InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

Responsabilidad penal internacional en el ciberespacio

Kai Ambos

Georg August Universität Göttingen

BARCELONA, ABRIL DE 2015

Abstract[*]

El principal objetivo de este trabajo es brindar una visión confiable sobre el estado de la discusión con respecto a los "ataques informáticos" o ciberataques. Un ataque informático constituye la forma más intensa de lo que puede ser considerado como una guerra cibernética, esto es, el uso de medios técnicos para pelear una guerra contra un enemigo en el ciberespacio. El motivo de interés en los ataques informáticos es que por lo general sólo estas formas de delitos cometidos en el ciberespacio son lo suficientemente serias para ser calificadas como crímenes internacionales y, así, quedar cubiertas por una jurisdicción penal internacional como la de la Corte Penal Internacional. En lo que se refiere a la "responsabilidad penal internacional", el debate actual se concentra principalmente en la aplicación del derecho de los conflictos armados, o derecho internacional humanitario, a los ataques informáticos (infra 2). El debate es menos intenso en relación a la posible responsabilidad penal por un crimen de agresión (infra 3). Por último, prácticamente no hay ningún debate con respecto a la comisión de crímenes contra la humanidad mediante ataques informáticos, pero vale la pena realizar una breve mirada a esta posibilidad siguiendo la discusión de los crímenes de guerra (infra 4). Por supuesto que hay muchas otras cuestiones relativas a la responsabilidad penal internacional en el ciberespacio pero su tratamiento excede el propósito de este artículo.

Der Beitrag will einen verlässlichen Überblick über den Diskussionsstand hinsichtlich sog. Cyberangriffen geben. Ein Cyberangriff stellt die stärkste Form eines Angriffs im Rahmen der Cyberkriegsführung dar, nämlich der Einsatz technischer Mittel zur Kriegsführung in der Cyberwelt. Lediglich solche Cyberangriffe sind schwerwiegend genug, um als internationale Verbrechen gelten und somit einer völkerstrafrechtlichen Gerichtsbarkeit unterwerfen werden zu können. Was die international strafrechtliche Verantwortlichkeit angeht, so geht es vor allem um die Anwendung des humanitären Völkerrechts auf Cyberangriffe (infra 2). Von geringerer Bedeutung ist die Diskussion hinsichtlich des Aggressionsverbrechens (infra 3), Verbrechen gegen die Menschlichkeit werden praktisch nicht diskutiert (infra 4). Natürlich gibt es weitere Probleme; diese müssen jedoch anderen Untersuchungen vorbehalten bleiben.

The primary objective of this paper is to give a reliable overview of the state of the art with regard to 'computer network attacks' (CNAs) or cyber-attacks. A CNA constitutes the strongest form of what is regarded to be cyber warfare, i.e., the use of technical means to wage war against an adversary in cyberspace. The focus on CNAs in this paper is explained by the fact that only these forms of crimes in cyberspace are normally serious enough to qualify as international crimes and thus be covered by an international criminal jurisdiction like the ICC. As to 'international criminal responsibility' the current debate in the cyber context is mostly concerned with the application of the law of armed conflict or international humanitarian law (IHL) to CNAs (infra 2). Less intense is the debate regarding a possible criminal responsibility for a crime of aggression (infra 3). Finally, there is virtually no debate regarding the commission of crimes against humanity by way of CNAs but it is worthwhile to take a brief look at this possibility too (infra 4). There are, of course, other issues regarding international criminal responsibility in cyberspace but they must be left to further inquiries.

[*] Agradezco a mi alumno asistente de investigación Torben Schlüter por su colaboración en la preparación de este trabajo y a Muriel Nißle por su asistencia en la revisión final. Traducción del inglés a cargo de Lucas Tassara, Buenos Aires.

Titel: Völkerstrafrechtliche Verantwortlichkeit im Cyberspace
Title: International Criminal Responsibility in Cyberspace

Palabras claves: derecho penal internacional, crímenes de guerra, crimen de agresión, crímenes de lesa humanidad, guerra cibernética, ciberataque
Stichworte: internationales Strafrecht, Kriegsverbrechen, Verbrechen der Aggression, Verbrechen gegen die Menschheit, Cyberkrieg, Cyberangriff
Keywords: international criminal law, war crime, crime of aggression, crimes against humanity, cyber warfare, cyber-attack

