Lecciones y Ensayos, Nro. 97, 2016
Padin, Juan Francisco, "Ciberparticipantes: participación directa en las hostilidades…", pp. 177-197

CIBERPARTICIPANTES: PARTICIPACIÓN DIRECTA EN LAS HOSTILIDADES A TRAVÉS DE MEDIOS Y MÉTODOS CIBERNÉTICOS*

Juan Francisco Padin**

Resumen: Este ensayo analiza el desarrollo de los medios y métodos de combate cibernéticos. El estudio se enfoca en cómo estos han cambiado la forma en que se entiende la participación directa en las hostilidades y cómo estas herramientas interactúan con sus elementos constitutivos. El propósito es deconstruir estos requisitos, tal como son presentados en la guía interpretativa elaborada por el Comité Internacional de la Cruz Roja, y confrontarlos con diferentes supuestos en que herramientas cibernéticas pueden ser utilizadas.

Palabras clave: participación directa en las hostilidades – ciberguerra – ciberataques

Abstract: This essay refers to the development of the cyber means and methods of warfare. The analysis focuses on the way that these means had change Direct Participation in Hostilities and how these tools interact with the constitutive elements of DPH. The purpose is to deconstruct the requirements, as they are mentioned in the interpretative guidance made the International Committee of the Red Cross, and to confront them with different situations where cybernetic tools could be used.

Keywords: direct participation in hostilities – cyberwarfare – cyberattacks

* Este trabajo ha obtenido el Primer Puesto en el XIII Concurso de Ensayos "Ignacio Winizky" sobre Derecho Penal Internacional y Derecho Internacional Humanitario.

** Estudiante de Derecho con orientación de Derecho Internacional Público. Investigador-estudiante en el Proyecto DeCyT 2014-2016: "Las pasiones del derecho internacional: Improntas afectivas, emociones estatales y sentimientos políticos en la historia del Ius Gentium", DCT1407. *Agradezco particularmente la colaboración e incentivo de la profesora Romina E. Pezzot en la elaboración de este trabajo.*

I. Introducción

El siglo XXI cambió el paradigma bajo el cual observamos los conflictos armados. El desarrollo de nuevas tecnologías, particularmente aplicadas al campo de batalla, obliga a repensar la aplicación de las normas, tanto convencionales como consuetudinarias, del Derecho Internacional Humanitario (DIH). En la medida en que las herramientas cibernéticas han sido implementadas en nuevos medios y métodos de combate, o en la modernización de armas anticuadas, se vuelve necesario discutir de qué forma las normas creadas con anterioridad a su desarrollo interaccionan con estas tecnologías.[1]

La evolución de estas herramientas aplicadas a las hostilidades ha derivado en la aparición de categorías específicas para definir su utilización.[2] Sin embargo, la invención de nuevas definiciones no excluye el necesario análisis jurídico respecto a la legitimidad en el uso de la fuerza armada, que deviene de la existencia de un conflicto armado. Aunque la definición respecto a que actos implican el uso de la fuerza corresponde al ámbito del *ius ad bellum*, también es necesaria su utilización en el *ius in bello* y, más precisamente, en la Participación Directa en las Hostilidades (PDH) aplicada al ciber-espacio.[3] Sin definir qué actos cibernéticos implican un

1. Ver al respecto Schmitt, M., "Wired Warfare: Computer Network Attack and Ius in Bello" en *International Review of the Red Cross*, Vol. 84, Nº 846, 2002, pp. 365-399. Ver también Vigevano, M. y Buis, E., "Medios de combate, uso de fuerza armada y las nuevas guerras cibernéticas: la regulación de los ataques por sistemas informáticos en el marco del Derecho de La Haya" en *Conducción de Hostilidades y Derecho Internacional. A propósito del centenario de las Convenciones de La Haya de 1907*, Medellín, Biblioteca Jurídica Diké, 2007, pp. 10-26. Existen restricciones en el desarrollo de nuevos medios y métodos de combate. Ver al respecto Art. 36, *Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales*, 08/06/1977. Ver también *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos*, Comité Internacional de la Cruz Roja (CICR), consultado en [https://www.icrc.org/spa/assets/files/other/icrc_003_0902.pdf] el 05/03/2016

2. Muchos analistas prefieren utilizar el término ciber-guerra (*cyber-warfare*). Ver al respecto Waxman, M., "Cyber-Attacks and the Use of Force: Back to the Future of Article 2.4" en *The Yale Journal of International Law*, Vol. 36, 2011, pp. 431-437. Ver también Huntley, T., "Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare" en *Naval Law Review*, Vol. 60, 2010, pp. 3-4.

3. Entiéndase por ciber-espacio "una red global dentro del ámbito de la información con-

ataque, no puede determinarse en qué casos un civil estaría participando en el conflicto.

Existen diversos motivos por los cuales un análisis comprehensivo de la PDH debe incluir a los medios cibernéticos. Por un lado, la rápida proliferación de estas herramientas implicó un acceso prácticamente irrestricto por parte de la comunidad civil.[4] Por otra parte, las herramientas cibernéticas han surgido como una opción viable con la cual contrarrestar el avance tecnológico de ciertos Estados desarrollados. Una sencilla computadora de escritorio, con el *software* indicado, acceso a la red objetivo y un técnico especializado, puede realizar ataques aun sobre las redes más seguras.[5]

La naturaleza de estos medios ha modificado la estructura de las fuerzas armadas regulares incrementando la participación del personal civil en los conflictos actuales. Una mayor dependencia en los avances tecnológicos ha conllevado un traslado de tareas tradicionalmente realizadas por militares hacia personal civil especializado.[6] Esta progresiva

---

sistente de infraestructuras de redes interdependientes de tecnología informática y datos residentes, incluyendo a la internet, redes de telecomunicación, sistemas de computación y procesadores y controladores relacionados." Roberts, S., "Cyber Wars: Applying Conventional Laws of War to Cyber Warfare and Non-State Actors" en *Northern Kentucky Law Review*, Vol. 41, 2014, p. 538 (traducción propia).

4. "La mayoría de las computadoras están conectadas entre sí de alguna manera. Usualmente comparten el sistema operativo y se comunican con otras computadoras usando el mismo protocolo estándar TCP/IP. La facilidad y la velocidad de dispersión de virus y gusanos como Ninda y Sasser demuestran el vínculo entre las computadoras en línea." *Ibid*., p. 7 (traducción propia).

5. Schmitt, M., "War, Technology, and International Humanitarian Law" en *Program on Humanitarian Policy and Conflict Research (Occasional Paper Series)*, Universidad de Harvard, 2005 (Nº 4), p. 43.

