fin de evitar confusiones, aquí se introduce una nota para aclarar dos términos: "derecho de los conflictos armados" y "derecho internacional humanitario". Existen algunas preocupaciones acerca del uso inexacto de estos dos términos. Hay quienes piensan que su significado es básicamente el mismo y que se pueden usar indistintamente, por ejemplo: "...el derecho de los conflictos armados, también conocido como el derecho internacional humanitario, incluye principios tales como la distinción entre los objetivos militares y civiles" (Comité Internacional de la Cruz Roja (CICR), *The Law of Armed Conflict: Basic Knowledge*, Ginebra, junio de 2002, p. 2, disponible en: www.icrc.org/eng/assets/files/other/law1_final.pdf), mientras que otros interpretan que el "derecho internacional humanitario" es un concepto potencialmente más limitado que se relaciona únicamente con las normas de los conflictos armados destinadas a reglamentar el trato de las personas –civiles o militares, heridas o activas– en los conflictos armados (Mary O'Connell, "Historical Development and Legal Basis", en Dieter Fleck (ed.), *The Handbook of International Humanitarian Law*, 3.ª ed., Oxford University Press, Oxford, 2013, p. 11). La fusión de las normas del campo de batalla con los objetivos humanitarios ha suscitado algunas críticas. Por ejemplo, "una posible desventaja del término [DIH] es que podría interpretarse que excluye algunas partes del derecho de los conflictos armados (como la ley de la neutralidad) cuyo propósito básico no es humanitario" (Jean Pictet, *Humanitarian Law and the Protection of War Victims*, A. W. Sijthoff, Leiden, 1975, p. 11). La Comisión de Derecho Internacional traza una distinción entre el derecho de los conflictos armados y el derecho internacional humanitario, señalando que el primero rige la conducción y las consecuencias de los conflictos armados, en tanto que el segundo forma parte del primero y constituye la *lex specialis* que rige la conducción de hostilidades (párr. 4 de "Commentary to Art. 2 of the Draft Articles on the Effects of Armed Conflicts on Treaties", *ILC Yearbook*, vol. 2, parte 2, 2011). Para consultar un examen más detallado de la terminología, v. Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, Cambridge University Press, Cambridge y Nueva York, 2010, pp. 22–26. En general, los libros de texto y los artículos chinos sostienen que el DIH ha derivado del derecho de los conflictos armados y por ende consideran que esos términos son sinónimos. V., por ejemplo, 朱文奇, 何谓国际人道*, 武大国际*评论, 2003, 1 (Wenqi Zhu, "What Is International Humanitarian Law?", *Wuhan University International Law Review*, vol. 1, 2003, disponible solo en chino). A los fines del presente artículo, el término "DIH" se utilizará en forma general, en tanto que "derecho de los conflictos armados" se usará cuando las fuentes citadas emplean ese término en particular.

2 V., por ejemplo, Li Zhang, "A Chinese Perspective on Cyber War", *International Review of the Red Cross*, vol. 94, n.° 886, 2012, p. 804, disponible en: https://international-review.icrc.org/sites/default/files/irrc-886-zhang.pdf (se accedió a todas las referencias de internet en enero de 2021); Longdi Xu, "The Applicability of the Laws of War to Cyberspace: Exploration and Contention", 2014, p. 7, disponible en: www.gov.uk/government/publications/the-applicability-of-the-laws-of-war-to-cyberspace-exploration-and-contention; Chris Wu, "An Overview of the Research and Development of Information Warfare in China", en Edward Halpin, Philippa Trevorrow, David Webb y Steve Wright (ed.), *Cyberwar, Netwar and the Revolution in Military Affairs*, Palgrave Macmillan, Londres, 2006; 朱莉欣, 信息网络战的国际*问题研究, 河北*学, 2009, 27(01) (Lixin Zhu, "Research on the International Law of Information Network Operations", *Hebei Law Science*, vol. 27, n.° 1, 2009, solo disponible en chino); 姜世波, 网络攻击与战争*的适用, 武大国际*评论, 2013, 16(02) (Shibo Jiang, "War by Internet Cyber Attack and the Application of the Law of War", *Wuhan University International Law Review*, vol. 16, n.° 2, 2013, solo disponible en chino); 李伯军, 论网络战及战争*的适用问题, *学评论, 2013, 31(04) (Bojun Li, "On Cyber Warfare and the Application of the Law of War", *Law Review*, vol. 31, n.° 4, 2013, solo disponible en chino); 朱莉欣, 平战结合与网络空间国际规则制定, 信息安全与通信保密, 2018(07) (Lixin Zhu, "Competition for International Rules in Cyberspace under the Combination of Peacetime and Wartime", *Information Security and Communications Privacy*, n.° 7, 2018).

3 王海平, 武装冲突*研究进展及需要关注的问题, 当代*学, 2012, 26(05) (Haiping Wang, "The Research

del principio de distinción en el ciberespacio adolece de limitaciones tanto en su extensión como en su profundidad académica. En comparación con Occidente, las investigaciones de los académicos chinos acerca de esta cuestión siguen en una etapa relativamente preliminar, y algunas tesis de doctorado sobre la aplicación del DIH al ciberespacio se encuentran en curso de elaboración. En la actualidad, no hay deconstrucciones ni aclaraciones específicas sobre la aplicación del principio de distinción en el ciberespacio que hayan sido elaboradas por académicos chinos.

Este es el primer informe escrito por académicos chinos que versa específicamente sobre la aplicación del principio de distinción en la ciberguerra. Por ello, ofrece una perspectiva diferente, incorporando al debate las posiciones de los funcionarios chinos y las opiniones de los académicos de ese país. En opinión de los autores, si bien los Estados tienen interpretaciones muy diferentes acerca de cómo se aplica exactamente el DIH al ciberespacio, no cabe duda alguna de que el principio básico de la distinción es aplicable en ese ámbito. El propósito de este artículo es esclarecer si las normas existentes siguen siendo plenamente aplicables en la ciberguerra y, si es necesario, determinar qué tipos de mejoras y aclaraciones podrían hacerse. Partiendo de esta base, la primera parte del artículo presenta el *statu quo* de la aplicación del DIH al ciberespacio y echa luz sobre la postura oficial de China y las opiniones de los académicos chinos acerca de esta cuestión. A continuación, en la segunda parte se analiza el concepto del principio de distinción y se señalan los desafíos y las controversias vinculados con su aplicación en el contexto cibernético. Aplicando la dicotomía personas-objetos, en las partes tercera y cuarta se examinan los desafíos jurídicos de fondo actuales y se presentan los puntos de vista chinos pertinentes. En lo que respecta a los objetivos humanos, en la tercera parte se analiza la aplicación de los criterios tradicionales usados para definir quiénes pueden ser atacados en el campo de batalla cibernético, se identifican los obstáculos relevantes y se formulan las sugerencias pertinentes. En la cuarta parte, se aborda el tema de los objetivos no humanos y se analiza qué se puede atacar en la ciberguerra, esto es, qué constituye un objetivo militar. Además, se examina la opinión de los académicos chinos acerca de si los datos digitales *per se* constituyen un objeto. En la última parte, se formulan algunas observaciones finales preliminares.

No cabe ninguna duda de que el uso pacífico del ciberespacio es de suma importancia para el bienestar común de la humanidad. Afortunadamente, hasta ahora el mundo se ha mantenido a salvo de ciberataques catastróficos con

Progress of the Law of Armed Conflict and the Issues Needing Attention", *Contemporary Law Review*, vol. 26, n.° 5, 2012, solo disponible en chino); 李莉, 鲁笑英.浅析信息化战争条件下武装冲突*所面临的问题, 西安政治学院学报, 2012, 25(01) (Li Li y Xiaoying Lu, "A Brief Analysis of the Problems Faced by the Law of Armed Conflict under the Condition of Information-Based Warfare", *Journal of Xi'an Politics Institute of PLA*, vol. 25, n.° 1, 2012, solo disponible en chino); 朱雁新, 计算机网络攻击之国际*问题研究, 中国政*大学, 2011 (Yanxin Zhu, "The Research on the International Issues of Computer Network Attack", disertación de doctorado, Universidad China de Ciencias Políticas y Derecho, 2011, solo disponible en chino); 张天舒, 从 "塔林手册" 看网络战争对国际*的挑战, 西安政治学院学报, 2014, 27(01) (Tianshu Zhang, "The Challenges of Cyber Warfare to International Law: From the Perspective of The Tallinn Manual on the International Law Applicable to Cyber Warfare", *Journal of Xi'an Politics Institute of PLA*, vol. 27, n.° 1, 2014, solo disponible en chino).

múltiples víctimas y de catalizadores de la guerra similares, como un "Pearl Harbor cibernético"[4]. Sin embargo, el preocupante aumento del número de incidentes cibernéticos beligerantes, con la inclusión de medios y métodos cibernéticos en los conflictos armados, nos obliga a prestar mucha atención a la aplicación del DIH en el ciberespacio.

Si bien, según las circunstancias, la ciberguerra[5] permite cierto grado de anonimato y brinda un sentido de interconexión, sigue siendo un tipo de guerra. En este sentido, hace ya más de una década que se celebran debates multilaterales sobre si el DIH –"un conjunto de normas destinado a limitar los efectos de los conflictos armados"[6]– se aplica en el ámbito del ciberespacio. Aún no se ha llegado a un consenso. El informe 2014-2015 del Grupo de expertos gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional pareció ofrecer alguna esperanza, ya que mencionó la aplicabilidad de los principios de distinción y proporcionalidad en el ciberespacio[7]: la frase "principios jurídicos internacionales... incluidos los principios de... distinción"[8] se considera un compromiso, porque algunos Estados

4 James J. Wirtz, "The Cyber Pearl Harbor", *Intelligence and National Security*, vol. 32, n.° 6, 2017; James J. Wirtz, "The Cyber Pearl Harbor Redux: Helpful Analogy or Cyber Hype?", *Intelligence and National Security*, vol. 33, n.° 5, 2018; Departamento de Defensa de EE. UU. (DoD), "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City", 12 de octubre de 2012, disponible en: https://content.govdelivery.com/accounts/USDOD/bulletins/571813.

5 En este artículo, el término "ciberguerra" se entiende como los "medios y métodos de guerra que se basan en la tecnología de la información y que se usan en el contexto de un conflicto armado". V. Jakob Kellenberger, "El derecho internacional humanitario y las nuevas tecnologías armamentísticas, 34.ª Mesa Redonda sobre problemas actuales de derecho internacional humanitario, San Remo, 8–10 de septiembre de 2011: discurso principal por el Dr. Jakob Kellenberger", *International Review of the Red Cross*, n.° 886, 2012, disponible en: https://international-review.icrc.org/es/articulos/el-derecho-internacional-humanitario-y-las-nuevas-tecnologias-armamentisticas-34a-mesa. Para algunos académicos chinos, la ciberguerra es una forma especial de la guerra de la información y constituye un nuevo medio o método de guerra. La guerra de la información consiste en una serie de actividades hostiles realizadas por las partes beligerantes con el fin de mantener su derecho a adquirir, controlar y usar la información. Su connotación y su extensión son más amplias que las de la ciberguerra y puede incluir la ciberguerra, la guerra de inteligencia, la guerra electrónica, la guerra psicológica y otros conceptos. La ciberguerra se refiere al proceso de adulterar, destruir o amenazar los sistemas y redes de información de las otras partes beligerantes, a la vez que se garantiza la seguridad de los sistemas y redes de información propios a través de las redes de ordenadores. V., por ejemplo, B. Li, nota 2 *supra*. Hay quienes argumentan que la cuestión principal que se expresa a través del concepto de la ciberguerra es si los atacantes cibernéticos, "armados" de teclados, virus informáticos y software maliciosos pueden transformarse (o ya se han transformado) en un nuevo medio o método de guerra. V. 黄志雄主编, 网络空间国际规则新动向: "塔林手册 2.0 版" 研究文集, *±会科学文献出版*±, 2019: 301 (Zhixiong Huang (ed.), *New Trends in International Rules for Cyberspace: Collection of Papers on Tallinn Manual 2.0*, Social Sciences Academic Press, China, 2019, p. 301); 黄志雄, 国际法视角下的 "网络战" 及中国的对策——以诉诸武力权为中心, 现代法学, 2015, 37(05) (Zhixiong Huang, "International Legal Issues concerning 'Cyber Warfare' and Strategies for China: Focusing on the Field of Jus ad Bellum", *Modern Law Science*, vol. 37, n.° 5, 2015).

6 V. CICR, "Guerra y derecho", disponible en: https://www.icrc.org/es/guerra-y-derecho.

7 V. Grupo de expertos gubernamentales de la 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, disponible en: https://undocs.org/sp/A/70/174

8 Ibíd.

(supuestamente, también China) no desean referirse en forma directa al DIH[9]. Sin embargo, el Grupo de expertos gubernamentales de la ONU que trabajó en el período siguiente (2016-2017) no pudo llegar a un consenso, y una de las cuestiones controvertidas fue la aplicación del DIH en el ciberespacio[10]. Con la adopción de dos resoluciones separadas (y, según algunos, contrapuestas) del Primer Comité de la Asamblea General en 2018[11], el futuro consenso de los Estados acerca del DIH en el ciberespacio se presenta cada vez más incierto y confuso.