Sumario

1. Introducción: alcance de este trabajo y aclaraciones conceptuales

El principal objetivo de este trabajo será brindar una visión confiable sobre el estado de la discusión con respecto a nuestro tema. Esto no es una tarea sencilla debido a la gran incertidumbre, complejidad y dinámica que existe al respecto[1]. En todo caso, teniendo en cuenta el amplio alcance que tienen la "responsabilidad penal" y el "ciberespacio", en primer lugar tenemos que determinar de forma más precisa el ámbito de aplicación de esta investigación. Si bien el "ciberespacio" puede ser definido en términos generales como un ámbito caracterizado por el "uso de la electrónica… y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas en red e infraestructuras físicas asociadas"[2], y por lo tanto, el "ciberdelito" abarca una amplia variedad de actividad criminal por o a través de Internet (desde actividad económica delictiva hasta violaciones de los derechos de autor y pornografía infantil[3]), este trabajo sólo se focalizará en los ataques informáticos a la Red, también conocidos

[1] Esto se admite desde el principio en las publicaciones serias sobre el tema, ver por ejemplo TURNS, «Cyber Warfare and the Notion of Direct Participation in Hostilities», *J.C. & S. L.*, (17), 2012, p. 282 (en donde sostiene que es "bastante difícil escribir con autoridad sobre el derecho internacional y la guerra cibernética: uno tiene la sensación de que la tinta aún no se ha secado en la página…").
[2] Departamento de Defensa de EE.UU., según LIN, «Cyber Conflict and International Humanitarian Law», *IRRC*, (94), 2012, p. 516; igualmente SCHMITT, «Classification of Cyber Conflict», *J.C.& S.L.*, (17), 2012, p. 258. Sobre las diferencias entre el conflicto en el ciberespacio y el espacio físico (i.e. conflicto tradicional) LIN, ibíd., p. 520.
[3] No es sencillo encontrar una definición completa del término "ciberdelito". Frecuentemente se lo usa en forma alternativa con los términos "delito informático", "delitos de índole informática", "delitos tecnológicos" o "ciberdelito". El Convenio sobre cibercriminalidad del Consejo de Europa del 23 de noviembre de 2001 enumera los siguientes supuestos: acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la integridad del sistema, abuso de equipos e instrumentos técnicos, falsedad informática, estafa informática, infracciones relativas a la pornografía infantil e infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines (arts. 2-10). El PA del 28 de enero de 2003 agrega a esta lista aquellos

más brevemente como "ciberataques" [o ataques informáticos]. Un ataque informático es la forma más intensa de lo que puede ser considerado como una guerra cibernética[4], esto es, el uso de medios técnicos para pelear una guerra contra un enemigo en el ciberespacio[5]. Además de los ataques informáticos a la Red existen otras formas de ataques, como las operaciones cibernéticas[6] y el ciberespionaje[7]. El motivo de interés en los ataques informáticos es que por lo general sólo estas formas de delitos cometidos en el ciberespacio son lo suficientemente serias para ser calificadas como crímenes internacionales y, así, quedar cubiertas por una jurisdicción penal internacional como la de la Corte Penal Internacional. Sin embargo, todavía se discute el significado exacto de un ataque informático[8]. Según la opinión mayoritaria deben distinguirse tres elementos. Primero, un ataque informático no se realiza para obtener (directamente) una ventaja financiera o una ganancia, tal como ocurre con los clásicos ciberdelitos económicos[9]. Segundo, el ataque no se realiza con el propósito de obtener información ("ciberespionaje")[10]. Tercero, un ataque informático interrumpe, degrada o destruye una red computarizada y puede llevar a la interrupción de los equipos conectados con la red bajo ataque[11]. Este último elemento

---

actos de racismo y naturaleza xenofóbica cometidos a través de sistemas computarizados. Hay documentos de la UE que adoptan una interpretación igualmente amplia que abarca cualquier conducta que se refiera a "a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica y b) la circulación de datos intangibles y volátiles", ver European Commission, "Fight against cybercrime" (12 de septiembre de 2005) <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_en.htm> consultado el 22 de octubre de 2013. Para una interpretación igualmente amplia desde una perspectiva norteamericana, ver HATHAWAY et al., «The Law of Cyber-Attack», *Cal.L. Rev.*, (110), 2012, pp. 833-834; WEISSBRODT, «Cyber-Conflict, Cyber-Crime, and Cyber Espionage», *Minnesota J. Intl L*, (22), 2013, pp. 366-370.