6. Schmitt, M., "Direct Participation in Hostilities and 21st Century Armed Conflict" en Fischer, H. *et al* (eds.), *Crisis Management and Humanitarian Protection: Festschrift fur Dieter Fleck*, 2004a, p. 514. Ver el ejemplo de los Estados Unidos: "Miembros de la fuerza de trabajo expedicionaria civil del Departamento de Defensa serán organizados, entrenados, equipados y preparados para ser desplegados en soporte de las operaciones de combate del personal militar, contingencias, operaciones de emergencia, misiones humanitarias, desastres naturales, restauración del orden, operaciones de drogas y operaciones de estabilidad". Directiva 1401.10, *Fuerza de Trabajo Expedicionaria Civil*, Departamento de Defensa, 23/01/2009 (traducción propia). Ver también Schmitt, M., "Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees" en *Chicago Journal of International Law*, Vol. 5, Nº 2, 2005b, pp. 512-518.

civilinización[7] de los conflictos armados dificulta el análisis práctico del principio de distinción. En la medida en que la línea que divide a los combatientes de la población civil se torna difusa, y debido a la inconmensurable cantidad de opciones que presentan los medios cibernéticos, deben definirse los actos que superan el umbral de requisitos de la PDH (o establecer los parámetros necesarios para su definición).

II. Medios y Métodos Cibernéticos

El desarrollo de herramientas cibernéticas no ha encontrado una réplica en las normas o en la jurisprudencia internacional.[8] No existe una definición unánime o vinculante respecto a la categoría de ciberataques. Asimismo, la particular naturaleza del ciberespacio permite que este sea utilizado tanto como un medio (un arma en sí) o como un método (a través del cual canalizar otros medios)[9] de combate. Cualquier enunciación posible depende, eventualmente, de las referencias de la doctrina o del desarrollo realizado por los manuales militares. Delimitar una categoría para los medios y métodos cibernéticos estriba en las aproximaciones que han sido utilizadas para definir que es un ciber-ataque. Por ejemplo, el *Manual Tallin sobre Derecho Internacional aplicable a las guerras cibernéticas*, elaborado por un grupo de expertos de la OTAN, establece una definición sobre medios y métodos intrínsecamente relacionada con el uso de la fuerza armada.[10]

7. Este concepto, acuñado por Michael Schmitt, se utiliza para graficar la progresiva inclusión de civiles en las fuerzas armadas de varios Estados. Schmitt, M., ob. cit., p. 512. Otros autores prefieren hablar de la "desmilitarización" de los conflictos armados considerando la progresiva disminución de las fuerzas profesionales y la menor importancia estratégica de los objetivos militares. Ver Munkler, H., "The Wars of the 21st Century" en *International Review of the Red Cross*, Vol. 85, Nº 849, marzo 2003, pp. 18-19.

8. Turns, D., "Cyber Warfare and the Notion of Direct Participation in Hostilities" en *Journal of Conflict & Security Law*, Oxford, Oxford University Press, Vol. 17, Nº 2, 2012, pp. 282-283.

9. En particular, las armas de control remoto. Ver *Cyber Warfare and Cyber Weapons, a Real and Growing Threat*, INFOSEC Institute, consultado en [http://resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/] el 05/03/2016.

10. "Los medios cibernéticos de guerra incluyen cualquier tipo de dispositivo electrónico, material, instrumento, mecanismo, equipamiento o software, usado, diseñado o preparado

El Estado Conjunto de las Fuerzas Armadas de los Estados Unidos (*Joint Chiefs of Staff*) ha establecido una definición que entiende los ciberataques como: "acto hostil usando una computadora o redes o sistemas relacionados, con intención de interrumpir y/o destruir sistemas, bienes o funciones criticas del adversario. Los efectos pretendidos por un ciberataque no están necesariamente limitados a los sistemas de redes o a la información".[11] Este enunciado es lo suficientemente amplio para incluir no solo aquellas armas que generen efectos en la red (no cinéticos), sino también aquellas que puedan tener efectos cinéticos.[12] De esta manera se amplía la perspectiva respecto a las aproximaciones que discriminan los ataques cibernéticos de aquellos que provoquen efectos físicos.[13]

Desde este concepto las armas cibernéticas pueden ser tanto un medio como un método de combate. Mediante medios cibernéticos puede destruirse una red de computadoras y volverlas inoperables o alterar sus servicios (como sucedió en Estonia).[14] Pero también puede accederse mediante un virus a la administración de una central nuclear para destruirla

---

para la conducción de un ciber-ataque". Schmitt, M. (ed.), *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013, p. 142 (traducción propia). Para una categorización técnica de armas cibernéticas ver De luca, C., "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors" en *Pace International Law Review Online Companion*, Vol. 3, Nº 9, 2013 pp. 282-285. Ver también Kelsey, J., "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare" en *Michigan Law Review*, Vol. 106, 2008, pp. 1434-1437.

11. *Memorandum for Chiefs of the military services commanders of the combatant commands directors of the joint staff directorates*, Department of Defense, p. 5 (traducción propia). Disponible en [http://www.nsci-va.org/CyberReferenceLib/2010-11joint%20Terminology%20for%20Cyberspace%20Operations.pdf].

12. Turns, D., ob. cit. p. 284.

13. Ver Computer Network Attack (CNA), *Dictionary of Military and Associated Terms, Department of Defense* (JP 1-02), 31/01/2011, p. 79. Estas críticas fueron respaldadas por la doctrina. Ver Dinstein, Y., "Computer Network Attacks and Self Defense" en Schmitt, M. y O'Donnel, B. (eds.), *International Law Studies*, Vol. 76, 2002, pp. 102-105. Hay autores que sostienen que los ciber-ataques únicamente comprenden la destrucción o alteración de información o redes de información. Schmitt, M., ob. cit., p. 526.

14. Estonia es uno de los países con mayor desarrollo cibernético en el mundo. En mayo de 2007, sufrió un ciber-ataque masivo que paralizo los sistemas informáticos del gobierno y de diversas empresas. Ver *Hackers Take Down the Most Wird Country in Europe*, 21/08/07, Wired, consultado en [http://www.wired.com/2007/08/ff-estonia/] el 20/02/2016.