En un mundo ideal, pareciera que cuando una situación ha alcanzado el umbral de un conflicto armado, la aplicación de las normas del *jus in bello* al ciberespacio no debería ser más difícil que verter vino viejo en una botella nueva. Si la ciberguerra fuese meramente un nuevo medio o método de guerra, entonces se aplicarían automáticamente las normas del *jus in bello* existentes y no habría nada misterioso o inescrutable en ello. Sin embargo, la realidad frecuentemente choca con los ideales. Debido a la enorme diferencia entre los campos de batalla cibernéticos y los tradicionales, muchas de las normas existentes parecen ser más confusas en la ciberguerra y deben ser reconceptualizadas. Esto sucede, en particular, en el caso del principio de distinción. Por ejemplo, un problema importante relacionado con este principio radica en la distinción entre los cibercombatientes y las personas civiles. Los combatientes tienen la obligación de llevar las armas a la vista y tener un signo distintivo fijo reconocible a distancia[12]. Esto no parece ser viable en el contexto cibernético, donde la norma suele ser el anonimato y donde es imposible saber quién está sentado frente al ordenador que ejecuta un ataque. Las normas fueron redactadas en una época en la que la guerra involucraba un cierto nivel de proximidad física entre los contendientes; en la mayoría de los casos, los combatientes se veían entre sí y, por ello, podían distinguir entre combatientes y no combatientes, entre amigos y enemigos[13]. Pero en el caso de las personas

9 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: www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

10 V., por ejemplo, ibíd.; Arun Mohan Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?", *Lawfare*, 4 de julio de 2017, disponible en: https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

11 V. "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased", *Council on Foreign Relations Blog*, 15 de noviembre de 2018, disponible en: www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased. Las dos resoluciones fueron patrocinadas por Rusia (Doc. ONU A/C.1/73/L.27/Rev.1) y por Estados Unidos (Doc. ONU A/C.1/73/L.37), respectivamente.

12 III. Convenio de Ginebra del 12 de Agosto de 1949 relativo al trato debido a los prisioneros de guerra, 75 UNTS 135 (fecha de entrada en vigor: 21 de octubre de 1950) (CG III), art. 4 A) 2); Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (PA I), 1125 UNTS 3, 8 de junio de 1977 (fecha de entrada en vigor: 7 de diciembre de 1978) (PA I), art. 44 3); Jean-Marie Henckaerts y Louise Doswald-Beck (ed.), *El derecho internacional humanitario consuetudinario*, Volumen 1: Normas, Cambridge University Press, Cambridge, 2005 (en adelante, "Estudio del CICR sobre DIH consuetudinario"), pp. 16–19, disponible en: https://www.icrc.org/es/doc/assets/files/other/icrc_003_pcustom.pdf.

13 Heather Harrison Dinniss, "Participants in Conflict – Cyber Warriors, Patriotic Hackers and the Laws of War", en Dan Saxon (ed.), *International Humanitarian Law and the Changing Technology of War*, Martinus Nijhoff, Boston, MA, y Leiden, 2013, p. 256; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 145.

civiles que participan directamente en las hostilidades[14], el problema se torna aún más confuso. Es muy posible que personas no organizadas lancen un ataque contra un adversario; el ejemplo típico sería un grupo de piratas informáticos activistas que implementan un ataque distribuido de denegación de servicio por razones patrióticas o ideológicas. Por ejemplo, el ciberataque anónimo lanzado en 2007 contra las estructuras esenciales, las telecomunicaciones, los servidores DNS, los sitios web y los servidores de correo electrónico de Estonia parece haber sido consecuencia de una disputa política sobre el traslado del "Monumento a los libertadores de Estonia", una obra soviética que representa la victoria de la URSS sobre el nazismo, del centro de Tallin a un cementerio militar situado en las afueras de la ciudad[15]. ¿Cuál es la persona que participa directamente en las hostilidades? ¿La que ingresa el código malicioso, la que formula (pero no ejecuta) el código o la que ordena la creación del código?

China es el país con el mayor número de internautas y ha sufrido frecuentes ataques cibernéticos[16], por lo cual ha participado activamente en la promoción del respeto de las leyes en el ciberespacio. Sin embargo, aunque hace ya muchos años que es uno de los Estados partes en los Convenios de Ginebra[17] y en los Protocolos adicionales I y II a los Convenios de Ginebra (PA I y PA II)[18], China no se ha mostrado muy entusiasta con respecto a la cuestión del DIH en el ciberespacio y siempre ha evitado abordar el problema de la ciberguerra y el derecho aplicable[19].

La renuencia de China a examinar la cuestión del DIH en profundidad se ha evidenciado en numerosas ocasiones. Por ejemplo, en su reciente presentación ante el Grupo de trabajo de composición abierta sobre los avances en la esfera de la

14 El Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 6, estipula que las personas civiles gozan de protección contra los ataques, salvo si participan directamente en las hostilidades y mientras dure tal participación. Para acceder a un debate sustantivo sobre la "participación directa en las hostilidades", v. Nils Melzer, *Guía para interpretar la noción de participación directa en las hostilidades según el derecho internacional humanitario*, CICR, Ginebra, 2009 (en adelante, "Guía sobre la participación directa en las hostilidades").

15 Para acceder a una descripción detallada del ciberataque contra Estonia en 2007, v. "Cyber Attacks against Estonia (2007)", *International Cyber Law in Practice: Interactive Toolkit*, Ciberdefensa Cooperativa, Centro de Excelencia de la OTAN (CCD COE), disponible en: https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_ Estonia (2007); Eneken Tikk, Kadri Kaska y Liis Vihul, *International Cyber Incidents: Legal Considerations*, CCD COE, Tallin, 2010, pp. 15–16, 31.

16 Academia China de Estudios sobre el Ciberespacio (ed.), *China Internet Development Report 2017*, Springer, Berlín, 2019, p. 107; 国家互联网应急中心, 2020 年上半年我国互联网网络安全监测数据分析报告, 2020 (Equipo Técnico de Respuesta a emergencias relacionadas con la red informática nacional/ Centro de Coordinación de China, *Analysis Report of China's Internet Network Security Monitoring Data in the First Half of 2020*, 2020, solo disponible en chino), disponible en: https://tinyurl.com/y2lpzdh4; Ministerio de Relaciones Exteriores de la República Popular China, "Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on September 29, 2020", disponible en: https://tinyurl.com/y4xolw3g.

17 La ratificación de los Convenios de Ginebra por China tuvo lugar el 28 de diciembre de 1956. V. la base de datos sobre tratados del CICR, disponible en: https://ihl-databases.icrc.org/applic/ihl/ihl-search.nsf/content.xsp?lang=ES.

18 China ratificó y se adhirió a los Protocolos adicionales I y II el 14 de septiembre de 1983. V. ibíd.

19 Binxin Zhang, "Cyberspace and International Humanitarian Law: The Chinese Approach", en Suzannah Linton, Tim McCormack y Sandesh Sivakumaran (ed.), *Asia-Pacific Perspectives on International Humanitarian Law*, Cambridge University Press, Cambridge, 2019, p. 323.

información y las telecomunicaciones en el contexto de la seguridad internacional, China declaró que "la aplicabilidad de la ley de los conflictos armados y del *jus ad bellum* se debe manejar con prudencia"[20]. Esto sugiere que China, por alguna razón (quizás política), no quiere discutir en detalle el tema del DIH en el ciberespacio y, por ende, pone trabas al esclarecimiento de la cuestión. En lugar de describir su postura y su razonamiento, China se ha limitado a afirmar reiteradamente que "la licitud de la ciberguerra no debe reconocerse en circunstancia alguna"[21]. Esa actitud de resistencia se observa claramente en el discurso pronunciado por el delegado chino ante la Sesión Anual de la Organización Consultiva Jurídica Asiático-Africana (AALCO) celebrada en 2019:

> China adhiere al principio del uso pacífico del ciberespacio y se opone con firmeza... a la ciberguerra y [a la] carrera armamentista cibernética... En ausencia de la práctica de los Estados, deberíamos actuar con gran prudencia al debatir la aplicación del derecho humanitario en las llamadas "ciberguerras". La razón es muy simple pero fundamental: en primer lugar, las ciberguerras no deberán permitirse; y en segundo lugar, la ciberguerra será una forma completamente novedosa de la guerra, que se basará en tecnologías de avanzada. Teniendo en cuenta la "brecha digital" entre los países desarrollados y los países en desarrollo, estos últimos se encontrarán, en general, en una posición desventajosa en cuanto al estudio y el desarrollo de esas normas, y será difícil garantizar que estas sean justas y equitativas"[22].

China otorga gran importancia al uso pacífico del ciberespacio y afirma que el exceso de debate sobre la aplicación del DIH podría tener efectos negativos en la paz y la seguridad internacionales, lo cual exacerbaría tanto la carrera armamentista como la militarización del ciberespacio. Por ejemplo, China ha expresado esta crítica diciendo que "este paradigma militar"[23] prescinde del principio de la no utilización de la fuerza[24] y podría afectar la confianza estratégica entre los países y aumentar el riesgo de las falsas percepciones y los conflictos entre los Estados"[25]. En este contexto, no sorprende que el gobierno de China no se haya expresado claramente sobre la aplicación del principio de distinción en el ciberespacio. Hasta cierto punto, la actitud conservadora de China es comprensible. En primer lugar, no

20 V. "China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", p. 6, disponible en: www.un.org/disarmament/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

21 Ibíd.

22 AALCO, *Acta Literal de los Debates: 58.ª Sesión Anual*, AALCO/58/DAR ES SALAAM/ 2019/VR, Dar es Salaam, 21–25 de octubre de 2019, disponible en: www.aalco.int/Final%20Verbatim%202019.pdf.

23 AALCO, *Acta Literal de los Debates: 54.ª Sesión Anual*, AALCO/54/BEIJING/2015/VR, Pekín, 13–17 de abril de 2015.

24 Xinmin Ma, "What Kind of Internet Order Do We Need?", *Chinese Journal of International Law,* vol. 14, n.º 2, 2015. Xinmin Ma se desempeñó como director adjunto del Departamento de Tratados y Derecho del Ministerio de Relaciones Exteriores de China entre 2014 y 2019.

25 *AALCO, Acta Literal de los Debates: 55.ª Sesión Anual*, AALCO/55/NEW DELHI (HEADQUARTERS)/ 2016/VR, Nueva Delhi, 17–20 de mayo de 2016.

hay una práctica nacional ampliamente reconocida que constituya un ciberataque; en segundo lugar, debido a la índole histerética del derecho, la aplicación del DIH en el ciberespacio no debería determinarse con demasiada anticipación[26]. La actual actitud negativa del gobierno chino acerca de esta cuestión también podría constituir una táctica dilatoria que China utiliza a la espera de adoptar una postura clara. Desde el punto de vista de los autores, no existe ningún obstáculo jurídico a la aplicación del DIH en el ciberespacio, particularmente en lo que respecta al principio de distinción. Es innegable que ya se han producido guerras cibernéticas y que esa práctica continuará. Le guste o no a China, es probable que se vea obligada expresar su postura sobre el DIH en el ciberespacio.

El principio de distinción y el desafío de su aplicación al ciberespacio

Tras haber presentado, como punto de partida para nuestro análisis, el estado actual de la aplicación del DIH en el ciberespacio, la actitud oficial de China y las opiniones de algunos estudiosos chinos sobre este tema, es el momento de analizar el principio de distinción *per se* y resumir los desafíos y las controversias que entraña su aplicación en el contexto cibernético. Según la Corte Internacional de Justicia (CIJ), en su opinión consultiva *Legalidad de la amenaza o el empleo de armas nucleares*, el principio de distinción es un principio fundamental del derecho de los conflictos armados que ha alcanzado la categoría de norma del derecho internacional consuetudinario[27]. El artículo 48 del PA I estipula que las partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares, y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares[28].

En términos generales, el principio de distinción adopta un enfoque de dos niveles con respecto a la regulación de las hostilidades. Prohíbe los medios y métodos de guerra indiscriminados, y también reglamenta el uso de los medios y métodos que son lícitos. Esto significa que se debe distinguir entre los objetivos militares y los combatientes, por un lado, y las personas y bienes que se deben respetar y proteger, por el otro. Se prohíben los ataques indiscriminados[29].

Un "ataque" activa una amplia gama de protecciones jurídicas relacionadas con la distinción, sobre todo aquellas contenidas en los artículos 49 a 58 del PA I. Por lo tanto, para explicar con exactitud cómo se puede aplicar el principio de distinción al ciberespacio, es preciso contar, como condición previa, con una definición adecuada de "ciberataque". Hubo algunos debates académicos profundos y significativos acerca de qué constituye un ciberataque[30]. La definición más

26 Para acceder a más explicaciones sobre la actitud de China hacia el DIH, v. B. Zhang, nota 19 *supra*.

27 CIJ, *Legalidad de la amenaza o el empleo de armas nucleares*, Opinión consultiva, 8 de julio de 1996, ICJ Reports 1996, p. 266.