[4] Sobre las distintas interpretaciones de la "guerra cibernética" en la práctica estatal, DROEGE, «Get off my Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians», *IRRC*, (94), 2012, pp. 536-537. Sobre la explotación de las redes informáticas (CNE) y la defensa de las redes informáticas (CND) ver MELZER, *Cyberwarfare and International Law*, 2011, p. 5.

[5] Ver LIN, *IRRC*, (94), 2012, p. 519 (en donde discute las diferencias entre la guerra tradicional y la ciberguerra con respecto al derecho de los conflictos armados); DROEGE, *IRRC*, (94), 2012, p. 538 (refiere a las "operaciones cibernéticas que son equiparables a o realizadas en el contexto de un conflicto armado…"); también MELZER, *Cyberwarfare*, 2011, p. 4; HARRISSON DINNISS, *Cyber Warfare and the Laws of War*, 2012, p. 4 y ss.

[6] El *Manual de Tallinn* (SCHMITT (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, disponible en <http://www.ccdcoe.org/249.html> consultado el 20 de octubre de 2013, en adelante "Manual de Tallin" de la edición de CUP), probablemente la fuente con mayor autoridad en esta materia, define a una ciberoperación como "la utilización de las capacidades cibernéticas con la finalidad principal de alcanzar sus objetivos en o a través del uso del ciberespacio" (258). Para una crítica sobre el abordaje metodológico del Manual y la composición del grupo experto ver KESSLER/WERNER, «Expertise, Uncertainty, and International Law: A Study on the Tallinn Manual on Cyberwarfare», *LJIL*, (26), 2013, p. 793 (sostiene que "el Manual reduce la incertidumbre a través del consenso sobre determinados temas pero también reproduce o incluso radicaliza la incertidumbre" al hacer "afirmaciones de autoridad ante la falta de consenso" y reintroduce "principios genéricos y factores contextuales en el razonamiento jurídico").

[7] Según el Manual de Tallinn, *Tallinn Manual,* 2013, regla 66 con p. 193, esto significa "cualquier acto realizado clandestinamente o bajo falsas pretensiones que utiliza capacidades cibernéticas para reunir (o intentar reunir) información con la intención de comunicarla a la parte contraria". Ver también WEISSBRODT, «Cyber-Conflict, Cyber-Crime, and Cyber Espionage», *Minnesota J. Intl L*, (22), 2013, pp. 370-371.

[8] Cfr. MCCLURE, «International Adjudication Options in Response to State-Sponsored Cyber-Attacks Against Outer-Space Satellites», *New England J. of Intl & Comparative L.*, (18), 2012, p. 432 (con mayores referencias).

[9] MELZER, *Cyberwarfare*, 2011, p. 21; SWANSON, «The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict», *Loyola L.A.Int'l & Comp.L.J.*, (32), 2010, p. 307 ("... [los delitos informáticos] están regulados por las leyes penales locales e incluyen actos como el robo de identidad y el fraude por internet").

[10] LIN, «Cyber Conflict», *IRRC*, (94), 2012, p. 519; ver también GOLDSMITH, «How Cyber Changes the Laws of War», *EJIL*, (24), 2013, p. 135.

[11] Esta es, básicamente, la definición del Departamento de Defensa de EE.UU. según la cita LUBELL, «Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?», *Int'l L.Stud.*, (89), 2013, p. 258; ver también MELZER, *Cyberwarfare*, 2011), p. 5; LIN, *IRRC*, (94), 2012, pp. 518-519; O'DONNELL/KRASKA, «Humanitarian

es definido con toda claridad por el Manual de Tallinn sobre Guerra Cibernética como: "…una operación cibernética, ofensiva o defensiva, de la que razonablemente se puede esperar que cause lesiones o la muerte de personas, o que dañe o destruya objetos"[12].