(como sucedió en Irán).[15] En este último caso la destrucción de un sistema informático podría haber derivado directamente en la liberación de fuerzas peligrosas.[16]

En la medida que esta definición incluya actos cinéticos y no cinéticos, es lo suficientemente amplia para referir a la PDH de manera comprensiva.[17] Descartar los actos cibernéticos aislados que produzcan efectos cinéticos significaría ignorar una infinidad de posibles casos. Una perspectiva que solo incluya a los actos no cinéticos contendría únicamente a aquellos individuos que participen en una operación militar compleja.

Sin embargo, no cualquier tipo de acto llevado a cabo en relación o a través de medios o métodos cibernéticos alcanza los requisitos de la PDH, incluso en el contexto de un conflicto armado.[18]

III. Fuentes normativas de la PDH

El sustrato primigenio de la PDH surge del principio de distinción, reconocido como un principio cardinal del Derecho Internacional Humanitario y que engendra la protección de la cual gozan las personas civiles.[19] El

15. En 2010, el virus Stuxnet, que ingreso mediante un dispositivo USB infectado, ordenó detenerse a las maquinas centrifugadoras de una central nuclear en Natanz, Irán. El incidente casi genera una falla crítica masiva. Ver *El virus que tomó control de mil máquinas y les ordenó autodestruirse*, 11/09/2015, BBC, consultado en [http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet] el 20/02/2016.
16. Dormann, K., *Applicability of the Additional Protocols to Computer Network Attacks*, ICRC Resource Centre. Consultado en [https://www.icrc.org/eng/resources/documents/misc/68lg92.htm] el 15/02/2016.
17. Melzer, N., *Guía para interpretar la noción de participación directa en las hostilidades según el Derecho Internacional Humanitario*, CICR, 2010, pp. 47-48.
18. *Ibid.*, p. 41.
19. "Los Estados nunca deben hacer a los civiles el objeto de sus ataques y, consecuentemente, no deben usar armas que son incapaces de distinguir entre civiles y objetivos militares". *Opinión Consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares*, Corte Internacional de Justicia (CIJ), 08/07/1996, párr. 78 (traducción propia).Ver Dinstein, Y., *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge, Cambridge University Press, 2004, p. 113. Schmitt, M.; Garraway, C. y Dinstein, Y., *The Manual on the Law of Non-International Armed Conflict With Commentary*, San Remo, International Institute of Humanitarian Law, 2006, pp. 10-11. "El principio de distinción […] tiene como objetivo fundamental cumplir con uno de los propósitos del derecho interna-

Protocolo Adicional I a los Convenios de Ginebra de 1949 (PAI) establece: "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".[20] De esta protección se distinguen los objetivos permitidos de aquellos que no lo son.[21] Esta norma también cuenta con carácter consuetudinario.[22]

Los civiles no son combatientes y gozan con una presunción a favor en caso de duda,[23] protección que es extensible a los conflictos armados no internacionales.[24] Sin embargo, pueden perder este privilegio en la

---

cional humanitario que es el de proteger a las personas que no toman parte directamente en las hostilidades." Gutierrez Posse, H., *Elementos de Derecho Internacional Humanitario*, Buenos Aires, Eudeba, 2014, p. 71.

20. Protocolo Adicional I, art. 48.

21. "Los ataques se limitaran estrictamente a los objetivos militares. En lo que respecta a los bienes, los objetivos militares se limitaran 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." *Ibid*., art. 52.2.

22. "Norma 1. Las partes en conflicto deberán distinguir en todo momento entre personas civiles y combatientes. Los ataques sólo podrán dirigirse contra los combatientes. Los civiles no deben ser atacados. (CAI/CANI)". Henckaerts, J. M., "Estudio sobre el derecho internacional humanitario consuetudinario: contribución a la comprensión y al respeto del derecho de los conflictos armados" en *International Review of the Red Cross*, Vol. 87, Nº 857, marzo 2005, p. 30. Ver *Prosecutor v. Blaskic*, Caso Nº IT-95-14-A, Tribunal Penal Internacional para la Ex-Yugoslavia, fallo (29/07/2004), Cámara de Apelaciones, párr. 110. Ver también Sandoz, Y., Swinarsky, C. y Zimmerman, B. (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Ginebra, Comité Internacional de la Cruz Roja – Martinus Nijhoff Publishers, 1987, p. 585.

23. "Es persona civil cualquiera que no pertenezca a una de las categorías de personas a que se refieren el artículo 4, A, 1), 2), 3), y 6), del III Convenio, y el artículo 43 del presente Protocolo. En caso de duda acerca de la condición de una persona, se la considerará como civil". PAI, art. 50.1.

24. Protocolo II adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional, 08/06/1977, art. 13. "Personas no tomando parte activa en las hostilidades", art. 3 común a los 4 Convenios de Ginebra de 1949. "Todas las personas que no son miembros de las fuerzas armadas estatales o de los grupos armados organizados de una parte en conflicto son personas civiles". Melzer, N., ob. cit., p. 27.

medida en que participen activa o directamente[25] en las hostilidades.[26] Según la guía interpretativa presentada por el Comité Internacional de la Cruz Roja (en adelante guía interpretativa), participar implica realizar "actos específicos ejecutados por personas como parte de la conducción de hostilidades entre partes en un conflicto armado".[27] Esto significa que, a pesar de la protección general de la cual gozan, aquellos civiles que participen en las hostilidades pueden ser el objeto de ataques.[28] Mientras dure dicha participación no forman parte del cálculo de proporcionalidad[29] y pueden ser un blanco de ataque legítimo.[30] Además, en tanto 'combatientes ilegítimos', pueden ser juzgados por tribunales internos por la mera participación o por la comisión de crímenes de guerra en caso de serias violaciones al DIH.[31]

Sin embargo, no cualquier tipo de participación alcanza, es necesario que se cumpla con los tres requisitos que la constituyen. Estos tres elementos plantean nuevas cuestiones en cuanto se los analiza en consideración de los medios cibernéticos.