28 PA I, art. 48; Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, normas 1, 7, pp. 3, 29.

29 PA I, art. 51 4); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 11, p. 43.

30 V. Marco Rossini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, pp. 178–182; William H. Boothby, "Where Do Cyber Hostilities Fit in the International Law Maze?", en Hitoshi Nasu y Robert McLaughlin (ed.), *New Technologies and the Law of Armed Conflict*,

aceptada adopta un enfoque basado en las consecuencias. Por ejemplo, el *Manual de Tallin 2.0 sobre el Derecho Internacional Aplicable a las Ciberoperaciones* (en adelante, Manual de Tallin 2.0) define un ciberataque como "una operación cibernética, ofensiva o defensiva, cuando sea de prever razonablemente que cause lesiones o muerte a las personas o daños o destrucción a los objetos"[31]. Nosotros adoptamos la definición contenida en dicho artículo[32]. Ninguna disposición jurídica aparente prohíbe en forma explícita ni aborda el uso de la ciberguerra como una práctica distinta de otras formas de la guerra. Por ahora, el DIH guarda silencio acerca de los temas vinculados con la distinción en la ciberguerra y, por ello, algunos estudiosos aducen que el actual marco basado en tratados no es adecuado para abordar esa cuestión; este aspecto de la guerra virtual afecta negativamente la aplicación del principio de distinción[33]. Ciertos académicos afirman que una de las causas de esta situación[34] es que las infraestructuras civiles y militares no solo están estrechamente interconectadas y relacionadas entre sí, sino que, de hecho, son la misma cosa. Esta afirmación puede llevar a conclusiones que plantean importantes obstáculos a la aplicación del principio de distinción. Si la mayoría de los componentes del ciberespacio –como los cables de fibra óptica, los satélites, los enrutadores y los nodos– son objetos de doble uso que se utilizan simultáneamente para fines civiles y militares, su clasificación puede ser problemática y causar cuestiones espinosas en relación con el principio de proporcionalidad[35]. Al mismo tiempo, la clasificación

Springer, Berlín, 2014, pp. 60–62; Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks", artículo presentado ante la Conferencia Internacional de Expertos sobre ataques contra redes informáticas y aplicabilidad del derecho internacional humanitario, Estocolmo, 17–19 de noviembre de 2004; Cordula Droege, "Fuera de mi nube: guerra cibernética, derecho internacional humanitario y protección de la población civil", *International Review of the Red Cross*, n.° 886, 2012; Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?", *Stanford Law and Policy Review*, vol. 25, n.° 2, 2014.

31 Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Manual de Tallin 2.0), norma 92, p. 415.

32 El enfoque basado en las consecuencias es de suma utilidad, dado que traslada el foco de los medios y de la naturaleza del ataque a los efectos y consecuencias del acto, cumpliendo así con el requisito de la "violencia" y manteniendo el dinamismo y el carácter evolutivo de la disposición. Sin embargo, los autores de este artículo se plantean dos preocupaciones. La primera es que, desde el punto de vista práctico, la evaluación de los daños es extremadamente complicada, sobre todo cuando las consecuencias son mayormente indirectas. La segunda preocupación estriba en que el enfoque basado en las consecuencias limita la noción de ataque y excluye así las operaciones que causan daños no físicos, pero graves y problemáticos. Las mismas preocupaciones se señalan en el documento de posición del CICR *Derecho internacional humanitario y ciberoperaciones durante conflictos armados*, Ginebra, noviembre de 2019 (en adelante, documento del CICR sobre DIH y Ciberoperaciones), p. 9. El CICR también ha mencionado que sería difícil conciliar un entendimiento demasiado restrictivo de la noción de ataque con el objeto y el fin de las normas sobre la conducción de hostilidades, esto es, garantizar la protección de la población civil y de los bienes de carácter civil contra los efectos de las hostilidades. V. CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, 32IC/15/11, octubre de 2015 (Informe del CICR sobre DIH y desafíos, 2015), p. 54.

33 V. Jeffrey Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review*, vol. 106, n.° 7, 2008, pp. 1429–1430.

34 Robin Geiss y Henning Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review*, vol. 45, n.° 3, 2012, pp. 381, 383.

35 El principio de distinción establece que, en los conflictos armados, solo los objetivos militares pueden ser objeto de ataques directos. No obstante, el ataque contra un objetivo militar lícito puede, a veces, causar

de las personas como combatientes o civiles no siempre es clara, porque la creciente participación de personas civiles en la guerra[36], caracterizada por el mayor uso de tecnologías informáticas de avanzada, ha difuminado los límites. Las empresas militares y civiles se comunican, cooperan entre sí y se integran con una intensidad sin precedentes[37]. Por ejemplo, China ha incluido dos veces en sus libros blancos la estrategia de la integración entre civiles y militares[38]. Además, la atribución de responsabilidades dista de ser fácil[39]: mientras que es relativamente fácil determinar desde dónde se lanzó un cohete, el despliegue de ciberoperaciones no crea columnas de humo.

Son muchos los académicos que han hecho esfuerzos rigurosos para investigar cómo se aplica el principio de distinción en la ciberguerra[40], y varios Estados, como Estados Unidos[41] y Dinamarca[42], han incorporado la aplicación del principio de distinción en la ciberguerra en sus respectivos manuales militares. En general, se reconoce, por ejemplo, que un ataque no necesita ser cinético para que se le apliquen las normas del DIH; que se prohíben los ataques indiscriminados[43]; y que si un ataque no está dirigido contra personas u objetos militares particulares, no se permite en ningún caso. Esto podría suceder con un virus informático, si es capaz de propagarse en forma incontrolada desde los sistemas militares a los sistemas civiles conectados. Si bien existe consenso en que se debe distinguir entre los objetivos/los combatientes militares y las personas/los bienes de carácter civil, cuando en la práctica se intenta determinar exactamente qué constituye un objetivo militar y quién es un combatiente en un conflicto armado informático, la cuestión se torna sumamente controvertida. Por otra parte, como señala un estudioso

daños indirectos a personas civiles o a bienes de carácter civil. Estos efectos colaterales perjudiciales son regulados por el principio de proporcionalidad, que prohíbe los ataques cuando sea de prever que causen daños a la población civil o a bienes de carácter civil que sean excesivos en relación con la ventaja militar prevista. El art. 51 5) b) del PAI contiene una definición clara del principio de proporcionalidad. V. también Jonathan Crowe y Kylie Weston-Scheuber, *Principles of International Humanitarian Law*, Edward Elgar, Cheltenham, 2013, pp. 55–57.

36 "Los civiles desempeñan un papel cada vez más importante y complejo en los conflictos armados, como víctimas y como autores de crímenes". Esta tendencia general se describe como "*civilianization*" (participación directa de civiles) en Andreas Wenger y Simon J. A. Mason, "Participación directa de civiles en conflictos armados: tendencias e implicancias", *International Review of the Red Cross*, n.° 872, 2008.

37 L. Zhu, "Competition for International Rules in Cyberspace", nota 2 *supra*, p. 40.

38 Oficina de Información del Consejo de Estado de la República Popular China (SCIO), *China's National Defense in the New Era*, Beijing, julio de 2019, disponible en: www.scio.gov.cn/zfbps/32832/Document/1660325/1660325. htm; SCIO, *China's Military Strategy*, Beijing, mayo de 2015, disponible en: www.scio.gov.cn/zfbps/ndhf/2015/ Document/1435159/1435159.htm.

39 V. documento del CICR sobre DIH y Ciberoperaciones, nota 32 *supra*, pp. 10–11.

40 V., por ejemplo, J. Kelsey, nota 33 *supra*, p. 1427; Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts", *Journal of Conflict and Security Law*, vol. 17, n.° 2, 2012, p. 261; Michael N. Schmitt, "Wired Warfare: Computer Network Attack and *Jus in Bello*", *International Review of the Red Cross*, vol. 84, n.° 846, 2002, p. 365.

41 Departamento de Defensa, *Law of War Manual*, Wáshington, DC, 12 de junio de 2015, pp. 985–999.

42 Ministerio de Defensa de Dinamarca, Comando de Defensa de Dinamarca, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, Copenhague, septiembre de 2016.

43 PA I, art. 51 4).

chino, la característica subyacente de la no letalidad de los medios y métodos cibernéticos hace que los objetos y las personas protegidos sean más vulnerables en la ciberguerra que en la convencional. Esto dará lugar a confusión a la hora de evaluar la legalidad de las operaciones cibernéticas y causará violaciones más frecuentes del principio de distinción en las ciberoperaciones militares[44]. Vista la importancia del principio de distinción en el campo de batalla cibernético, es necesario esclarecer si las normas existentes siguen siendo plenamente aplicables en la ciberguerra e investigar qué tipos de mejoras y aclaraciones podrían hacerse.

El principio de distinción aplicado a los objetivos humanos en la ciberguerra

Para definir la índole del objetivo, el principio de distinción recurre a la dicotomía personas-objetos. No importa cuánto evolucione la tecnología, el autor de un acto hostil sigue siendo una persona, e incluso cuando introduce virus o ataca un cortafuegos en formas que parecen meras pulsaciones de teclas y clics del ratón, la dicotomía personas-objetos, que define *quién* y *qué* puede ser atacado, sigue siendo aplicable. En esta parte del artículo, abordaremos la cuestión de quién puede ser objeto de un ataque lícito en el contexto cibernético. El principio básico es que está prohibido atacar a personas civiles[45]. El principio de distinción presupone que los beligerantes pueden distinguir claramente entre civiles y combatientes. Sin embargo, debido al anonimato del ciberespacio, resulta difícil sostener esta suposición.

Todos los combatientes antes han sido civiles, y todos los civiles pueden convertirse en combatientes[46], sea porque han sido reclutados, porque se incorporan voluntariamente a las fuerzas armadas de una parte beligerante, porque participan directamente en las hostilidades (lo cual conlleva la pérdida del estatuto de persona protegida mientras dure tal participación)[47], o porque forman parte de un levantamiento en masa, concepto que permite la transición de persona civil a combatiente lícito[48]. Los autores no tratarán el tema del levantamiento en masa aquí, porque este concepto exige la invasión física de un territorio nacional y la participación de un segmento importante de la población[49], lo cual es prácticamente imposible que suceda con medios informáticos[50].

44 陈鹏飞, 论当代武装冲突法面临的挑战, 西安政治学院学报, 2014, 27(05) (Pengfei Chen, "Análisis de los desafíos del derecho de los conflictos armados contemporáneo", *Journal of Xi'an Politics Institute of PLA*, vol. 27, n.° 5, 2014, solo disponible en chino).

45 PA I, art. 51 2); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 6, pp. 22–27.

46 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2016, p. 174.

47 PA I, art. 51 3); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 6, pp. 23–24; Guía sobre la participación directa en las hostilidades, nota 14 *supra*, pp. 41–68.

48 CG III, art. 4A 6); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 106, pp. 437–439 y, en particular, la norma 5, que explica que los miembros de un levantamiento en masa constituyen una excepción a la definición de personal civil, dado que, aunque no son miembros de las fuerzas armadas, reúnen las condiciones para ser considerados combatientes.

49 III CG, art. 4A 6).

50 Manual de Tallin 2.0, nota 31 *supra*, norma 88, p. 409.

Debido a que ofrecen ciertas ventajas, como su bajo costo y la facilidad con que el Estado puede negar su responsabilidad en ellas, "la mayoría de las ciberoperaciones se subcontratan a expertos informáticos civiles"[51]. A la luz de esta tendencia, es muy probable que, a excepción de las unidades cibernéticas incorporadas en las fuerzas armadas regulares, "muchos miembros del personal que participan de forma sustantiva en las ciberoperaciones sean personas civiles"[52]. De este modo, ¿pueden un *hacker* patriótico o un experto informático transformarse en objetos de ataque? La respuesta a esta pregunta depende de la interpretación de la "participación directa en las hostilidades" en el contexto de las ciberoperaciones.

¿Quiénes son los cibercombatientes?

Los civiles que participan directamente en las hostilidades pierden el estatuto de persona protegida y no tienen derecho a la inmunidad del combatiente. Algunos estudiosos incluso afirman que son combatientes "ilícitos"[53]. El DIH favorece una división clara y fiable entre combatientes y no combatientes, lo que refleja el papel esencial del principio de distinción en este ordenamiento jurídico. Los combatientes tienen derecho a participar directamente en las hostilidades[54] y gozan de inmunidad contra el enjuiciamiento por actos que realizaron conforme al DIH[55]; por ende, pueden ser atacados. La ciberguerra no es una excepción a esta regla. Puesto que la definición de persona civil es puramente negativa (son personas civiles quienes no son combatientes)[56], la pregunta de quién es un cibercombatiente cobra una importancia fundamental[57].

Algunos Estados han establecido, dentro de sus fuerzas armadas, secciones especiales responsables de las ciberoperaciones. Por ejemplo, Estados Unidos ha creado el Comando Cibernético de EE. UU. (USCYBERCOM), una subunidad del Comando Estratégico de EE. UU. elevada al rango de Comando de Combate Unificado[58], mientras que Colombia estableció un Comando Conjunto Cibernético

51 Elizabeth Mavropoulou, "Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks", *Journal of Law and Cyber Warfare*, vol. 4, n.° 2, 2015, p. 78.

52 David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities", *Journal of Conflict and Security Law*, vol. 17, n.° 2, 2012, p. 292; v. también Michael N. Schmitt, "'Direct Participation in Hostilities' and 21st Century Armed Conflict", en Horst Fischer y Dieter Fleck (ed.), *Crisis Management and Humanitarian Protection: Festschrift for Dieter Fleck*, BWV, Berlín, 2004, p. 527.