El segundo límite se refiere al concepto de la "responsabilidad penal internacional". Esta responsabilidad presupone la existencia de crímenes internacionales y la participación en ellos. El debate actual se concentra principalmente en la aplicación del derecho de los conflictos armados, también conocido –eufemísticamente- como derecho internacional humanitario[13], a los ataques informáticos (infra B). Esto no es llamativo puesto que conforme al art. 36 del Protocolo I adicional a los Convenios de Ginebra los Estados tienen la obligación de determinar la aplicación de las reglas del derecho internacional humanitario para una nueva arma, nuevos medios o métodos de guerra[14]. El debate es menos intenso en relación a la posible responsabilidad penal por un crimen de agresión (infra C). Esto tampoco es llamativo puesto que ha sido codificado recientemente y es poco probable que sea aplicado a corto plazo a los ataques armados tradicionales, mucho menos a los casos de ciberataques. Por último, prácticamente no hay ningún debate con respecto a la comisión de crímenes contra la humanidad mediante ataques informáticos, pero vale la pena realizar una breve mirada a esta posibilidad siguiendo la discusión de los crímenes de guerra (infra D). Por supuesto que hay muchas otras cuestiones relativas a la responsabilidad penal internacional en el ciberespacio, pero no serán tratadas en este artículo. Un tema particularmente complejo y de importancia práctica se vincula con el asunto de la jurisdicción para los ciberataques teniendo en cuenta que estos ataques, por definición, son trasnacionales y, por lo tanto, tras- o supra-jurisdiccionales. De hecho, normalmente estos ataques se originan en una jurisdicción pero afectan a todas las jurisdicciones por las que atraviesa y donde puede producir resultados dañosos. Por lo tanto, la jurisdicción de la Corte Penal Internacional (CPI) se derivaría de la(s) jurisdicción(es) nacionales afectadas por los respectivos ataques informáticos.

Law: Developing International Rules for the Digital Battlefield», *J.C.& S.L.*, (8), 2003, p. 138; crit. sobre el alcance de la definición, LUBELL, op.cit., p. 258 y s.

[12] Manual de Tallinn, *Tallinn Manual,* 2013, Regla 30 (p. 106); para una definición aún mayor, LIN, *IRRC,* (94), 2012, pp. 518-519; ver también DROEGE, *IRRC,* (94), 2012, pp. 556-561 (incluye la interferencia "con el funcionamiento de un objeto al perturbar el sistema informático subyacente", p 560); para una definición demasiado amplia (aunque llamada "restringida"), HATHAWAY et al., *Cal.L.Rev.* (110), 2012, pp. 826 y ss. (basta "cualquier acción… para afectar las funciones de un sistema computarizado…"). Por qué los propios autores consideran que esta es una definición "restringida" es un secreto que sólo ellos saben, el requisito del propósito especial ("propósito político o de seguridad nacional") en todo caso no es suficiente y sus ejemplos también son demasiado genéricos (ibíd., pp. 837 y ss.). Para una discusión sobre distintas operaciones cibernéticas y ataques, ver LÜLF, «International Humanitarian Law in Times of Contemporary Warfare – The New Challenge of Cyber Attacks and Civilian Participation», *Humanitäres Völkerrecht – Informationsschriften*, (26), 2013, pp. 76-77.

[13] El derecho internacional humanitario se refiere a todas las reglas del derecho de los conflictos armados que protegen a los individuos en conflictos armados (O'CONNELL, «Historical Developments and Legal Basis», en FLECK (ed.), *The Handbook of International Humanitarian Law*, 2ª ed., 2008, pp. 1-43, número marginal ["nm."] 101) y a los casos de guerra declarada u ocupación (WERLE/JESSBERGER, *Principles of International Criminal Law*, 3ª ed., 2014, nm. 1092; WERLE, *Völkerstrafrecht*, 3ª ed., 2012, nm. 1078).

[14] Cfr. DÖRMANN, «Applicability of the Additional Protocols to Computer Network Attacks», 2004, p. 2; DROEGE, *IRRC*, (94), 2012, pp. 540-541; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 260-261; BOOTHBY, «Methods and Means of Cyber Warfare», *Int'l L.Stud.*, (89), 2013, p. 400.

2. Ciberataques como crímenes de guerra

2.1. Aclaraciones previas

Actualmente los crímenes de guerra se encuentran definidos en forma exhaustiva en el art. 8 del Estatuto CPI que contiene 51 delitos individuales que se basan, en su totalidad, en las prohibiciones primarias del derecho de La Haya y de Ginebra[15]. De acuerdo con una interpretación estructural y sistemática focalizada en los intereses y derechos protegidos, se puede distinguir entre delitos básicos contra las personas y los bienes protegidos, ataques a la población y bienes civiles (medios de guerra prohibidos) y otros delitos (que incluyen métodos de guerra prohibidos)[16]. Los ciberataques pueden constituir estos delitos si reúnen los requisitos objetivos (*actus reus*) y subjetivos (*mens rea*). Esto no se puede determinar en abstracto sino que depende de las circunstancias concretas de cada caso. A todo evento, la aplicación del régimen de los crímenes de guerra a cualquier forma de ataque –sea a través de los tradicionales medios cinéticos o bien los modernos cibernéticos- supone la existencia de los requisitos generales para la aplicación del derecho internacional humanitario, pues éste contiene las reglas primarias de los crímenes de guerra (secundarios). Por lo tanto, primero se deben analizar estos requisitos generales antes de analizar cómo juegan los principios tradicionales del derecho internacional humanitario en el campo de los ciberataques.