IV. Los elementos de la PDH

Según la guía elaborada por el CICR, debe cumplirse con tres requi-

25. Los términos "activo" y "directo" se reconocen como sinónimos. Ver *The Prosecutor v. Jean Paul Akayesu*, ICTR-96-4-T, Tribunal Penal Internacional para Ruanda, Cámara de Apelaciones, Fallo, (02/08/1998), párr. 629.
26. Art. 51, PAI, art.13, PAII.
27. Melzer, N., ob. cit., p. 43.
28. Schmitt, M., "The Interpretative Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis" en *Harvard National Security Journal,* Vol. 1, 2010(a), p. 13.
29. No confundir entre el cálculo de proporcionalidad respecto a las bajas civiles que comprende cualquier ataque y la respuesta al ataque de un participante. La respuesta debe ser proporcional al ataque recibido. Ver las conclusiones de este trabajo.
30. "Concretamente, cuando civiles como los que atacaron el cuartel de La Tablada, asumen el papel de combatientes al participar directamente en el combate, sea en forma individual o como integrantes de un grupo, se convierten en objetivos militares legítimos. En tal condición, están sujetos al ataque directo individualizado en la misma medida que los combatientes". Comisión Interamericana de Derechos Humanos, *Abella v. Argentina*, Caso Nº 11.137, Informe Nº 55/97, 18/11/1997, párr. 178 (traducción propia).
31. Dormann, K., "The legal situation of unlawful/unprivileged combatants" en *International Review of the Red Cross*, Vol. 85, Nº 849, 2003, pp. 70-71.

sitos acumulativos:[32] umbral de daño, causalidad directa y nexo beligerante.

IV.A. Umbral de daño

No cualquier tipo de daño alcanza para cumplir con este requisito. Es necesaria la causación, materializada o probable, de "un daño de índole específicamente militar o causando la muerte, heridas o destrucción a las personas o bienes protegidos contra los ataques directos".[33] Es indistinto que este daño genere (o pueda objetivamente generar) efectos sobre operaciones o la capacidad militar de una de las partes en conflicto y/o sobre personas o bienes protegidos, siendo esta última limitada a las tres posibilidades propuestas.[34] La dificultad de este punto se encuentra en determinar la naturaleza o el grado del daño, en tanto el concepto de actos dañosos abarca mucho más que entrar en combate con el enemigo.[35] La PDH no requiere la ejecución de actos de violencia por parte del individuo, ni siquiera es necesario que dicho acto se produzca en el contexto de una operación militar.[36]

Teniendo en cuenta únicamente este elemento (sin tomar en cuenta la causalidad directa o el nexo beligerante), parecería claro que se incluirían dentro de esta categoría todo tipo de utilización cibernética, sobre la base de las definiciones provistas anteriormente, que produzca un daño militar o genere un efecto determinado (muerte, heridas o destrucción) sobre personas o bienes protegidos. En este último supuesto, analizado a partir de la guía interpretativa,[37] solo podrían incluirse las armas que produzcan efectos cinéticos o la utilización de otro tipo de instrumentos que, articulados a través de métodos cibernéticos, puedan producir dichos efectos.[38] Como podría suceder, por ejemplo, si se utilizan herramientas informáticas para

32. Melzer, N., ob. cit., p. 46.
33. *Ibid.*, p. 47.
34. Delerue, F., "Civilian Direct Participation in Cyber Hostilities" en *Revista de Internet, Derecho y Política*, Universidad Abierta de Cataluña, Vol. 19, octubre 2014, p. 8.
35. Schmitt, M., "Deconstructing Direct Participation in Hostilities: The Constitutive Elements" en *International Law and Politics*, Vol. 42, 2010(b), pp. 713-714.
36. *Ibid*., p. 716.
37. Melzer, N., ob. cit. pp. 47-51.
38. Hay autores que prefieren descartar este supuesto debido a las dificultades que se presentan cuando se trata la cuestión de la causalidad directa. Ver Delerue, F., ob. cit., p. 8.

manipular una red que controla el tráfico ferroviario. Si dicha operación produce un accidente que tuviera como resultado, entre otros posibles efectos, muertos o heridos civiles (sujetos protegidos por el DIH), el umbral de daño sería alcanzado.

El otro supuesto (daño militar) comprende un sinnúmero de actividades que abarcan un amplio prospecto de armas cibernéticas que pueda causar daños de naturaleza militar,[39] implicando cualquier tipo de consecuencia adversa en las operaciones militares o la capacidad militar de la otra parte.[40] La guía interpretativa incluye, entre otros ejemplos, la limpieza de minas, la intercepción de las líneas telefónicas de los altos mandos de la parte adversaria, la transmisión de información o inteligencia táctica en relación con los objetivos de un ataque o, incluso, la interferencia electrónica en las redes informáticas militares.[41]

La cuestión radica en aquellos actos cibernéticos en los que el cumplimiento de este umbral de daño es discutible, aquellos casos en que no se genera un daño militar ostensible aun cuando pueda contribuir con el esfuerzo militar general.[42] No resulta difícil discernir respecto a este umbral en los casos en que los actos son realizados de forma aislada o por un solo sujeto participante, como en el ejemplo del tren. Distinto es el caso en que se consideran operaciones realizadas por varios intermediarios o en el contexto de una operación militar.[43]

En aquellos casos en los que varios sujetos participan de una operación militar compleja, debe analizarse la actuación de cada individuo para

39. "Cuando razonablemente quepa esperar que un acto causara daños de naturaleza claramente militar, el requisito en relación con el umbral se cumplirá independientemente de la gravedad de los daños en términos cuantitativos". Melzer, N., ob. cit., p. 47.
40. *Idem*.
41. *Ibid*., p. 48.
42. *Ibid*., p. 50. Según la Guía Interpretativa para superar el umbral de daño "podría bastar una interferencia electrónica en las redes informáticas militares, sea mediante ataques contra la red informática o la explotación de la red informática" pero también se utiliza como ejemplo la "manipulación de redes informáticas" como un acto en el que no se generan daños de índole militar de forma directa. Ver el cuadro sinóptico en Turns, D., ob. cit., p. 295. Sandoz, Y., Swinarsky, C.y Zimmerman, B., ob. cit., p. 619.
43. Como ejemplo de la participación de civiles en operaciones militares, ver Turner, L., *Civilians at the Tip of the Spear: Civilian Issues Commanders Encounter during Deployments*, Air Command and Staff College Air University Maxwell, 2001. Consultado en [http://www.dtic.mil/dtic/tr/fulltext/u2/a407127.pdf] el 27/02/2016.

determinar en cada situación particular si se supera el umbral. Dicho acto formara parte necesaria del daño militar en la medida en que contribuya de forma objetiva y cierta a dicho daño (*harmful acts*).[44] Eso significa que actos como, por ejemplo, tareas de planificación, inteligencia, diseño de herramientas cibernéticas específicas, introducción de agentes hostiles en las redes del adversario (DoS/DDoS, troyanos, virus) o ejecución de redes de control de armas convencionales o de destrucción masiva, cumplen con este requisito.[45]