53 Y. Dinstein, nota 46 *supra*, p. 44.

54 PA I, art. 43 2).

55 H. Harrison Dinniss, "Participants in Conflict", nota 13 *supra*, p. 254.

56 PA I, art. 50 1); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 5, pp. 20–22.

57 Vijay M. Padmanabhan, "Cyber Warriors in the Jus in Bello", *International Law Studies*, vol. 89, 2013; Maurizio D'Urso, "The Cyber Combatant: A New Status for a New Warrior", *Philosophy and Technology*, vol. 28, n.° 3, 2015; Jake B. Sher, "Anonymous Armies: Modern 'Cyber-Combatants' and Their Prospective Rights under International Humanitarian Law", *Pace International Law Review*, vol. 28, n.° 1, 2016; Sean Watts, "The Notion of Combatancy in Cyber Warfare", artículo presentado en la IV Conferencia Internacional sobre los Conflictos Cibernéticos, Tallin, 5–8 de junio de 2012.

58 Donald Trump, "Statement by President Donald J. Trump on the Elevation of Cyber Command", 18 de agosto de 2017, disponible en: https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

de las Fuerzas Armadas encargado de prevenir y contrarrestar las amenazas o los ataques informáticos que afecten los valores e intereses nacionales[59]. La definición de cibercombatiente merece ser analizada, porque no solo afecta la cuestión de quién es un objetivo lícito, sino que también influye en la determinación de quién tiene derecho al estatuto de prisionero de guerra en caso de captura.

Básicamente, los combatientes son miembros de las fuerzas armadas de una parte beligerante –independientemente de que esas fuerzas sean regulares o irregulares o que pertenezcan al ejército permanente o a unidades de reservistas–, con inclusión de las milicias paramilitares incorporadas *de facto* en las fuerzas armadas. La tarea concreta que se asigna a una persona dentro del aparato militar no es relevante[60].

Los Convenios de Ginebra enumeran cinco condiciones que se deben cumplir para dar lugar al estatuto de combatiente lícito[61]. Las primeras cuatro son condiciones acumulativas establecidas por el Reglamento de La Haya y los Convenios de Ginebra para la aplicabilidad del estatuto de prisionero de guerra y de combatiente lícito: i) estar mandados por una persona que responda de sus subordinados (organización); ii) tener un signo distintivo fijo reconocible a distancia; iii) llevar las armas a la vista; y iv) dirigir sus operaciones de conformidad con las leyes y costumbres de la guerra (cumplimiento)[62]. Estas cuatro condiciones se aplican a los miembros de milicias y de otros cuerpos de voluntarios, pero también constituyen requisitos implícitos para los miembros de las fuerzas armadas de una parte en el conflicto. Una condición adicional que se puede inferir de los Convenios de Ginebra es: v) pertenecer a una parte en el conflicto[63].

Los autores consideran que los elementos i), iv) y v) son sustantivos, en tanto que los elementos ii) y iii) son formales. Teniendo en cuenta que el estado normal en la ciberguerra es el anonimato, es más lógico centrarse en los elementos sustantivos que en los formales.

El primer elemento, la organización, es esencial en la ciberguerra. Esta es una cuestión más fáctica que jurídica, y el requisito refleja la presencia de un mando responsable y de una relación jerárquica[64]. Si un grupo cibernético no cuenta con una organización suficiente, que normalmente incluye una estructura

59 ONU, *Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional: Informe del Secretario General*, Doc. ONU A/67/167, 23 de julio de 2012, p. 5.

60 Y. Dinstein, nota 46 *supra*, p. 41.

61 H. Harrison Dinniss, *Cyber Warfare*, nota 13 *supra*, p. 144.

62 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, 75 UNTS 31 (fecha de entrada en vigor: 21 de octubre de 1950), art. 13 2); 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, 75 UNTS 85 (fecha de entrada en vigor: 21 de octubre de 1950), art. 13 2); CG III, art. 4 a) 2); IV. Convenio de Ginebra del 12 de agosto de 1949 relativo a la protección debida a las personas civiles en tiempo de guerra (fecha de entrada en vigor: 21 de octubre de 1950), art. 4 2); H. Harrison Dinniss, *Cyber Warfare*, nota 13 *supra*, p. 145.

63 CG III, art. 4A 6); H. Harrison Dinniss, *Cyber Warfare*, nota 13 *supra*, p. 145.

64 Y. Dinstein, nota 46 *supra*, p. 39; Tribunal Penal Internacional para Ruanda (TPIR), *The Prosecutor v. Jean-Paul Akayesu*, caso n.° ICTR-96-4-T, Fallo (Sala de Primera Instancia), 2 de septiembre de 1998, párr. 626.

formada por superiores y subordinados, la división de tareas, la responsabilidad y determinados elementos de disciplina y de supervisión, sus miembros no pueden ser combatientes lícitos y ciertamente no tendrían derecho a la inmunidad del combatiente. Teniendo en cuenta que los miembros de la mayoría de los cibergrupos tienen la misma intención pero carecen de una disciplina común, es poco probable que un grupo armado que exista exclusivamente en línea esté suficientemente organizado[65]. Por ejemplo, si no se producen consecuencias cuando los miembros de un grupo de pronto deciden interrumpir las hostilidades cibernéticas o no participar en ellas (puede suceder que los miembros de un grupo no se conozcan entre sí), o si los miembros de un grupo no se sienten obligados a acatar las órdenes de un comandante, no es razonable afirmar que un grupo tan poco organizado satisfaga los requisitos del elemento de la organización. Así sucede, en particular, con los cibergrupos patrióticos[66].

El cuarto elemento, el cumplimiento del DIH, sigue siendo indispensable y no ha cambiado mucho con el advenimiento de la tecnología de las redes informáticas[67]. Si los propios combatientes no están dispuestos a respetar el DIH, no se les permite recurrir a ese ordenamiento jurídico cuando quieren aprovechar los beneficios que ofrece[68].

El último elemento se relaciona con la pertenencia a una parte en el conflicto, y su finalidad es demostrar la existencia de una cierta relación entre un grupo que lanza ataques informáticos y un estado beligerante[69]. Aunque los ataques por redes informáticas permiten el uso de "milicias cibernéticas" y son atractivos para los Estados porque les permiten "negar creíblemente" su participación en ellos, los participantes no se consideran combatientes lícitos a menos que pueda establecerse una relación entre el grupo y el Estado en cuestión[70]. Las fuerzas armadas regulares del Estado no necesitarían demostrar esa conexión, pero cuando se trata de grupos organizados que actúan en línea, el nivel de control que se debe tener sobre ellos no está claro[71].

65 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, p. 195.

66 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.

67 H. Harrison Dinniss, *Cyber Warfare*, nota 13 *supra*, p. 149.

68 Y. Dinstein, nota 46 *supra*, p. 54.

69 V. Denise Bindschedler-Robert, "A Reconsideration of the Law of Armed Conflicts", en *The Law of Armed Conflicts: Report of the Conference on Contemporary Problems of the Law of Armed Conflict*, 1971, p. 40; Katherine Del Mar, "The Requirement of 'Belonging' under International Humanitarian Law", *European Journal of International Law*, vol. 21, n.° 1, 2010.

70 H. Harrison Dinniss, "Participants in Conflict", nota 13 *supra*, p. 262.

71 La norma de control efectivo elaborada por la CIJ en Nicaragua parece inadecuada para definir el significado de "perteneciente a una de las partes en el conflicto", ya que, a diferencia de las normas de control general y dependencia total, expresa el control sobre el acto y no sobre el actor, por lo cual se centra en actividades específicas. Marko Milanović, "State Responsibility for Acts of Non-State Actors: A Comment on Griebel and Plücken", *Leiden Journal of International Law*, vol. 22, n.° 2, 2009, p. 317. Con respecto a las normas de control efectivo, control general y dependencia total, v. Antonio Cassese, "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", *European Journal of International Law*, vol. 18 n.° 4, 2007.

La cuestión más compleja se relaciona con el segundo y el tercer elemento, que exigen que los combatientes tengan un signo distintivo fijo reconocible a distancia y lleven las armas a la vista. Estas dos condiciones están estrechamente vinculadas con el principio de distinción entre combatientes y civiles. La finalidad de esas condiciones es eliminar las dudas en este sentido y prevenir intentos de engaño[72], pero hay una dificultad intrínseca que impide su transposición al entorno informático, donde, debido al anonimato del ciberespacio, es imposible saber quién se encuentra frente a un ordenador determinado. En vista de la imposibilidad de identificar a los usuarios de ordenadores mediante signos distintivos, algunos estudiosos han propuesto que este requisito se aplique a los ordenadores o a los sistemas, al igual que los automóviles, aviones y naves militares, que deben portar signos distintivos. Esta propuesta no es viable, dado que marcar un ordenador militar equivale a transformar en objetivos lícitos a todos los sistemas conectados a ese ordenador[73].

Cabe argüir que, aun así, las fuerzas armadas podrían llevar uniformes para cumplir con la obligación de tener un signo distintivo fijo reconocible a distancia[74]; por ejemplo, se podría obligar a los miembros de USCYBERCOM a utilizar uniformes militares mientras conducen las ciberoperaciones. Esta opinión parece tener algún mérito. Sería ideal que las fuerzas regulares utilizaran uniformes o se distinguieran de las personas civiles de algún otro modo. Pero en la práctica, ese requisito probablemente significaría poco, dado que las partes beligerantes permanecen anónimas. El objeto y el propósito de esta disposición es que el uso del uniforme sirva para eliminar la posibilidad de confusión a la hora de distinguir entre civiles y combatientes. En los conflictos armados tradicionales, el uso de uniformes casi siempre permite saber con certeza quién es combatiente y quién no[75]. Sin embargo, cuando los cibercombatientes están sentados frente a sus ordenadores, en ocasiones a gran distancia de los objetivos atacados, al otro Estado beligerante le da igual que lleven uniforme o no. Sea como sea, incluso si insistimos en que las fuerzas militares formales deben llevar uniforme, este requisito es absurdo cuando se trata de cibermilicias, cuerpos de voluntarios informáticos u otros cibergrupos organizados. Por otra parte, el ciberespacio no parece dejar margen alguno para el requisito de llevar las armas a la vista. Ya es de por sí difícil definir las armas

72 Y. Dinstein, nota 46 *supra*, p. 37.

73 Millones de *bots* (programas informáticos) recorren internet constantemente con la intención de hallar ordenadores conectados; un *bot* que busca direcciones de IP con designaciones militares las encontraría en cuestión de minutos. Una vez identificado un ordenador o un sistema, la única forma de ponerlos fuera de alcance es desconectarlos, pero esta solución probablemente altere su funcionamiento y/o su utilidad normales. Por ello, todo sistema que siga conectado a la red de alguna manera dependerá únicamente de sus defensas electrónicas para prevenir intrusiones y defenderse contra ellas. Por ende, si bien la idea de exhibir signos distintivos en los ordenadores o sistemas parece una solución útil en principio, en la práctica crea un desequilibrio entre la finalidad de este requisito y la capacidad de los militares de conducir sus operaciones. V. H. Harrison Dinniss, "Participants in Conflict", nota 13 *supra*, p. 257; H. Harrison Dinniss, *Cyber Warfare*, nota 13 *supra*, pp. 145–149.

74 Manual de Tallin 2.0, nota 31 *supra*, norma 87, p. 405.

75 No siempre es así; por ejemplo, los civiles que participan directamente en las hostilidades pueden ser atacados, pero es muy improbable que usen uniformes militares.

cibernéticas, y llevarlas a la vista es sencillamente inviable[76]. Por cierto, no se debe descartar la posibilidad de un ataque cinético contra los cibercombatientes. A modo de conclusión, nuestra opinión es que, en la ciberguerra, el segundo y el tercer elemento no se eliminarían de entrada, pero no habría necesidad de examinarlos en profundidad.

Quizás algunos piensen que, en el campo de batalla digital, esas distinciones no son realmente necesarias; en el contexto de un ciberataque contra bienes militares, el que efectúa el ataque es un combatiente o un civil que participa directamente en las hostilidades. En cualquiera de los dos casos, esa persona pierde el estatuto de persona protegida. Sin embargo, quedan algunos interrogantes por resolver, en particular si esa persona gozaría del estatuto de prisionero de guerra si fuese capturada[77]. Además, un atacante civil tal vez no satisfaga los requisitos del "umbral de daño" y del "nexo beligerante"[78], por lo cual no perdería el estatuto de persona protegida.

En suma, la tarea de definir quién es un cibercombatiente no solo es un problema jurídico complejo, sino también una cuestión técnica extremadamente difícil para la mayoría de los Estados. La realidad es que actualmente no existe la forma de identificar claramente a los cibercombatientes y, por ende, las normas vigentes son aplicables solo hasta cierto punto. Es más probable que las personas civiles participen en un conflicto armado informático que en un conflicto armado tradicional[79]. Como ha señalado Michael Schmitt, las razones de la creciente participación de los civiles son varias. Desde la perspectiva de costos y beneficios, para muchos países, el entrenamiento del personal militar en ataque y defensa cibernéticos es sumamente costoso y prolongado; además, los resultados no están garantizados. Por otra parte, la índole de la tecnología informática no permite su estandarización ni su cuantificación. La tecnología no solo se desarrolla y mejora constantemente; también es demasiado limitada y especializada[80].