2.2. Requisitos generales

a) Existencia de un conflicto armado

De acuerdo con el art. 2 común de las Convenciones de Ginebra[17], la aplicación del derecho internacional humanitario encuentra su fundamento en la existencia de un conflicto armado. Este término no está definido positivamente en el derecho internacional humanitario escrito, pero el Tribunal Penal Internacional para la ex Yugoslavia (TPIY) ha dado una definición generalmente aceptada en su trascendente decisión sobre la jurisdicción en el caso "Tadic". En consecuencia, "…existe un conflicto armado cuando hay un recurso a la fuerza armada entre Estados, o a la violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados, o entre estos grupos dentro de un Estado"[18]. Por lo tanto, lo que es relevante es el uso de la fuerza armada y su atribución a una de las partes en conflicto[19].

---

[15] Sobre estas reglas primarias, ver AMBOS, *Treatise on International Criminal Law. Volume I: Foundations and General Part*, 2013, p. 11 y ss.

[16] Cfr. AMBOS, *Treatise of International Criminal Law. Volume II: The Crimes and Sentencing*, 2014, p. 164 y ss.

[17] Convenio de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña (aprobado el 12 de agosto de 1949, entrada en vigor el 21 de octubre de 1950) (GC I) 75 UNTS 31 (GC I); Convenio de Ginebra para aliviar la suerte que corren los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar (aprobado el 12 de agosto de 1949, entrada en vigor el 21 de octubre de 1950) 75 UNTS 85 (GC II); Convenio de Ginebra relativo al trato debido a los prisioneros de guerra (aprobado el 12 de agosto de 1949, entrada en vigor el 21 de octubre de 1959) 75 UNTS 135 (GC III); Convenio de Ginebra relativo a la protección debida a las personas civiles en tiempos de guerra (aprobado el 12 de agosto de 1949, entrada en vigor el 21 de octubre de 1950) 75 UNTS 267 (GC IV).

[18] *Prosecutor v Tadic,* TPIY (Jurisdiction) ICTY-94-1-AR (2 de octubre de 1995) [70]; *Prosecutor v Lubanga* (Confirmation of Charges) ICC-01/04-01//06 (29 de enero de 2007) [209]; cfr. WERLE/JESSBERGER, *Principles of ICL*, 3ª ed., 2014, nm. 1078; CASSESE et al., *Cassese's International Criminal Law*, 3ª ed., 2013, p. 66.

[19] Cfr. AMBOS, *Treatise of ICL II*, 2014, p. 123 con mayores referencias en la nota 47.

Los mismos principios se aplican a los ciberataques[20] mientras no exista una definición específica de "guerra" o "conflicto armado" para este tipo de ataques[21]. Así, primero debería distinguirse entre una situación en la que ese ataque es parte de un conflicto armado (convencional) que se está desarrollando, de aquella otra en la que se lleva a cabo en forma independiente de un conflicto de esa naturaleza (i.e. cuando ese conflicto no existe o no es contemporáneo)[22]. Teniendo en cuenta que en el primer supuesto el requisito del conflicto armado de todos modos se ve satisfecho debido al empleo de la fuerza armada convencional, la pregunta sobre una evaluación separada de la cualidad del ataque informático tiene sentido solo en el segundo caso, lo cual podría decirse que configura un ciberataque "puro". En este supuesto se debe determinar si se ha utilizado la fuerza armada[23] y si esto puede ser atribuido a una de las partes en conflicto.

Para establecer si efectivamente se ejerció la *fuerza armada* hay que analizar los medios o instrumentos utilizados –"interpretación con base en los medios"- o los efectos, consecuencias o resultados generados por su utilización –"interpretación con base en los efectos (equivalentes)"[24]. Según el primer abordaje, sería difícil considerar a un ataque informático como un uso de la fuerza "armada" en el sentido tradicional puesto que carece de toda expresión cinética de la fuerza[25]. Sin embargo, esta interpretación no sólo ignora el entendimiento moderno del uso de la fuerza que no se focaliza en las armas utilizadas[26], sino que tampoco logra captar la calidad especial de los ciberataques que se pone de manifiesto en los efectos de esos ataques en

---

[20] DROEGE, *IRRC,* (94), 2012, pp. 543 y ss.; HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 126 y ss.; generalmente más cauto LIN, *IRRC,* (94), 2012, pp. 515 y ss. (quien concluye que muchas de las supuestos del derecho internacional humanitario "...no son válidos en el ciberespacio o solo son aplicables con dificultad", p. 530).