IV.B. Causalidad Directa

La exigencia de que la participación sea directa implica distinguir entre aquellos actos que forman parte de la conducción de las hostilidades y los que se relacionan con el esfuerzo general de guerra (participación indirecta).[46] En la PDH se incluye todas las actividades "que objetivamente contribuyan a la derrota del adversario",[47] en la medida en que están destinadas a causar el daño pretendido.[48] Dicho daño debe ser el proceso de una sola secuencia causal, sin importar la cantidad de

44. "Actos con el propósito o el efecto que es dañar a la parte adversa, facilitando o impidiendo operaciones militares". Pictet, J. (ed.), *Commentary to the I Geneva Convention for the Ameloriation of the Condition of the Wounded and Sick in Armed Forces in the Field*, Ginebra, ICRC, 1952, p. 200 (traducción propia). "Los actos hostiles deberían ser interpretados como actos que por su naturaleza o propósito buscan causar daño real al personal o equipamiento de las fuerzas armadas". Sandoz Y.; Swinarsky, C. y Zimmerman, B., ob.cit., p. 618 (traducción propia).
45. Turns, D., ob. cit., p. 295. Melzer, N., ob. cit., p. 48. Schmitt, M., *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, La Haya, Second Expert Meeting on the Notion of Direct Participation in Hostilities - CICR, 2004, p. 23.
46. Melzer, N., ob. cit., p. 51. "La noción de participación directa en las hostilidades debe referirse a algo más que a actos violentos o dañosos en contra de la parte contraria. Al mismo tiempo, la participación directa en las hostilidades no pueden contener todas las actividades en apoyo de las operaciones militares de una parte o del esfuerzo general de guerra". *Prosecutor v. Pavle Strugar*, Caso Nº IT-01-42-A, Tribunal Penal Internacional para la Ex Yugoslavia, fallo (17/07/2008), Cámara de Apelaciones, párr. 176 (traducción propia).
47. *Ibid.*, p. 51.
48. *Ibid.*, p. 52.

actividades o participantes incluidos,[49] pero distinguiéndolo del esfuerzo general de guerra.[50]

Este elemento requiere un análisis profundo en la medida en que se analizan instrumentos cibernéticos. La "virtualidad" del ciberespacio envuelve barreras e implica distancias que no se encuentran en otros medios o métodos de combate. Ya que estos casos pueden involucrar desde computadoras de escritorio hasta complejos sistemas de seguridad, existe al menos un intermediario (sea un *software*, un dispositivo electrónico, etc.) entre el sujeto que participa y el objetivo del ataque. Lo que agrega nuevas variables en cualquier secuencia causal que contenga medios o métodos cibernéticos.

Sin embargo, este elemento no requiere que exista una cadena ininterrumpida de eventos, ni siquiera que exista proximidad temporal o geográfica entre la causa y su consecuencia.[51] El componente esencial para determinar el papel del acto en cuestión se encuentra en su obligatoriedad en la secuencia para producir el efecto deseado en un objetivo específico.[52] Este concepto excluye la conducta individual que contribuye a mantener o mejorar la capacidad de una parte para dañar al enemigo de forma genérica.[53] Un individuo que desarrolla un programa informático sin tener en miras provocar un daño en particular no cumpliría con este requisito,[54] mientras que si lo haría quien diseña un programa para una operación especifica.[55]

49. *Ibid*., p. 53. "Los expertos recordaron que el adjetivo 'integral' usado en la guía interpretativa deliberadamente no excluye actos que representen partes menores en una operación militar […] Consecuentemente, el uso de adjetivos como 'clave' o 'necesario' requiere que los actos en cuestión tengan una parte decisiva o indispensable en la cadena causal en una operación". *Fourth Expert Meeting on the Notion of Direct Participation in Hostilities*, Ginebra, Summary Report - CICR, 2006, p. 47 (traducción propia).
50. "En contraste, los civiles cuyas actividades simplemente apoyen a la parte adversa o a su fuerza militar o que de otra manera participen indirectamente en las hostilidades no pueden, exclusivamente bajo estas actividades, ser considerados combatientes". *Third Report on the Human Rights Situation in Colombia*, Comisión Interamericana de Derechos Humanos, OEA/Ser. L/V/II.102, 26/02/1999, Cáp. 4, párr. 56 (traducción propia). Ver también Sandoz, Y.; Swinarsky, C. y Zimmerman, B., ob. cit., p. 619.
51. *Ibid*., pp. 54-55.
52. Schmitt, M., ob. cit., p. 726.
53. *Ibid.*, p. 727.
54. Turns, D., ob. cit., p. 295.
55. Crawford, E., "Virtual Battlegrounds: Direct Participation in Cyber Warfare", en *I/S: A Journal of Law and Policy for the Information Society*, Vol. 9, 2013, p. 16. Entre el grupo

IV.C. Nexo Beligerante

No cualquier acto realizado en el contexto de un conflicto armado puede ser considerado PDH, es necesario que dicho acto sea realizado en favor de una de las partes y en detrimento de la otra.[56] De esta forma se excluyen aquellos actos que no tienen relación o aprovechan la situación de inestabilidad derivada del conflicto, incluso si generan un perjuicio para una de las partes.[57]

Según la guía interpretativa este requisito depende del propósito objetivo del acto sin que el ánimo del sujeto afecte la calificación.[58] En la medida en que se exige que el comportamiento esté "destinado específicamente a prestar apoyo a una parte en conflicto causando daño a otra parte"[59] dicha observación resulta exigua en el caso de los ciberataques ya que exigen cierta experticia (y por ende el conocimiento del sujeto). No se cumple con este punto solo por causar un daño a una de las partes, es necesario también prestar apoyo a la otra.[60] La guía interpretativa considera la voluntad del sujeto en algunos casos excepcionales, si ignoran la función que están desempeñando, como sucede con los escudos humanos involuntarios.[61]

Es importante determinar el cumplimiento de ambas condiciones en el caso de ciberataques, en tanto la línea que separa el uso de la fuerza armada del cibercrimen puede depender del contexto en el cual suceden.[62] Es

---

de expertos que elaboraron la guía interpretativa existieron posturas encontradas en este punto utilizándose como referencia la preparación de artefactos explosivos improvisados. Ver *Fourth Expert Meeting on the Notion of Direct Participation in Hostilities*, Ginebra, Summary Report - CICR, 2006, p. 58.