Los elementos ii) y iii) identificados anteriormente –tener un signo distintivo fijo reconocible a distancia y llevar las armas a la vista– no se adaptan al contexto cibernético y probablemente no sea necesario tenerlos en cuenta en la ciberguerra. Sin embargo, para que una persona sea considerada un combatiente lícito, se deben satisfacer al menos los elementos i), iv) y v), a saber, la presencia de un mando responsable y la existencia de una relación jerárquica, la conducción de las operaciones conforme a las leyes y costumbres de la guerra, y la pertenencia a una de las partes en el conflicto. De otro modo, la persona en cuestión gozará de protección contra los ataques o se considerará que participa directamente en las hostilidades. En estas

76 V. Prashant Mali, "Defining Cyber Weapon in Context of Technology and Law", en Information Management Association, *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications*, IGI Global, Hershey, PA, 2019; 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; H. Harrison Dinniss, *Cyber Warfare*, nota 13 *supra*, pp. 250–278.

77 H. Harrison Dinniss, *Cyber Warfare*, nota 13 *supra*, p. 148.

78 Guía sobre la participación directa en las hostilidades, nota 14 *supra*, p. 46.

79 L. Zhu, "Competition for International Rules in Cyberspace", nota 2 *supra*, p. 40.

80 M. N. Schmitt, nota 52 *supra*, p. 527.

circunstancias, la prioridad debería ser prevenir el exceso de militarización y reducir el daño innecesario a las personas civiles. Mientras tanto, cabe recordar que, en caso de duda acerca de la condición de una persona, se la considerará como civil[81]. Por consiguiente, interpretar la definición de cibercombatiente con demasiada amplitud sería no solo poco ético, sino también ilícito.

Personas civiles que participan directamente en hostilidades cibernéticas

A diferencia de los combatientes, los civiles no tienen derecho a participar directamente en las hostilidades; los que lo hacen, pierden su protección general contra los peligros de las operaciones militares y pueden ser atacados mientras dure tal participación[82]. Asimismo, pueden ser sometidos a juicio en los tribunales nacionales por sus acciones, incluso si los actos que cometieron eran lícitos conforme al DIH[83]. En el contexto cibernético, la importancia del concepto de los civiles que participan directamente en las hostilidades puede ser incluso mayor, en vista de la tendencia contemporánea de las fuerzas armadas a subcontratar a personas civiles para realizar trabajos que requieren conocimientos informáticos especializados[84].

Como ya se ha dicho, el término "participación directa en las hostilidades" hace referencia a la noción de que, como regla general, los civiles no deben ser objeto de ataques a menos que participen directamente en las hostilidades y mientras dure tal participación[85]. Este concepto también se conoce como la regla sobre la inmunidad de los no combatientes[86]. Al examinar el artículo 51 del PA I, los Estados no definieron con precisión el significado de la frase "participación directa en las hostilidades"[87]. Tanto el caso de los *Asesinatos selectivos*[88] como la *Guía del CICR para interpretar la noción de participación directa en las hostilidades según el derecho internacional humanitario*[89] (Guía sobre la participación directa en las hostilidades) han aportado una contribución valiosa a la interpretación de la noción de la participación directa en las hostilidades. La Guía ha generado un debate considerable y también algunas controversias[90]. Dado que subsiste la

81 PA I, art. 50 1); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 6, p. 27.

82 PA I, art. 51 3); Protocolo adicional 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 (PA II), 1125 UNTS 609, 8 de junio de 1977 (fecha de entrada en vigor: 7 de diciembre de 1978), art. 13 3); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 6, pp. 22-26.

83 H. Harrison Dinniss, "Participants in Conflict", nota 13 *supra*, p. 258.

84 D. Turns, nota 52 *supra*, p. 279.

85 PA I, art. 51 3).

86 Judith G. Gardam, *Non-Combatant Immunity as a Norm of International Law*, Martinus Nijhoff, Dordrecht, 1993.

87 Michael Bothe, Karl Josef Partsch y Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Dordrecht, 1982, pp. 301–304.

88 Alto Tribunal de Justicia de Israel, *Public Committee against Torture in Israel v. Israel et al.*, caso n.° HCJ 769/ 02, Fallo, 11 de diciembre de 2005 (*Asesinatos selectivos*).

89 Guía sobre la participación directa en las hostilidades, nota 14 *supra*, p. 46.

90 "Forum: Direct Participation in Hostilities: Perspectives on the ICRC Interpretive Guidance", *New York University Journal of International Law and Politics*, vol. 42, n.° 3, 2010.

incertidumbre y no está del todo claro cómo pueden aplicarse esas orientaciones en los campos de batalla físicos, lo mismo sucede, y con mayor razón, cuando se trata del campo de batalla virtual[91].

Determinar la participación directa en las hostilidades es de por sí un problema complejo, y hacerlo en el contexto de las hostilidades cibernéticas parece aún más difícil. Como se ha señalado en el caso de los *Asesinatos selectivos*, es posible participar en las hostilidades sin emplear armas para nada[92]. Así pues, aunque los medios de guerra de hoy sean muy distintos de los utilizados en el siglo pasado, sus efectos son básicamente similares. Un sistema de comunicación militar quedará fuera de servicio ya sea que lo inutilice un virus informático o un ataque aéreo.

Para seguir analizando esta cuestión y brindar orientación a los profesionales, la Guía sobre la participación directa en las hostilidades plantea tres elementos acumulativos que, juntos, constituyen un acto de participación directa en las hostilidades. En primer lugar, debe haber probabilidades de que el acto tenga efectos adversos sobre las operaciones militares o sobre la capacidad militar de una parte en un conflicto armado, o bien, de que cause la muerte, heridas o destrucción a las personas o los bienes protegidos contra los ataques directos (umbral de daño). En segundo lugar, debe haber un vínculo causal directo entre el acto y el daño que pueda resultar de ese acto o de la operación militar coordinada de la que el acto constituya parte integrante (causalidad directa). Y en tercer lugar, el propósito específico del acto debe ser causar directamente el umbral exigido de daño en apoyo de una parte en conflicto y en menoscabo de otra (nexo beligerante)[93]. El análisis de los ataques contra las redes informáticas y la explotación de estas lleva a concluir que "[para considerar el acto como participación directa en las hostilidades] podría bastar una interferencia electrónica en las redes informáticas militares, sea mediante ataques contra la red informática o la explotación de la red informática, así como la interceptación de las líneas telefónicas de los altos mandos de la parte adversaria o la transmisión de información o inteligencia táctica en relación con los objetivos de un ataque"[94]. Esta prueba formada por tres partes combinadas, que se centra en el umbral de daño, la causalidad directa y el nexo beligerante, brinda un punto de partida útil para evaluar si un civil realiza actividades de cibercombatiente y en qué medida, y si debería por ende perder su estatuto de persona protegida[95]. Queda abierta la cuestión de si estos criterios son interpretados de igual forma en el contexto cibernético.

El primer elemento, el umbral de daño, se relaciona con la probabilidad objetiva de causar la muerte, heridas o destrucción a las personas o los bienes. Por ejemplo, si el incidente de 2007 en Estonia[96] y el de 2010 provocado por el virus

91 D. Turns, nota 52 *supra*, p. 285.
92 Alto Tribunal de Justicia de Israel, *Asesinatos selectivos*, nota 88 *supra*, párr. 33.
93 Guía sobre la participación directa en las hostilidades, nota 14 *supra*, p. 46.
94 Ibíd., p. 48.
95 Esta prueba de tres partes también fue adoptada para su aplicación a la ciberguerra en el Manual de Tallin 2.0, nota 31 *supra*, pp. 429–430.
96 "Cyber Attacks against Estonia (2007)", nota 15 *supra*; E. Tikk, K. Kaska y L. Vihul, nota 15 *supra*, pp. 14–33.

informático Stuxnet[97] hubiesen sido causados por personas civiles en un conflicto armado internacional, se podría concluir que los ciberataques en el incidente de Estonia no alcanzaron el umbral de daño, en tanto que, en el escenario del virus Stuxnet, sí lo hicieron. Los ciberataques contra la infraestructura digital de Estonia causaron inconveniencias de gran escala porque Estonia es uno de los Estados más "cableados" del mundo, pero nadie murió ni sufrió lesiones, ni se destruyeron ni dañaron bienes, y el hecho de causar meras inconveniencias, por desagradables que estas sean, no basta para alcanzar el umbral de daño[98]. Sin embargo, lo que abarca la "inconveniencia" no está definido, y esta terminología no se utiliza en el ámbito del DIH[99].

Por otra parte, el ciberataque contra las centrifugadoras nucleares iraníes utilizadas para enriquecer uranio causó daños físicos a esos componentes[100]. En este sentido, el Manual de Tallin 2.0 establece que "el acto debe causar el efecto previsto o real de afectar negativamente las operaciones o capacidades militares del adversario o de ocasionar la muerte, daños físicos o la destrucción material de las personas o los bienes protegidos contra ataques directos"[101]. Así pues, conforme al Manual, el umbral de daño se alcanza aun si los actos meramente causan el efecto previsto. Esta interpretación amplía el elemento del umbral de daño, que pasa de la probabilidad objetiva a la intención subjetiva o la probabilidad objetiva, y deja además un amplio margen de discreción en este aspecto.

El segundo elemento, el del vínculo causal directo, debería interpretarse en sentido amplio. Según la Guía sobre la participación directa en las hostilidades, el daño en cuestión debe ser ocasionado en "una sola secuencia causal"[102]. Esa interpretación tan estricta de la causalidad directa sería muy problemática para el caso de las ciberoperaciones, en las que el efecto secundario o indirecto de un acto específico podría ser, de hecho, el propósito del ataque. Consideramos que la "causalidad directa", que abarca tanto la perspectiva subjetiva como la objetiva, es más adecuada para el contexto cibernético: objetivamente, el daño causado por el acto cibernético es la consecuencia normal y natural, y es subjetivamente previsible[103].

Algunos escenarios hipotéticos podrían ayudarnos a comprender mejor la prueba de la causalidad directa en el contexto cibernético. No se consideraría que los civiles contratados para prestar servicios generales de computación y de TI

97 "Stuxnet (2010)", International Cyber Law in Practice: Interactive Toolkit, CCD COE, disponible en: https://cyberlaw.ccdcoe.org/wiki/Stuxnet_(2010); E. Tikk, K. Kaska y L. Vihul, nota 15 *supra*, pp. 66–89.

98 D. Turns, nota 52 *supra*, p. 286.

99 Informe del CICR sobre Desafíos del DIH, 2015, nota 32 *supra*, p. 55.

100 En un informe, se demuestra que, entre finales de 2009 y principios de 2010, fue necesario reemplazar aproximadamente 1 000 centrifugadoras de una planta de enriquecimiento ubicada en Natanz, Irán, lo cual indica que estaban averiadas. David Albright, Paul Brannan y Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, Instituto de Ciencias y Seguridad Internacional, 22 de diciembre de 2010; "Stuxnet (2010)", nota 97 *supra*.

101 Manual de Tallin 2.0, nota 31 *supra*, p. 429.

102 Guía sobre la participación directa en las hostilidades, nota 14 *supra*, p. 53.

103 Bin Cheng, *General Principles of Law as Applied by International Courts and Tribunals*, Cambridge University Press, Cambridge, 1987, p. 181.

participan directamente en las hostilidades si sencillamente cumplen con contratos de servicio, como operar páginas web y gestionar las terminales de acceso del correo electrónico[104], porque la causalidad no es directa, los posibles daños causados no son la consecuencia normal y natural de las acciones efectuadas, y las consecuencias negativas pueden no ser previsibles por las personas que prestan los servicios. Por otro lado, cualquier empleado o contratista contratado específicamente para conducir ciberataques hostiles satisfaría, teóricamente, la prueba de la causalidad directa una vez cometidos los actos.

También cabe intentar aplicar el modelo "cadena de eliminación cibernética" (Cyber Kill Chain)[105], que Lockheed Martin desarrolló para comprobar si la causalidad directa existe en determinadas condiciones. Este modelo es una lista ordenada de los siete pasos comprendidos en un ciberataque: reconocimiento, preparación del ataque, transmisión, explotación, instalación, comando y control, y acción sobre los objetivos[106]. Ofrece un panorama general de cómo un *hacker* puede atacar un objetivo y, aunque no todos los ataques sigan estos pasos, sigue siendo un buen punto de partida. La primera fase es el reconocimiento, que incluye la investigación, identificación y selección de objetivos; a esto sigue la fase de preparación del ataque, que combina el *software* malicioso con un dispositivo de explotación de las vulnerabilidades para crear un "arma". El siguiente paso, la transmisión, consiste en transmitir el arma al objetivo (por ejemplo, mediante llaves USB o adjuntos de correo electrónico); a continuación, el arma tratará de explotar una vulnerabilidad para acceder a la víctima. Hasta el final de la cuarta fase, es difícil determinar si el acto tiene un vínculo causal directo con la consecuencia, puesto que lo que vaya a suceder no es necesariamente previsible para los perpetradores. Sin embargo, cuando se trata de las fases de instalación, comando y control, y acción sobre los objetivos, hay altas probabilidades de que el perpetrador pueda prever lo que sucederá, y el daño causado es la consecuencia natural o normal de los actos en cuestión.

El elemento del nexo beligerante es un tema de hecho, más que de derecho. Es cierto que, para que exista el nexo beligerante, "el propósito específico del acto debe ser causar directamente el umbral exigido de daño en apoyo de una parte en conflicto y en menoscabo de otra"[107]. No es un elemento similar a la *mens rea*. Lo que importa es el propósito del acto, que debe concebirse objetivamente para causar daño en forma directa. Esto permite inferir que los actos hostiles ejecutados bajo coerción o sin conocimiento no satisfacen el elemento del nexo beligerante. Teniendo cuenta que los ataques de *botnet* ocurren con frecuencia, cabe señalar que debería haber una excepción a la pérdida de inmunidad si un ordenador civil es jaqueado por un *botnet* y el usuario relevante no está al tanto del virus ni del

104 V. Emily Crawford, *Virtual Battlegrounds: Direct Participation in Cyber Warfare*, Sydney Law School Research Paper n.° 12/10, 8 de febrero de 2012, disponible en: https://ssrn.com/abstract=2001794.