[21] Para una versión más amplia sobre el concepto de "guerra", ver el Anexo 1 del Acuerdo entre los gobiernos de los Estados Partes de la Organización de Cooperación de Shangai en el ámbito de la seguridad internacional de la información (aprobado el 16 de junio de 2009) citado en MELZER, *Cyberwarfare,* 2011, p. 22 y DROEGE, *IRRC,* (94), 2012, p. 535. Este Anexo define a la "guerra de la información" como "la confrontación entre dos o más estados en el espacio de la información dirigida a dañar los sistemas, procesos y recursos, las estructuras críticas y de otro tipo de la información, debilitando los sistemas políticos, económicos y sociales, efectuando un lavado de cerebros psicológico en masa para desestabilizar a la sociedad y el estado, así como para obligar al estado a tomar decisiones en el interés de una parte contraria".

[22] HARRISON DINNISS, *Cyber Warfare*, 2012, p. 127 y ss., distingue entre tres tipos de situaciones: durante un conflicto armado en curso, independiente de tal conflicto armado y el uso de la fuerza convencional que acompaña pero que no equivale a un conflicto armado. Sin embargo, esta última situación puede ser agrupada junto con la primera puesto que en ambos casos los ataques convencionales armados y los ataques cibernéticos ocurren junto con un menor grado de fuerza convencional en la última situación. Para MELZER, *Cyberwarfare,* 2011, p. 24, la operaciones cibernéticas "que no están acompañadas de la amenaza o del uso de la fuerza militar convencional" normalmente no superarían el umbral del conflicto armado pero "posiblemente serían consideradas como una amenaza criminal que deba ser tratada a través de medidas de aplicación de la ley".

[23] En la medida en que la diferencia entre "ataque" (según la definición del art. 49 (1) PA I) y el concepto más amplio de la "operación" militar (ver por ejemplo art. 54 (1) PA I; sobre esta discusión ver DROEGE, *IRRC,* (94), 2012, pp. 554 y ss.) no sea relevante puesto que en ambos casos se exige el empleo de la fuerza armada. Sin embargo, con respecto al principio de distinción (art. 48, PA I), ver infra nota 89.

[24] Los tres criterios relevantes (instrumentalidad, objetivo y con base en las consecuencias/efectos) han sido desarrollados con respecto al concepto *ius ad bellum* de un "ataque armado" (art. 51 Carta ONU) (ver HATHAWAY et al., *Cal.L. Rev.,* (110), 2012, pp. 845-846; WEISSBRODT, *Minnesota J. Intl L,* (22), 2013, pp. 363-364) pero también puede ser aplicado en el contexto *ius in bello* del umbral del conflicto armado.

[25] Sobre las diferencias entre la guerra tradicional y la guerra cibernética, ver: LIN, *IRRC,* (94), 2012, pp. 520 y ss.; ver también MELZER, «Cyber Operations and Ius in Bello», *Disarmament Forum*, (4), 2011, p. 5.

[26] Cfr. *Legalidad de la amenaza o el empleo de armas nucleares* (Opinión Consultiva) [1996] ICJ Rep 226 [párr. 39] ("cualquier uso de la fuerza, con independencia de las armas empleadas"); conc. *Manual de Tallinn, Tallinn Manual,* 2013, p. 42; MELZER, *Cyberwarfare,* 2011, p. 13; WEISSBRODT, *Minnesota J. Intl L,* (22), 2013, p. 356; BOOTHBY, *Int'l L. Stud*., (89), 2013, p. 391; sobre el concepto de arma con miras a la ventaja militar obtenida, HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 68-70.

comparación con los ataques armados tradicionales (cinéticos). Por lo tanto, debería seguirse la interpretación vinculada a los efectos[27].