56. Melzer, N., ob. cit., p. 58.

57. Schmitt, M., ob. cit., p. 735. Este criterio es más estricto que el utilizado para determinar la existencia de un crimen de guerra, ver *Prosecutor v. Dragoljub Kunarac, Radomir Kovac & Zoran Vukovic*, Caso IT-96-23 y IT-96-23/1-A, Tribunal Penal Internacional para la Ex Yugoslavia, fallo (12/06/2002), Cámara de Apelaciones, párr. 55-65. *Prosecutor v. Georges Rutaganda*, Caso ICTR-96-3-A, Tribunal Penal Internacional para Ruanda, fallo (26/05/2003), Cámara de Apelaciones, párr. 570.

58. Melzer, N., ob. cit., pp. 60-61.

59. *Ibid*., p. 61.

60. Schmitt, M., ob. cit., p. 736.

61. Melzer, N., ob. cit., p. 60.

62. Muchas de las herramientas utilizadas en los ciber-crímenes (troyanos, virus, bots, spyware, gusanos, etc.) son similares o idénticas a las utilizadas en ciber-ataques. Por ejem-

posible que un cibercrimen cumpla con una o ambas condiciones. Otra vez puede utilizarse el ejemplo del tren, imaginemos que como consecuencia de un ciberataque es destruido. Dicho ataque podría producirse tanto en tiempos de paz como en tiempos de conflicto. En el primer caso se trataría de un cibercrimen (ya sea homicidio, daños, etc.) mientras que en el segundo podría ser un ciberataque (además de un crimen de guerra).

V. Problemas en la determinación de la PDH. ¿Participantes o Combatientes?

La participación comienza con los eventos preparatorios de la operación y termina con el regreso del acto hostil específico.[63] En el caso que el acto individual no implique el traslado o el despliegue de la persona en cuestión, como puede suceder con los actos cibernéticos, la duración de la PDH se limita a "la ejecución inmediata del acto y a las medidas preparatorias que forman parte integrante de ese acto".[64] Durante ese lapso de tiempo el sujeto pierde la protección que le otorga su status de civil y puede ser objeto de ataques armados.[65] Sin embargo, un problema que puede presentarse en la práctica es determinar si dicho individuo es un civil o un combatiente en un momento específico. Cuestión determinante para definir si el ataque contra dicha persona es legítima o extemporánea. Si el individuo es un participante solo puede ser atacado en la franja temporal determinada por el acto y su preparación. Sin embargo los combatientes o participantes en función continua de combate pueden ser atacados sin dicha delimitación temporal.[66]

La aplicación del principio de distinción es relativamente sencilla en el caso de conflictos armados internacionales, en tanto los combatientes se

---

plo la relación entre los crímenes por robo de información y las tareas de inteligencia. Ver Gordon, S. y Ford, R., "On the Definition and Classification of Cybercrime" en *Journal on Computer Virology*, Vol. 2, Nº 1, 2006, p. 14.

63. Melzer, N., ob. cit., p. 68.

64. *Idem*. La guía interpretativa incluye específicamente en este supuesto a los ataques cibernéticos.

65. Esta protección se conoce como inmunidad del no-combatiente. Ver Gardam, J., *Non-Combatant Immunity as a Norm of International Humanitarian Law*, Dordrecht, Martinus-Nijhoff Publishers, 1993, pp. 2-4.

66. Turns, D., ob. cit., p. 664.

dividen en dos categorías: los miembros de las fuerzas armadas (en sentido amplio)[67] de una parte en conflicto y cualquier otra persona que tome parte activa en las hostilidades.[68] Parecería que toda persona que combate en nombre de una de las partes en conflicto es un combatiente.[69] Esta categorización podría plantear dificultades frente a los "*hacktivistas*" o *hackers*-patrióticos, aquellos que no pertenecen a las fuerzas de un Estado, pero que por iniciativa propia llevan a cabo ataques contra los sistemas informatizados de un Estado enemigo.[70] En la medida en que su participación no sea esporádica o no se encuentre delimitada en un conjunto de operaciones determinadas, dichas personas podrían/deberían ser consideradas participantes en las hostilidades por función continúa de combate.

David Turns ha sugerido la posibilidad de asimilar ciertas actividades como la realización de ciertos ciber-ataques o el espionaje cibernético dentro de la categoría de *levée en masse* o los movimientos de resistencia organizados respectivamente. Esto le otorgaría al individuo, en caso de ser capturado, el status de prisionero de guerra.[71] Los principales cuestionamientos a estas clasificaciones están en la redacción de las normas que regulan estas figuras. En el caso del *levée en masse* se exige que la población "tome espontáneamente las armas" y "las lleve a la vista".[72] Por su parte a los miembros de milicias, cuerpos voluntarios y movimientos de resistencia organizados, se les requiere llevar un "distintivo fijo" y "llevar

67. "Todas las fuerzas armadas que tengan un grado suficiente de organización militar y que pertenezcan a una parte en conflicto deben ser consideradas como pertenecientes a las fuerzas armadas de esa parte". Melzer, N., ob. cit., p. 22.
68. Dinstein, Y., ob. cit., p. 27. Ver también Garraway, C., "Combatants-Substance or Semantics?" en Schmitt, M. y Pejic, J. (eds.), *International Law and Armed Conflict: Exploring the Faultline, Essays in Honour of Yoram Dinstein*, Leiden, Martinus Nijhoff Publishers, 2007, p. 320.
69. Watkin, K., "Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretative Guidance" en *International Law and Politics*, Vol. 42, 2010, p. 652. "En esencia, esta definición de las fuerzas armadas cubre a todas las personas que luchan en apoyo de una de las partes en conflicto y que se subordinan a su comando". Henckaerts, J. M. y Doswald-Beck, L., *Customary International Humanitarian Law,* Vol. 1, Cambridge University Press, 2005, p. 15 (traducción propia).
70. Turns, D., ob. cit., p. 293.
71. *Idem*.
72. III Convenio de Ginebra relativo al trato debido a los prisioneros de guerra, 12/08/1949, art. 4.A.6.

las armas a la vista".[73] A pesar de que muchos de estos requerimientos fueron ideados para evitar la perfidia,[74] es difícil imaginar cómo podrían ser fehacientemente aplicables a las actividades cibernéticas.

En aquellos casos en que la participación es continua y no es posible discriminar cuando el sujeto participa o deja de participar en las hostilidades, podría ser considerado como miembro de un grupo armado organizado.[75] En cambio, en el caso de las fuerzas armadas regulares, sea tanto en conflictos armados internacionales como no internacionales, la calidad de combatiente está unida a la membresía en las fuerzas.[76]

Algo similar sucede con las unidades clandestinas o el personal civil contratado por las fuerzas armadas de un Estado que realizan operaciones militares o cumplen funciones esenciales en el desarrollo de estos procedimientos,[77] aunque en estos casos serían considerados combatientes.[78]

73. *Ibid.*, art. 4.A.2.