105 105 V. Lockheed Martin, "Gaining the Advantage, Applying Cyber Kill Chain Methodology to Network Defense", 2015, disponible en: www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/ cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

106 Ibíd.

107 Guía sobre la participación directa en las hostilidades, nota 14 *supra*, p. 46.

ataque. En este caso, no debería considerarse que el usuario relevante realiza una acción; por ende, ante la falta de una acción manifiesta, no se cumpliría el elemento del nexo beligerante.

Si un civil meramente elabora un programa malicioso que causaría la salida de servicio de una infraestructura crítica, esa acción no debería considerarse como participación directa en hostilidades cibernéticas, dado que normalmente no satisfaría los tres elementos y, de todos modos, la causalidad sería demasiado remota. Del mismo modo, los científicos y los expertos civiles en armas se consideran, por lo general, protegidos contra los ataques directos[108]. Si el civil envía el programa autoescrito malicioso que formuló a la fuerza armada que apoya, esa acción todavía no constituye participación directa en las hostilidades; este caso es similar al del transporte de armas. Pero si ese programa malicioso está destinado a realizar un acto hostil específico, esa acción se transformaría en parte integrante de una ciberoperación militar y se cumpliría el requisito de la causalidad directa. Cuando un civil, independientemente de que se halle bajo contrato con las fuerzas armadas o actúe en forma unilateral, ejecuta un programa malicioso, probablemente se cumplirían los criterios y perdería la protección, convirtiéndose así en un objetivo lícito, al menos mientras el programa se estuviese ejecutando.

El artículo 51 del PA I también fija el marco temporal de los actos específicos que constituyen participación directa en las hostilidades: los civiles que participan directamente en las hostilidades pierden la protección contra los ataques directos "mientras dure tal participación"[109]. Una vez transcurrido el lapso de la participación, se restablece la protección otorgada a los civiles. Esto debería distinguirse de las normas establecidas para los miembros de los brazos armados de los grupos armados organizados y para quienes pertenecen a una parte en el conflicto; esas personas dejan de ser civiles y, por ende, pierden la protección contra los ataques directos mientras asuman su función continua de combate, en tanto que los civiles pierden su protección mientras dure la comisión de actos específicos que equivalgan a la participación directa en las hostilidades[110].

Una cuestión de particular importancia en el contexto cibernético es la forma de calcular el marco temporal de la pérdida de protección de los civiles cuando se producen ciberoperaciones reiteradas en un período relativamente concentrado. Si un civil ejecuta repetidas veces ciberoperaciones que podrían constituir actos de participación directa en las hostilidades, ¿cuál es el marco temporal o el período durante el cual ese civil puede ser objeto de ataque?

108 CICR, *Fourth Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report*, Ginebra, 27–28 de noviembre de 2006, p. 48. Los autores de este artículo señalan que se expresaron algunas dudas sobre si esta evaluación puede sostenerse en situaciones extremas, esto es, cuando los conocimientos de una persona civil particular tienen un valor excepcional y posiblemente decisivo para el resultado de un conflicto armado, como fue el caso de los expertos en armas nucleares durante la Segunda Guerra Mundial.

109 PA I, art. 51 3); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 6, pp. 22–27.

110 Guía sobre la participación directa en las hostilidades, nota 14 *supra*, p. 73.

En un campo de batalla tradicional, la Guía sobre la participación directa en las hostilidades adopta la posición de tratar esas acciones por separado[111], pero en el caso de los *Asesinatos selectivos* se expresa preocupación acerca del fenómeno del "vaivén" en este sentido[112]. Según la Guía sobre la participación directa en las hostilidades, el "vaivén" de la protección civil impide atacar a civiles que, en las circunstancias, no representan una amenaza militar[113]. Como el concepto de la participación directa en las hostilidades se refiere a actos hostiles especificos, el DIH restablece la protección del civil contra ataques directos cada vez que deja de participar en un acto hostil[114]. Teniendo en cuenta que numerosas ciberoperaciones, como los ataques DDoS (denegación de servicio distribuido), se realizan múltiples veces dentro de un período, esta delimitación tan estricta del tiempo no tiene mucho sentido desde el punto de vista operacional. Sin embargo, los autores también son escépticos acerca del cálculo del período que media entre la primera operación hasta el fin de toda la actividad intermitente. El motivo es que los civiles que participan directamente en las hostilidades no son iguales a los miembros de los grupos militares organizados: aunque ambos pueden ser atacados, son dos tipos diferentes de objetivos humanos. Como ya se ha dicho, los miembros de los grupos militares organizados pueden ser objeto de ataques durante el lapso de su función continua de combate, pero los civiles que participan directamente en las hostilidades pueden ser atacados únicamente mientras duren sus actos específicos. "El civil que participa directamente en las hostilidades por única vez o esporádicamente, y que luego deja esa actividad, tiene derecho a la protección contra ataques"[115]. Por lo tanto, suponiendo que un civil realiza ataques cibernéticos reiterados, si todo el período de tiempo (desde el comienzo del primer ataque hasta el final del último) se calcula en forma continua como el período durante el cual ese civil puede ser atacado, en cierto sentido se estaría aplicando a ese civil que participa directamente en las hostilidades la norma de los combatientes (función continua de combate), porque se consideraría que los intervalos entre ataques son períodos en que también se lo podría atacar. En sentido estricto, los civiles que participan directamente en las hostilidades pierden su protección debido a sus actos específicos y no se considera que hayan cometido acciones hostiles en los intervalos. Por otra parte, el civil que se ha sumado a una organización militar y lleva a cabo una cadena de actos hostiles, con breves períodos de descanso en el medio, pierde su inmunidad contra los ataques durante todo el período de su actividad. Para esa persona, el descanso entre actos hostiles no es más que la preparación para el siguiente acto hostil[116].

111 Ibíd., pp. 70–71.

112 Alto Tribunal de Justicia de Israel, *Asesinatos selectivos*, nota 88 *supra*, párr. 40.

113 Guía sobre la participación directa en las hostilidades, nota 14 *supra*, pp. 70–71.

114 V. la descripción de la participación directa en hostilidades como potencialmente "intermitente y discontinua", en TPIR, *The Prosecutor v. Strugar*, caso n.° IT-01-42-A, Fallo (Sala de Apelaciones), 17 de julio de 2008, párr. 178.

115 Tribunal Supremo de Israel, *Public Committee against Torture in Israel v. Government of Israel*, caso n.° HCJ 769/02, 13 de diciembre de 2006, párr. 39.

116 Ibíd., párr. 39; Daniel Statman, "Targeted Killing", *Theoretical Inquiries in Law*, vol. 5, n.° 1, 2004, pp. 179, 195.

Como conclusión, al interpretar la participación directa en las hostilidades, el umbral de daño exige una probabilidad objetiva, no la mera intención subjetiva; el nexo beligerante debe confirmarse y el vínculo causal debe ser directo. El marco temporal es sumamente importante, pero muy difícil de establecer. Hasta ahora, ante la falta de jurisprudencia internacional sobre el tema, el esclarecimiento del concepto sigue siendo un tema para los estudiosos, la futura práctica de los Estados y las decisiones judiciales.

El principio de distinción en relación con los objetivos no humanos en la guerra cibernética

Todos los objetivos no humanos[117] pueden dividirse en dos categorías: objetivos militares y bienes de carácter civil. Los bienes de carácter civil son todos los bienes que no son objetivos militares[118]. Solo pueden ser atacados los objetivos militares[119]. En esta parte del artículo, examinaremos qué puede ser objeto de un ataque lícito aplicando el principio de distinción en la esfera cibernética, es decir, qué constituye un objetivo militar en el contexto cibernético. Es preocupante que, en el ciberespacio, casi todo exhiba un potencial militar enorme, y la cuestión de los bienes de doble uso es un factor más importante que nunca en el proceso de selección de los objetivos. Debido a la creciente importancia de los datos en un conflicto armado cibernético, también se examinará la cuestión de si los propios datos pueden considerarse un objetivo militar.

La noción de "objetivo militar": dos elementos equivalentes

La definición ampliamente aceptada de todos los objetivos militares no humanos es la siguiente: 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[120].

La noción de "objetivo militar" es crítica, dado que determina en forma directa lo que puede o no puede atacarse según el principio de distinción. En realidad, el término "objetivo militar" se ha interpretado en formas muy distintas. Algunos opinan que significa la capacidad de librar o de mantener la guerra para la acción militar conforme a la definición contenida en el artículo 52 2) del PA I y que incluye los objetivos que "en forma indirecta pero efectiva apoyan y sostienen

117 Los autores de este artículo tratan de no utilizar el término "objetos" aquí, porque la cuestión de si existen objetivos no humanos que no son "objetos" se examinará en los párrafos que siguen.

118 PA I, art. 52 1); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 9, pp. 37–38.

119 PA I, art. 52 2); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 7, pp. 29–33.

120 PA I, Art 52 2); Estudio del CICR sobre DIH consuetudinario, nota 12 *supra*, norma 8, pp. 34–36; Jacob Kellenberger, "International Humanitarian Law at the Beginning of the 21st Century", declaración ante la 26.ª Mesa Redonda sobre problemas actuales del derecho internacional humanitario, San Remo, 5–7 de septiembre de 2002.

la capacidad de guerra del enemigo"[121]. En términos prácticos, el cumplimiento con el primer criterio de la "contribución efectiva" por lo general producirá la ventaja requerida por el segundo criterio de la "ventaja militar definida"[122]. Otros argumentan que existe un objetivo militar en el sentido del Protocolo solo cuando estos dos elementos están presentes en forma acumulativa[123]. En otras palabras, la prueba para determinar el estatuto militar de un objeto es doble y los dos requisitos son equivalentes[124].

Los autores del presente artículo discrepan de la opinión de que la "contribución efectiva" incluye los objetivos que "en forma indirecta pero efectiva apoyan y sostienen la capacidad de guerra del enemigo", especialmente en la esfera cibernética. Esta interpretación es demasiado amplia y contradice la filosofía que sustenta la limitación de los objetivos militares: en efecto, al caracterizar a la contribución como "efectiva" y a la ventaja como "definida", los redactores del PA I trataron de evitar una interpretación muy amplia de lo que constituye un objetivo militar[125]. Y, en el contexto de la guerra cibernética, la interpretación amplia sembraría incluso más confusión en torno a la distinción[126], dado que casi todo tiene un potencial militar en el ciberespacio; si el apoyo indirecto contara como contribución efectiva, la interpretación sería casi ilimitada, puesto que permitiría que "cualquiera de las funciones informáticas del adversario que influyen en su capacidad de luchar sea un objetivo lícito"[127]. Por lo tanto, no concuerda con el objeto y el propósito del artículo 52 2) del PA I.

Así pues, la definición de objetivo militar debería contener dos elementos de igual importancia: la contribución efectiva y la ventaja definida. El cumplimiento del primer elemento no lleva automáticamente al cumplimiento del segundo, puesto que estos dos elementos son independientes. El elemento de la ventaja definida se analizó en profundidad en el momento de redactar el PA I. Los adjetivos considerados y rechazados fueron, entre otros, "preciso" (*distinct*), "directo" (*direct*), "claro" (*net*), "inmediato" (*immediat*), "obvio" (*évident*), "específico" (*spécifique*), y "sustancial" (*substantiel*)[128]. Claramente, la palabra "definido" tiene su propio valor y no debe dejarse de lado: la ventaja debe ser definida y concreta[129]. Las formas

121 Departamento de Defensa, nota 41 *supra*, p. 210; Charles J. Dunlap, "The End of Innocence: Rethinking Non-Combatancy in the Post-Kosovo Era", *Strategic Review*, vol. 9, 2000, p. 17; Departamento de Marina y Departamento de Seguridad Interior de EE.UU., *The Commander's Handbook on the Law of Naval Operations*, julio de 2007, párr. 8.2. También hay opiniones contrarias, como la de Laurent Gisel, "The Relevance of Revenue-Generating Objects in Relation to The Notion of Military Objective", en CICR, *The Additional Protocols at 40: Achievements and Challenges*, 18.° Coloquio de Brujas, 19–20 de octubre de 2017.

122 Programa de Política Humanitaria e Investigación de Conflictos de la Universidad de Harvard, *HPCR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge, MA, 2010, p. 49.

123 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds.), *Comentario de los Protocolos Adicionales,* CICR, Ginebra, 1987 (Comentario de los PA, del CICR), párr. 2018.

124 E. Mavropoulou, nota 51 *supra*, p. 44.

125 Marco Sassòli, "Military Objectives", en *Max Planck Encyclopedia of Public International Law*, 2015, párr. 7.

126 J. Kelsey, nota 33 *supra*, p. 1440.

127 M. Roscini, nota 65 *supra*, p. 186.

128 Comentario de los PA, del CICR, nota 123 *supra*, párr. 2019.

129 Robert Kolb y Richard Hyde, *An Introduction to the International Law of Armed Conflicts*, Hart Publishing, Oxford, 2008, pp. 60, 131.

potenciales e indeterminadas de la ventaja no son aceptables, y tampoco lo son las políticas[130]. En otras palabras, está prohibido lanzar un ataque que solamente ofrezca ventajas potenciales o indeterminadas[131].