Una interpretación que se base en los efectos producidos no se ve excluida por la definición del "ataque armado" como "acto de violencia contra el adversario" (art. 49 (1), PA I). Ello es así por cuanto la "violencia" también puede producirse por los efectos violentos de un ataque informático que produce un resultado perjudicial permanente[28]. En consecuencia, si un ataque informático logra reemplazar al elemento físico de la red informática atacada[29], entonces satisface el requisito de la fuerza armada o del ataque armado del derecho internacional humanitario[30]. Esto confirma que la cuestión decisiva no es la naturaleza del ataque en términos de sus medios, sino de sus efectos. Por el contrario, ello implica que un ataque informático que no cause ningún daño físico (permanente) o funcionalmente serio (e.g. un apagón/colapso temporal de un sistema computarizado) no satisface la exigencia del conflicto armado[31]. Por supuesto que los efectos del ataque deben ser considerados en sentido amplio. Si bien un ataque informático solo puede producir un daño limitado al sistema atacado como tal, lo cierto es que sus efectos más amplios pueden producir serias consecuencias, como sería, por ejemplo, el caso de una gran represa que estuviese controlada por este sistema y su desactivación implique vastas inundaciones. Por lo tanto, la pregunta siempre consiste en establecer si un ciberataque produce un daño comparable o análogo al que causa un ataque armado tradicional[32]. En este sentido, inclusive el mismo tratamiento de la "destrucción total o parcial, captura o neutralización" del art. 52 (2) del PA I parece sugerir una interpretación más flexible puesto que indica que la neutralización de un objetivo militar puede producir una ventaja militar, y así tener el mismo efecto que la destrucción de ese objetivo[33]. De hecho, los redactores del art. 52 (2) del PA I consideraban que un ataque "con el propósito de impedir al enemigo el uso de un bien" puede tener el mismo efecto militar

---

[27] Manual de Tallinn, *Tallinn Manual,* 2013, p. 107; en el mismo sentido, ALDRICH, «The International Legal Implications of Information Warfare», *Airpower Journal*, (10), 1996, p. 99; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 123 y 131-132; SCHMITT, «Cyber Operations and the Jus in Bello: Key Issues», *Int'l L. Stud*, (87), 2011, pp.92 y ss.; MELZER *Cyberwarfare,* 2011, p. 24; EL MISMO, *Cyberwarfare,* 2011, p. 5 (con mayores referencias); HASLAM, «Information Warfare: Technological Changes and International Law», *J.C.& S.L*, 2000, p. 170; LÜLF, «IHL», *Humanitäres Völkerrecht*, 2013, pp. 77-78 (quien también se concentra en los efectos de una operación cibernética y sostiene que alcanza el umbral "siempre que" "ponga en peligro a las personas o bienes protegidos" y "sea más que un incidente esporádico y aislado…"); BOOTHBY, *Int'l L. Stud*., (89), 2013, p. 389 ("factor crítico… efecto dañino o perjudicial…"), p. 402; DÖRMANN, « Additional Protocols», 2004, p. 3 ("grado de daño"); LUBELL, *Int'l L.Stud*., (89), 2013, pp. 262-363, 265 y 275 ("efectos violentos", "daño causado"); WEISSBRODT, *Minnesota J. Intl L*, (22), 2013, p. 364 (respecto al ataque armado); HATHAWAY et al., *Cal.L. Rev.,* (110), 2012, pp. 847-848; crit. por considerarlo un umbral demasiado alto, HINKLE, «Countermeasures in the Cyber Context: One More Thing to Worry About», *YJIL Online*, (37), 2011, pp. 11-12 y 21 (con respecto al supuesto ataque cibernético ruso en Estonia en 2007); crit. por las incertidumbres con respecto a la aplicación concreta, KESSLER/WERNER, *LJIL*, (26), 2013, p. 808.

[28] En el mismo sentido, SCHMITT, «Cyber Operations», *Int'l L. Stud*, (87), 2011, pp. 93-94; MELZER, *Cyberwarfare,* 2011, p. 26

[29] Manual de Tallinn, *Tallinn Manual,* 2013, p. 106.

[30] SCHMITT, *Int'l L. Stud*, (87), 2011, p. 93; ver también DINSTEIN, «Computer Network Attacks and Self-Defense», *Int'l L. Stud*, (76), 2002, p. 103; MELZER, *Disarmament Forum*, (4), 2011, p. 7.

[31] MELZER, *Disarmament Forum*, (4), 2011, p. 7; SCHMITT, *Int'l L. Stud*, (87), 2011, p. 95; igualmente: SWANSON, *Loyola L.A.Int'l & Comp.L.J.*, (32), 2010, p. 323; más detallado el *Manual de Tallinn*, *Tallinn Manual,* 2013, pp. 106-107.

[32] DROEGE, *IRRC*, (94), 2012, p. 546.