74. Pictet, J. (ed.), *Commentary III Geneva Convention Relative to the Treatment of Prisoners of War*, Ginebra, ICRC, 1960, p. 61.

75. Esto se conoce como la teoría de la 'puerta giratoria' o 'vaivén' (*revolvingdoor*). Melzer, N., p. 76. "Lo que sería particularmente controversial es la falta de una guía clara que determine el número de veces que un civil puede pasar a través de la 'puerta giratoria', aunque está indicado que en cierto punto, cuando los individuos van más allá de lo espontaneo, esporádico, o participación directa desorganizada, estos se convierten en miembros de un grupo armado organizado […] Clasificar a todos los participantes como civiles porque no califican como combatientes legítimos bajo el protocolo adicional I, significaría colocar individuos que participan en el conflicto, e incluso grupos armados organizados, bajo el status de protección civil". Watkin, K., ob. cit., pp. 661-666 (traducción propia). En estos casos, en el contexto de un conflicto armado internacional, debería discutirse la existencia de un conflicto armado no internacional paralelo.

76. Indistintamente de las actividades llevadas a cabo. Watkin, N., ob. cit., p. 661.

77. Schmitt, M., ob. cit., p. 515. "Por lo que respecta a los contratistas y a los empleados civiles que, para todos los fines y objetos, son incorporados en las fuerzas armadas de una parte en conflicto, sea mediante un procedimiento oficial de conformidad con el derecho interno, sea de facto porque se les ha asignado una función continua de combate. De conformidad con el DIH, esos se convierten en miembros de una fuerza, una unidad o un grupo armado organizado, bajo un mando responsable ante una parte en conflicto y, a los fines del principio de distinción, dejan de ser considerados personas civiles". Melzer, N., ob. cit., p. 39.

78. En caso de duda sobre el estatus de la persona que ha cometido un acto beligerante dicha persona debe tratarse como prisionero de guerra hasta que su estatus sea resuelto por un tribunal competente. Conf. III Convenio de Ginebra relativo al trato debido a los prisioneros de guerra, 12/08/1949, art. 5.

La clasificación de miembros de grupos armados organizados en conflictos armados no internacionales puede plantear distintas dificultades a las recién expuestas. En primer lugar el estatus de combatiente, o el de prisionero de guerra, no existe en estos conflictos, aunque sea utilizado de forma coloquial. Las personas que no participan en las hostilidades se encuentran cubiertos por el Art. 3 común a los cuatro convenios de Ginebra.[79] Los miembros de grupos armados organizados mantienen dicha calidad en virtud de su función continua de combate. Esto implica que dejan de beneficiarse de los límites temporales estrictos que establece la PDH.[80]

VI. El problema de la temporalidad en el ciber-espacio

La guía interpretativa, sobre la base de la fuente normativa,[81] establece una temporalidad precisa que marca la perdida de protección que otorga el status de civil y que permite que dicho individuo sea blanco de ataques. Sin embargo, los criterios utilizados son casi exclusivamente territoriales, en tanto conllevan un despliegue físico y comprenden cierto lapso de temporalidad.[82] Si bien muchas actividades cibernéticas conllevan un plazo, como las labores de inteligencia, otras tantas implican un efecto inmediato.

La posición restrictiva de la guía interpretativa anula la capacidad de respuesta de la otra parte ante a un ataque informático de ejecución, que no implique una brecha temporal entre la causa y el efecto. Una vez realizado el acto el participante recuperaría el status de civil. La visión de la guía está fundamentada en el Art. 51.3 del Protocolo Adicional I y no necesariamente la limitación temporal de base consuetudinaria es tan restringida.[83] Sería inconsistente con el normal desarrollo de las hostilidades, limitar tan severamente al combatiente e impedirle que responda

79. Pejic, J., "Unlawful/Enemy Combatants: Interpretation and Consequences" en Schmitt, M. y Pejic, J. (eds.), *International Law and Armed Conflict: Exploring the Faultline, Essays in Honour of Yoram Dinstein*, Leiden, Martinus Nijhoff Publishers, 2007, pp. 335-336.
80. Melzer, N., ob. cit., p. 71.
81. "Mientras dure tal participación". Art. 51.3, PAI.
82. Melzer, N., ob. cit., pp. 65-68.
83. *Targeted Killings Case*, Suprema Corte de Justicia de Israel, HCJ 769/02, Fallo, 11/12/2005, párr. 38.

a un ataque de esta especie. Siempre teniendo en cuenta la proporcionalidad de la respuesta,[84] la participación cibernética obliga a optar por la perspectiva amplia.

VII. Conclusiones

El rápido desarrollo de los medios y métodos cibernéticos ha superado cualquier aproximación que pudiera realizarse desde el derecho positivo. Si bien muchas de las normas aplicables a estas cuestiones son anteriores a la aparición del ciberespacio, esto no excluye que deba adecuarse a este ordenamiento. Una interpretación contemporánea del DIH obliga a considerar una aplicación dinámica y comprehensiva de los principios.[85] Debido a la infinidad de situaciones y actividades que alcanzan los medios cibernéticos no es posible vislumbrar un umbral claro entre la ciberparticipación directa e indirecta. Lo que sí es factible, es esclarecer los elementos constitutivos de la PDH para realizar una determinación en cada caso particular.[86] En la medida en que los combatientes tienen la obligación de realizar todos los pasos necesarios para determinar la legitimidad del ataque a un objetivo,[87] las reglas claras son fundamentales en la praxis del DIH.

Bibliografía

Billio, Charles y Ching, Welton*, Cyber Warfare: an analysis of the means and motivations of selected nation states*, Institute for Security Technology Studies at Darmouth College, 2004.

Crawford, Emily, "Virtual Battlegrounds: Direct Participation in Cyber

84. Gutiérrez Posse, H., ob. cit., p. 74.

85. "El concepto de PDH tiene un peso determinante en los conflictos armados contemporáneos. El desarrollo tecnológico ha expandido la capacidad de los individuos para aplicar fuerza letal mientras se encuentran localizados a miles de millas de sus objetivos". Goodman, R. y Jinks, D., "The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum" en *International Law and Politics*, Vol. 42, 2010, p. 637 (traducción propia).

86. "Como es evidente la determinación de la PDH es contextual, uno típicamente requerirá un análisis caso por caso". Schmitt, M., ob. cit., p. 508 (traducción propia).