Estos dos elementos, la contribución efectiva y la ventaja militar definida, también son equivalentes. A menudo, es complicado identificar la ventaja militar esperada de un ataque determinado, sobre todo en el contexto cibernético, donde puede resultar difícil medir los efectos de una ciberoperación[132]. En la esfera cibernética, donde los militares usan para su actividad militar la misma infraestructura informática que la población civil, el segundo requisito de la definición se torna más inclusivo aún y hay que ser prudente antes de llegar a una conclusión radical que subestime gravemente la importancia del segundo elemento[133]. El ciberespacio es relativamente resiliente en comparación con otros objetivos. En el caso de un ataque contra infraestructuras informáticas tales como las redes de comunicación, el flujo de datos es tan flexible que, aunque ciertas vías de comunicación sean destruidas por el ciberataque, los paquetes de datos dispondrán de otras rutas posibles para alcanzar el destino previsto[134]. En este caso, la destrucción parcial de la red podría contribuir efectivamente a la acción militar pero, en última instancia, difícilmente ofrezca una ventaja definida. Por ello, el juicio sobre una ventaja militar definida es complejo y no se satisface automáticamente una vez cumplido el elemento de la contribución efectiva.

En el contexto cibernético, es difícil, si no imposible, medir y cuantificar la ventaja militar definida. Después del incidente causado por el virus Stuxnet, mientras Irán negaba que el ataque hubiese causado daños importantes, el Organismo Internacional de Energía Atómica informó de que Irán había dejado de introducir uranio en miles de centrifugadoras ubicadas en Natanz. Nadie conoce las consecuencias causadas por el virus Stuxnet para el programa nuclear iraní, y todavía no está claro si la decisión de dejar de operar las centrifugadoras de Nantanz se debió al virus o a fallas técnicas inherentes a los equipos[135].

Lo que es importante destacar en el contexto del ciberespacio es que el requisito de identificar una ventaja militar definida asociada con el ataque contra un objetivo particular surge con mayor frecuencia cuando se trata de bienes de doble uso. Una instalación puede servir para fines solo civiles o solo militares, pero también es posible que sirva para ambos fines al mismo tiempo, lo que haría de ella un bien de doble uso[136]. La infraestructura esencial como los puentes, las plantas

130 Comentario de los PA, del CICR, nota 123 *supra*, párr. 2024.
131 Ibíd., párrs. 2024-2025.
132 M. Roscini, nota 65 *supra*, p. 188.
133 R. Geiss y H. Lahmann, nota 34 *supra*, p. 388.
134 Ibíd.
135 Marco Roscini, "Military Objectives in Cyber Warfare", en Mariarosaria Taddeo y Luciano Floridi (ed.), *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence of Excellence Initiative*, Springer, Cham, 2017, p. 108; Katharina Ziolkowski, *Stuxnet – Legal Considerations*, CCD COE, Tallin, 2012, p. 5, disponible en: https://ccdcoe.org/uploads/2018/10/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf.
136 Dominik Steiger, "Civilian Objects", en *Max Planck Encyclopedia of Public International Law*, 2011, párr. 12.

de generación eléctrica y las refinerías de petróleo también se pueden explotar con fines civiles y militares simultáneamente[137].

La diferencia fundamental de la guerra cibernética reside en la naturaleza *sui generis* del ciberespacio, esto es, la "interconectividad sistémica de la infraestructura civil y militar"[138]. Por ejemplo, se estima que aproximadamente el 98 % de las comunicaciones del gobierno de EE. UU.[139] utilizan redes de propiedad de civiles y operadas por civiles[140]. Todos los satélites, enrutadores, cables, servidores e incluso los ordenadores civiles son dispositivos informáticos de doble uso. La realidad es que "cada componente de la infraestructura informática, cada bit de capacidad de memoria tiene un potencial militar" y esto difumina la línea que separa a los bienes de carácter civil de los objetivos militares[141]. Zhu Lixin, un profesor chino de la Universidad de Ingeniería de la Fuerza Aérea, señaló que las fuerzas armadas estadounidenses consideran muy importante construir sistemas de inteligencia, reconocimiento y vigilancia resilientes y respaldados por dispositivos de inteligencia artificial y de informática cuántica, y que adquieren activamente armas tales como bombas inteligentes de diámetro pequeño, sistemas de enjambre no tripulados, armas hipersónicas y armas de energía dirigida para garantizar la letalidad. Los denominados sistemas de inteligencia, reconocimiento y vigilancia requieren máquinas costosas, como ordenadores cuánticos, satélites y sistemas de inteligencia artificial, muchos de los cuales sirven tanto para fines militares como civiles[142]. Pese a todos estos desafíos, para el derecho, los bienes de doble uso no conforman una categoría separada; también deben cumplir la prueba de dos partes del artículo 52 2) del PA I. La idea de que internet en sí pueda constituir un objetivo militar probablemente no sea sostenible, porque el uso de códigos militares a través de internet podría efectuar alguna contribución militar, pero esta difícilmente sería efectiva, y no justificaría un ataque porque sería muy improbable que la mera alteración de sus operaciones ofreciese la "ventaja militar definida" necesaria[143]. En todo caso, un ataque contra la red entera violaría el principio de proporcionalidad[144] y, por consiguiente, no sería lícito en modo alguno.

Además, como el concepto de doble uso no es una innovación de la ciberguerra, el PA I brinda una presunción notable para la *lex scripta:* en caso de duda sobre el carácter militar de un bien, se presumirá que no se utiliza con fines militares[145]. La norma 102 del Manual de Tallin 2.0 también establece que "[e]n caso de duda

137 Ibíd.

138 R. Geiss y H. Lahmann, nota 34 *supra*, p. 385.

139 Para evitar ambigüedades, en términos de las cifras señaladas, cabe recordar que no todas las comunicaciones de los gobiernos equivalen a comunicaciones militares o a objetivos militares.

140 Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks", *Texas Law Review*, vol. 88, n.° 7, 2010, pp. 1522, 1542.

141 R. Geiss y H. Lahmann, nota 34 *supra*, p. 388.

142 L. Zhu, "Competition for International Rules in Cyberspace", nota 2 *supra*, p. 40.

143 Tribunal Penal Internacional para ex Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, 13 de junio de 2000, párr. 75.

144 PA I, art. 51 5) b), 57 2) iii).

145 Ibíd., art. 52 3).

acerca de si un objeto y su infraestructura cibernética asociada que normalmente se dedican a fines civiles se usan para prestar una contribución efectiva a la acción militar, la determinación de la existencia de ese uso solo podrá hacerse tras un examen minucioso"[146].

Determinar si los datos se encuadran en el ámbito de los objetivos militares

En muchas sociedades, los datos han pasado a ser una de las piedras angulares de la vida. Durante un conflicto armado, la manipulación de los datos para causar daños físicos sin duda exige aplicar las restricciones del DIH, pero la cuestión de si los datos en sí mismos constituyen un objetivo militar también es objeto de controversia. Los ciberataques se pueden dirigir contra los datos sin causar efectos físicos, como aquellos que afectan los sistemas financieros civiles. Hay quienes opinan que solo un objeto material y tangible puede ser un objetivo militar y constituir un objetivo lícito para los ataques[147]. En el Manual de Tallin 2.0, solo unos pocos expertos opinaron que ciertos datos deberían ser considerados objetos y así constituir objetivos militares[148]. Es importante ilustrar la relación entre los términos "objetivo militar" y "objeto". Para decirlo en pocas palabras, citaremos el texto del artículo 52 2) del PA I: "[e]n lo que respecta a los *bienes*, los *objetivos militares* se limitan a aquellos *objetos* que...". Esto significa que un objetivo militar es un objeto que satisface ciertos criterios. El punto en discusión es si los datos *per se* pueden constituir un objeto. Hay dos motivos principales que llevan a dudar de que los datos puedan constituir un objetivo militar y ambos se relacionan con la noción de "objeto". Primero, el carácter intangible de los datos no encaja en el significado habitual de "objeto". Segundo, el Comentario del CICR sobre los Protocolos adicionales observa que "un objeto se caracteriza por ser algo visible y tangible"[149]. Por lo tanto, los datos obviamente no reúnen las condiciones necesarias para ser considerados "objetos". Algunos estudiosos argumentan que los datos deberían tratarse como objetos[150]. Su argumento es que las ciberoperaciones contra los datos civiles son, en el plano fáctico, ataques ilegales contra objetivos civiles. Es importante destacar que, en opinión de esos estudiosos, todo efecto, directo o indirecto, causado por acciones dirigidas contra objetivos cibernéticos lícitos que afecte los datos civiles debe medirse según el principio del

146 Manual de Tallin 2.0, nota 31 *supra*, p. 448.

147 Yoram Dinstein, "Legitimate Military Objectives under the Current *Jus in Bello*", *International Law Studies*, vol. 78, 2002, p. 142.

148 Manual de Tallin 2.0, nota 31 *supra*, norma 100, p. 437; M. N. Schmitt, nota 30 *supra*, p. 269; Michael N. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack", *International Review of the Red Cross*, vol. 96, n.° 893, 2015, p. 200.

149 Comentario de los PA, del CICR, nota 123 *supra*, párrs. 2007, 2008.

150 V., por ejemplo, Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, vol. 48, n.° 1, 2015; documento del CICR sobre DIH y Ciberoperaciones, nota 32 *supra*, p. 8; Informe del CICR sobre los Desafíos del DIH de 2015, nota 32 *supra*, pp. 53–55; CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos: Reafirmar el compromiso con la protección en los conflictos armados en el marco del 70.° aniversario de los Convenios de Ginebra*, Ginebra, 2019 (Informe del CICR sobre los Desafíos del DIH de 2019), p. 25.

análisis de proporcionalidad y estar sujeto al requisito de reducir al mínimo los daños civiles indirectos[151]. La ventaja de esta interpretación es que protege a las poblaciones civiles contra los posibles efectos negativos de las ciberoperaciones, pero es demasiado amplia e inclusiva, y hasta incluiría ciertas ciberoperaciones, como las operaciones psicológicas, que algunos países ya están ejecutando en forma sistemática[152]. En síntesis, estas críticas y dudas sobre la posición de la mayoría de expertos en el Manual de Tallin 2.0 se centran en la exclusión de los datos de la protección prevista por la norma sobre la selección de objetivos fijada en el PA I. Según este punto de vista, hasta las ciberoperaciones sin consecuencias físicas deberían someterse, como mínimo, a la prueba del principio de proporcionalidad y precaución[153] siempre que involucren daños o destrucción de datos, incluso si solo presentan riesgos potenciales para la población civil[154]. Otros académicos no coinciden con esta opinión y sugieren que los datos deben considerarse un objetivo militar solo una vez que satisfacen el criterio. Para ellos, interpretar los datos como un objeto "ampliaría en gran medida la clase de objetivos permisibles en la guerra"[155] y es contrario al objetivo y a la finalidad de fortalecer la protección de la población civil en situaciones de conflicto armado. Asimismo, la interpretación del significado habitual del término "objeto" es discutible. En los seis idiomas auténticos del PA I hay discrepancias provenientes de las traducciones[156], incluso en francés y en español. En este último, el término "*un bien*" se puede traducir al inglés como "*a good*" o "*a property*", y en francés, el término jurídico comprende tanto los objetos tangibles como intangibles[157]. De hecho, en el contexto chino, el término "objeto"[158] generalmente se refiere a cosas compuestas por materiales que ocupan una cierta cantidad de espacio[159] y, por lo tanto, los datos intangibles no cuentan.

151 Michael N. Schmitt, "International Cyber Norms: Reflections on the Path Ahead", *Netherlands Military Law Review*, 17 de septiembre de 2018, disponible en: http://puc.overheid.nl/doc/PUC_248171_11.

152 Ibíd.; Michael N. Schmitt, "Notion of Objects during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision", *Israel Law Review*, vol. 48, n.° 1, 2015.

153 Como se señala en Y. Dinstein, nota 46 *supra*, pp. 164–174, el principio de precaución incluye tanto las precauciones activas en el ataque (PA I, art. 57) como la precaución pasiva (PA I, art. 58). Las precauciones activas exigen: a) hacer todo lo que sea factible para verificar que los objetivos que se proyecta atacar son lícitos [y] b) tomar todas las precauciones factibles en la elección de los medios y métodos de ataque para evitar o, al menos, reducir los daños a la población civil y a los bienes de carácter civil. La precaución pasiva exige a las partes beligerantes, "hasta donde sea factible", a) esforzarse por alejar de la proximidad de objetivos militares a la población civil, las personas civiles y los bienes de carácter civil que se encuentren bajo su control; b) evitar situar objetivos militares en el interior o en las proximidades de zonas densamente pobladas; y c) tomar las demás precauciones necesarias para proteger contra los peligros resultantes de operaciones militares a la población civil, las personas civiles y los bienes de carácter civil.

154 Paul Ducheine y Terry Gill, "From Cyber Operations to Effects: Some Targeting Issues", *Netherlands Military Law Review*, 17 de septiembre de 2018, disponible en: https://puc.overheid.nl/doc/PUC_248377_11/1.

155 K. Mačák, nota 150 *supra*.

156 PA I, art. 102: "El original del presente Protocolo, cuyos textos árabe, chino, español, francés, inglés y ruso son igualmente auténticos, (...)".

157 K. Mačák, nota 150 *supra*.

158 La versión china del PA I emplea el término "物体". V. www.icrc.org/zh/doc/assets/files/other/mt_070116_prot1_c.pdf.

159 "由物质构成的，占有一定空间的个体". V. 当代汉语词典，上海辞书出版*±，2001 (*Contemporary Chinese Dictionary*, Shanghai Dictionary Publishing House, 2001); 现代汉语大词典, 下册, 上海辞书出

Algunos estudiosos también opinan que los datos deberían dividirse en dos categorías: datos "de nivel operativo" y datos "de nivel de contenido"[160]. Según esa opinión, los datos de nivel de contenido, como el texto de este artículo o el contenido de las bases de datos médicas, los catálogos de bibliotecas y otros similares, están mayormente excluidos del ámbito de los objetivos militares[161]. Los datos de nivel operativo, esto es, los tipos de datos que dotan al *hardware* de funcionalidad y de capacidad de ejecutar las tareas requeridas, se considerarían un objetivo militar[162].

Lamentablemente, la cuestión de si los datos civiles deberían considerarse bienes de carácter civil y, por consiguiente, gozar de protección en virtud del DIH, parece no haber recibido mucha atención por parte de los académicos chinos. Zhu Yanxin, profesor adjunto de la Facultad de Ciencias Políticas de la Universidad de Defensa Nacional PLA, opina que los datos podrían definirse como objetivo militar aun sin ser objetos[163]. Afirma que los datos son un objetivo militar formado por "no objetos"[164]. Este argumento se basa en el texto que figura al principio de la segunda frase del artículo 52 del PA I:

> Los ataques se limitarán estrictamente a los 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[165].

La formulación literal de la disposición claramente permite la existencia de objetivos militares que son objetos y de objetivos militares que no son objetos.

Las opiniones de los autores del presente artículo sobre este tema coinciden básicamente con el documento de posición del CICR de 2019[166]. Ciertos datos, al menos los que son esencialmente civiles[167], deberían corresponder al ámbito de los bienes de carácter civil, dado que el significado común del término "objeto" está evolucionando y que esto respondería al objetivo y a la finalidad de los Convenios de Ginebra y de sus Protocolos adicionales. El término "objeto" no

版*±, 2009 (*Modern Chinese Dictionary*, vol. 2, Shanghai Dictionary Publishing House, 2009);新华汉语词典, 崇文书局, 2006 (*Xinhua Chinese Dictionary*, Chongwen Publishing House, 2006); 近现代词源, 上海辞书出版*±, 2010 (*Etymology of Modern Times*, Shanghai Dictionary Publishing House, 2010).

160 Heather Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review*, vol. 48, n.° 1, 2015, p. 41.

161 Ibíd.

162 Ibíd.

163 朱雁新, 数据的性质: 对军事目标法律含义的重新解读, 载黄志雄主编, 网络空间国际规则新动向: "塔林手册2.0版" 研究文集, *±会科学文献出版*±, 2019: 410–413 (Yanxin Zhu, "The Nature of Data: A Reinterpretation of the Legal Meaning of Military Objective", en Zhixiong Huang (ed.), *New Trends in International Rules for Cyberspace: Collection of Papers on Tallinn Manual 2.0*, Social Sciences Academic Press, China, 2019, pp. 410–413, disponible solo en chino).

164 Ibíd., p. 410.

165 PA I, art. 52 2).

166 CICR, DIH y Ciberoperaciones, nota 32 *supra*, p. 10.

167 Ibíd., p. 10.

excluye necesariamente a los datos del alcance de los objetivos militares; se debe tener en cuenta que el significado habitual de "objeto" no debe limitarse al que tenía cuando se adoptó el tratado y que seguirá evolucionando con el tiempo[168]. La interpretación de un tratado que se basa exclusivamente en un enfoque textual deja de lado otros métodos de interpretación consagrados en la Convención de Viena sobre el derecho de los tratados[169]. Por ejemplo, desde el punto de vista del objeto y la finalidad del PA I, la idea de que "la eliminación o la adulteración de esos datos esenciales de carácter civil no estarían prohibidas por el DIH en un mundo tan dependiente de los datos parece difícil de conciliar con el objeto y fin de esta rama del derecho"[170]. Afirmar que el reemplazo de archivos y documentos en papel por datos digitales no debe disminuir la protección que les confiere el DIH[171] es un argumento convincente. Si los datos no son bienes ni objetos, las ciberoperaciones contra los datos de carácter civil caen en un vacío del DIH y las ciberoperaciones que causan daños graves a la vida de la población civil no están prohibidas por el derecho[172].

El Manual de Tallin 2.0 equipara a los objetivos militares con objetos. Por ejemplo, la definición de objetivo militar propuesta en la norma 100 no deja margen alguno para los "no objetos": "Los objetivos militares son los objetos que..."[173]. La posición de que los datos podrían constituir un objetivo militar aun sin ser objetos es cuestionable por dos razones principales. En primer lugar, esta idea entraría en conflicto con la tradicional dicotomía personas-objetos, la cual, en lo tocante a la redacción de estas disposiciones, parece ser correcta; los Estados hasta han rechazado una tercera categoría, que es la de "lugares"[174]. En segundo lugar, no quedaría ningún criterio válido para evaluar si un conjunto de datos específico constituye un objetivo militar[175]. La dicotomía personas-objetos proporciona el criterio de la contribución efectiva y de la ventaja definida para entidades no vivientes, mientras que para los objetivos vivientes hay otros requisitos[176]. Si los datos no son objetos, ello llevaría a la posición ilógica de que los datos se deben evaluar sobre la misma base que los objetivos vivientes. Por lo tanto, la idea de que los datos se pueden definir como objetivos militares sin ser objetos no resulta convincente.

168 K. Mačák, nota 150 *supra*.
169 V. Convención de Viena sobre el derecho de los tratados, 1155 UNTS 331, 23 de mayo de 1969 (fecha de entrada en vigor: 27 de enero de 1980), art. 31(3)(a).
170 CICR, DIH y Ciberoperaciones, nota 32 *supra*, p. 10.
171 CICR, Informe del CICR sobre Desafíos del DIH de 2019, nota 150 *supra*, p. 25.
172 V. M. N. Schmitt, nota 151 *supra*.
173 Manual de Tallin 2.0, nota 31 *supra*, p. 435.
174 M. Bothe, K. J. Partsch y W. A. Solf, nota 87 *supra*, pp. 301–304.
175 K. Mačák, nota 150 *supra*.
176 PA I, art. 52 2).

Conclusión

El aforismo de Cicerón "Cuando las armas hablan, las leyes callan" (*silent enim legis inter arma*) no refleja la realidad moderna. Pese a todas las dificultades, el principio de distinción del *jus in bello* es aplicable a la ciberguerra. Debido a la ausencia de disposiciones convencionales y de decisiones judiciales específicas sobre el ámbito cibernético, la interpretación del derecho existente se basa en los debates académicos disponibles y en la limitada práctica de los Estados. Existe la necesidad de un esclarecimiento general y de un mayor desarrollo del principio de distinción en el contexto cibernético; por ejemplo, las definiciones de "objetivo militar cibernético" y de "cibercombatiente" siguen siendo objeto de controversia. Como señaló el secretario general de las Naciones Unidas en el Foro Económico Mundial, "es preciso alcanzar un consenso mínimo en el mundo acerca de cómo integrar estas nuevas tecnologías en las leyes de la guerra que se definieron hace décadas y en un contexto completamente distinto"[177].

Hasta ahora, el gobierno chino no se ha manifestado con claridad acerca de la aplicación del DIH en el ciberespacio. Por cierto, hay algunos artículos académicos chinos que analizan la aplicación del DIH en el ciberespacio, pero el examen del principio de distinción en el ciberespacio adolece de limitaciones tanto en su extensión como en su profundidad académica. En comparación con Occidente, las investigaciones de los estudiosos chinos acerca de esta cuestión siguen en una etapa relativamente preliminar. En la actualidad, no hay deconstrucciones ni aclaraciones específicas sobre la aplicación del principio de distinción en el ciberespacio que hayan sido elaboradas por académicos chinos.

Pese a los posibles problemas técnicos y a las incertidumbres que surgen en relación con esta cuestión, el principio de distinción debería aplicarse al ciberespacio. Este principio también debería reexaminarse y esclarecerse para prevenir la militarización excesiva y fortalecer la protección de los intereses de las poblaciones civiles. En lo que respecta a los objetivos humanos, los elementos que determinan el estatuto del combatiente definidos en el derecho internacional consuetudinario y en los tratados de DIH relevantes no resultan adecuados para el campo de batalla digital pero, aun así, los cibercombatientes están obligados a distinguirse de las personas civiles. Al aplicar el principio de distinción, los autores de este artículo afirman que es más lógico centrarse en los elementos sustantivos que en los elementos formales tales como llevar las armas a la vista o tener un signo distintivo fijo que sea reconocible a distancia. Al interpretar la "participación directa en las hostilidades", el umbral de daño exige una probabilidad objetiva, no la mera intención subjetiva; el nexo beligerante debería confirmarse y el vínculo causal debería ser, como mínimo, directo. La aplicación por analogía del modelo de la "cadena de eliminación cibernética" nos ayuda a comprender todo el proceso de la participación directa en las hostilidades durante la ciberguerra. En

177 Foro Económico Mundial, "António Guterres: Read the UN Secretary-General's Davos Speech in Full", 24 de enero de 2019, disponible en: www.weforum.org/agenda/2019/01/these-are-the-global-priorities-and-risks-for-the-future-according-to-antonio-guterres/.

cuanto a los objetivos no humanos, todos los objetivos militares deben satisfacer acumulativamente tanto el criterio de la "contribución efectiva" y de la "ventaja militar definida", que son igualmente indispensables. Los mismos requisitos se aplican a los objetos de doble uso. Con respecto al carácter de los datos, el significado habitual de "objeto" es discutible. Hay discrepancias de traducción en los seis idiomas auténticos del PA I: en francés, el término jurídico comprende tanto los objetos tangibles como intangibles, mientras que en el contexto chino, el término generalmente se refiere a cosas compuestas por materiales que ocupan una cierta cantidad de espacio y, por lo tanto, los datos intangibles no cuentan. Además, un académico chino opina que ciertos datos pertenecen a la categoría de los objetivos militares formada por los "no objetos".

En el siglo XXI, la popularización de la tecnología de internet trajo consigo cambios inéditos. El futuro del DIH en el ciberespacio sigue en manos de los Estados, particularmente porque ellos interpretan las disposiciones y normas vigentes. La guerra, la tecnología y el *jus in bello* se han entremezclado en forma sustancial y han interactuado entre sí desde los comienzos de los conflictos humanos organizados, pero el derecho se ha visto constantemente forzado a adaptarse y siempre parece estar "una guerra detrás de la realidad"[178]. Por lo tanto, al encarar la evolución de la tecnología y de la ciencia, es preferible interpretar los tratados internacionales y los principios del derecho internacional empleando métodos que sean dinámicos y adaptables, a fin de dar efecto pleno a esos instrumentos. Hay que reconocer que la creciente evolución de las armas y el rápido desarrollo de la ciencia y la tecnología tendrán un impacto enorme en la sociedad humana y que el *jus in bello* deberá ajustarse y adaptarse en consecuencia. Sin embargo, es ingenuo imaginar que los cambios del DIH serán oportunos y eficaces.

Probablemente sea demasiado pronto para promover la adopción de un tratado nuevo en este ámbito. De todas formas, las probabilidades de que los Estados lleguen a un acuerdo sobre una convención integral relacionada con la ciberguerra en el futuro próximo son más que exiguas. Sin embargo, la *lex lata* existente proporciona la normativa básica para la selección de objetivos en la esfera cibernética. La práctica de los Estados, las decisiones judiciales y las opiniones y enseñanzas de los estudiosos deberían ser las principales fuentes para interpretar el marco jurídico vigente y evaluar si este, en la esfera interconectada del ciberespacio, satisface o socava las preocupaciones humanitarias. Es previsible que, en el curso de esa evolución, a la hora de implementar nuevas estrategias en la era de la ciberguerra, los Estados intenten razonar en forma analógica o inductiva, rellenar creativamente las lagunas existentes en el DIH actual, o forzar la *lex lata* sobre el principio de distinción más allá de sus límites normativos. Esas tendencias deben limitarse rigurosamente; sin embargo, excluir la posibilidad de establecer normas nuevas sería arbitrario. Para prevenir el exceso de militarización y fortalecer la protección de los

178 Jimena M. Conde Jiminián, "The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law", *Tilburg Law Review*, vol. 15, n.° 1, 2010. V. también Marco Sassòli, Antoine Bouvier y Anne Quintin, *How Does Law Protect in War?*, 3.ª ed., vol. 1, CICR, Ginebra, 2011, p. 52.

intereses de las poblaciones civiles, es preciso que el principio sea objeto de una nueva y cuidadosa lectura. Hasta ahora no se han producido eventos cibernéticos con múltiples víctimas. Sin embargo, teniendo en cuenta que la interpretación y el esclarecimiento de las normas actuales resultan insuficientes, es indispensable proponer normas nuevas antes de que ocurra un "Pearl Harbor cibernético"[179].

179 Departamento de Defensa, nota 4 *supra*; J. J. Wirtz, "The Cyber Pearl Harbor", nota 4 *supra*; J. J. Wirtz, "The Cyber Pearl Harbor Redux", nota 4 *supra*.