87. Sandoz, Y.; Swinarsky, C. y Zimmerman, B., ob. cit., pp. 680-682.

Warfare" en *I/S: A Journal of Law and Policy for the Information Society*, Vol. 9, 2013, pp. 1-19.

Delerue, Francois, "Civilian Direct Participation in Cyber Hostilities" en *Revista de Internet*, *Derecho y Política*, Universidad Abierta de Cataluña, Vol. 19, octubre, 2014, pp. 3-17.

Deluca, Christopher, "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors", en *Pace International Law Review Online Companion*, Vol. 3, Nº 9, pp. 278-315.

Dinstein, Yoram, "Computer Network Attacks and Self Defense" en Schmitt, Michael y O´Donnell, Brian (Eds.), *International Law Studies*, Vol. 76, 2002, pp. 99-119.

—, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, 2004.

Dormann, Knut, "The legal situation of 'unlawful/unprivileged combatants'" en *International Review of the Red Cross*, Vol. 85, N° 849, 2003, pp. 45-74.

—, *Applicability of the Additional Protocols to Computer Network Attacks,* ICRC Resource Centre, 19/11/2004, p. 7. Consultado en [https://www.icrc.org/eng/resources/documents/misc/68lg92.htm]

Garraway, Charles, "Combatants-Substance or Semantics?" en Schmitt, Michael y Pejic, Jelena (eds.), *International Law and Armed Conflict: Exploring the Faultline, Essays in Honour of YoramDinstein*, Leiden, Martinus Nijhoff Publishers, 2007, pp. 317-334.

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

Gooman, Ryan y Jinks, Derek, "The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum" en *International Law and Politics*, Vol. 42, 2010, pp. 637-640.

Gordon, Sarah y Ford, Richard, "On the Definition and Classification of Cybercrime" en *Journal on Computer Virology*, Vol. 2, N° 1, 2006, pp. 13-20.

Gutierrez Posse, Hortensia, *Elementos de Derecho Internacional Humanitario*, Buenos Aires, Eudeba, 2014.

Henckaerts, Jean-Marie, "Estudio sobre el derecho internacional humanitario consuetudinario: contribución a la comprensión y al respeto del derecho de los conflictos armados" en *International Review of the Red Cross*, Vol. 87, N° 857, marzo de 2005, pp. 3-46.

— y Doswald-Beck, Louise, *Customary International Humanitarian Law*, Vol. 1, Cambridge University Press, 2005.

Huntley, Todd, "Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare" en *Naval Law Review*, Vol. 60, 2010, pp. 1-40.

Kelsey, Jeffrey "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare" en *Michigan Law Review*, Vol. 106, 2008, pp. 1427-1452.

Melzer, Nils, *Guía para interpretar la noción de participación directa en las hostilidades según el Derecho Internacional Humanitario*, Ginebra, Comité Internacional de la Cruz Roja, 2010.

Munkler, Herfried, "The Wars of the 21st Century", en *International Review of the Red Cross*, Vol. 85, Nº 849, marzo 2003, pp. 7-22.

Pejic, Jelena, "Unlawful/Enemy Combatants: Interpretation and Consequences", en Schmitt, Michael y Pejic, Jelena (eds.), *International Law and Armed Conflict: Exploring the Faultline, Essays in Honour of Yoram Dinstein*, Leiden, Martinus Nijhoff Publishers, 2007, pp. 335-355.

Pictet, Jean (ed.), *Commentary to the I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, Ginebra, ICRC, 1952.

—, *Commentary III Geneva Convention Relative to the Treatment of Prisoners of War*, Ginebra, ICRC, 1960.

Roberts, Shaun, "Cyber Wars: Applying Conventional Laws of War to Cyber Warfare and Non-State Actors" en *Northern Kentucky Law Review*, Vol. 41, 2014, pp. 535-572.

Sandoz, Yves, Swinarsky, Christophe y Zimmerman, Bruno (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Ginebra, Comité Internacional de la Cruz Roja –Martinus Nijhoff Publishers, 1987.

Schmitt, Michael, "Wired Warfare: Computer Network Attack and Ius in Bello" en *International Review of the Red Cross*, Vol. 84, Nº 846, 2002, pp. 365-399.

—, "Direct Participation in Hostilities and 21st Century Armed Conflict" en Fischer, H. U. *et al* (eds.), *Crisis Management and Humanitarian Protection: Festschrift fur Dieter Fleck*, 2004(a), pp. 505-529.

—, *Humanitarian Law and Direct Participation in Hostilities by Private*

Contractors or Civilian Employees, La Haya, Second Expert Meeting on the Notion of Direct Participation in Hostilities - CICR, 2004(b).

—, "War, Technology, and International Humanitarian Law" en *Program on Humanitarian Policy and Conflict Research (Occasional Paper Series),* Universidad de Harvard, Nº 4, 2005(a).

—, "Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees" en *Chicago Journal of International Law*, Vol. 5, N° 2, 2005(b), pp. 511-546.

—, "The Interpretative Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis" en *Harvard National Security Journal*, Vol. 1, 2010(a), pp. 6-44.

—, "Deconstructing Direct Participation in Hostilities: The Constitutive Elements" en *International Law and Politics*, Vol. 42, 2010(b), pp. 697-739.

—, *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.

—, Garraway, Charles y Dinstein, Yoram, *The Manual on the Law of Non-International Armed Conflict With Commentary, International Institute of Humanitarian Law*, San Remo, 2006.

Turner, Lisa, *Civilians at the Tip of the Spear: Civilian Issues Commanders Encounter during Deployments*, Air Command and Staff College Air University Maxwell, 2001. Consultado en [http://www.dtic.mil/dtic/tr/fulltext/u2/a407127.pdf].

Turns, David, "Cyber Warfare and the Notion of Direct Participation in Hostilities" en *Journal of Conflict & Security Law*, Oxford University Press, Vol. 17, N° 2, 2012, pp. 279-297.

Vigevano, Marta y Buis, Emiliano, "Medios de combate, uso de fuerza armada y las nuevas guerras cibernéticas: la regulación de los ataques por sistemas informáticos en el marco del Derecho de La Haya" en *Conducción de Hostilidades y Derecho Internacional. A propósito del centenario de las Convenciones de La Haya de 1907*, Medellín, Biblioteca Jurídica Diké, 2007, pp. 10-26.

Watkin, Kenneth, "Oportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretative Guidance" en *International Law and Politics*, Vol. 42, 2010, pp. 641-695.

Waxman, Matthew, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2.4" en *The Yale Journal of International Law*, Vol. 36, 2011, pp. 421-459.