[33] Cfr. DÖRMANN, «Additional Protocols», 2004, p. 4, 6; crit. SCHMITT, *Int'l L. Stud*, (87), 2011, pp. 95-96 (quien advierte sobre el riesgo de la sobre-inclusividad y sostiene que el art. 52 (2) PA I se basa en la existencia de un "ataque" y que excluiría a las operaciones cibernéticas); HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 197-198; para un enfoque matizado, MELZER, *Cyberwarfare,* 2011, p. 26 (quien sostiene que ambas posiciones tienen puntos sólidos).

que la destrucción de ese bien[34]. En otras palabras, una operación cibernética que deja el objeto físicamente intacto pero que lo neutraliza en su funcionalidad puede equipararse a un ataque militarmente relevante[35], al menos si la operación desarma la "infraestructura crítica" del Estado en cuestión[36]. Por supuesto que aquellas interrupciones menores, como la caída del sistema de emisión de televisión, no constituye un ataque militar; en rigor de verdad normalmente esto produce menos inconvenientes que una guerra económica o psicológica[37] y estas situaciones no encuadran en la definición de un ataque[38]. Los arts. 51 (5) (b), 57 (2) (a) (iii) y 57 (2) (b) del PA I confirman esta postura puesto que sólo mencionan a las consecuencias físicas de los ataques armados[39].

En definitiva, de acuerdo a la interpretación que se basa en los efectos, un ataque informático, tal como fue definido anteriormente, i.e., como un ataque que causa un daño humano considerable o de otro tipo, o una perturbación seria a un sistema computarizado, normalmente equivaldrá a la utilización de la fuerza armada y en consecuencia constituirá un ataque militar relevante[40]. Por supuesto que la cantidad de víctimas por sí solo no convierte a un conflicto en un conflicto armado[41], sino que la calidad de los ataques –en contra de personas y objetos protegidos- siempre juega un rol importante para evaluar la naturaleza del conflicto[42]. Esto habla a favor de la combinación de diferentes factores en donde los efectos son lo más importante, pero en donde la naturaleza y los medios utilizados en el ataque también deben ser tenidos en cuenta[43]. El mismo criterio puede ser aplicado con respecto a la intensidad y duración necesarias –"violencia armada prolongada"[44]- de un conflicto armado (no internacional)[45] que presupone una serie de ataques que duren una considerable cantidad de tiempo[46]. De todos modos, es cuestionable si además se

---

[34] Cfr. DROEGE, *IRRC*, (94), 2012, p. 558.

[35] DROEGE, *IRRC*, (94), 2012, p. 559 ("...operaciones que interrumpen el funcionamiento de los bienes sin daño físico o destrucción, incluso si la interrupción es temporaria"); ver también BOOTHBY, *Int'l L. Stud*., (89), 2013, pp. 389-390 (quien afirma, en relación a los "datos", que sólo se convierten en un "bien" cuando son críticos para la operación del sistema atacado"): LUBELL, *Int'l L.Stud.*, (89), 2013, pp. 265-256 (critica el análisis exclusivo en el daño físico).

[36] Sobre este criterio con definiciones (respecto al *ius ad bellum*), MELZER, *Cyberwarfare,* 2011, pp. 14-16.

[37] SCHMITT, *Int'l L. Stud*, (87), 2011, p. 95; en igual sentido: MELZER, *Cyberwarfare,* 2011, p. 26.

[38] DROEGE, *IRRC*, (94), 2012, p. 559; ver también BOOTHBY, *Int'l L. Stud*., (89), 2013, p. 403 (quien enfatiza que sólo deberían ser considerados la "muerte, lesiones, daño o destrucción de las personas o bienes protegidos"); con respecto a la práctica estatal, SCHMITT, *Int'l L. Stud*, (87), 2011, p. 103.

[39] SCHMITT, «Wired warfare: Computer Network Attack and Ius in Bello», *IRRC*, (84), 2002, pp. 377-378.

[40] SCHMITT, *IRRC*, (84), 2002, p. 374; DROEGE, *IRRC*, (94), 2012, pp. 560 y 578; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 131 y 137-138 (umbral de "gravedad significativa"); MELZER, *Disarmament Forum*, (4), 2011, p. 5; EL MISMO, *IRRC*, (94), 2012, p. 14 (crítico hacia el requisito de la consecuencia similar a los ataques armados tradicionales); Manual de Tallinn, *Tallinn Manual,* 2013, p. 106; HASLAM, «Information Warfare», *J.C.& S.L*, 2000, p. 170; SWANSON, *Loyola L.A.Int'l & Comp.L.J.*, (32), 2010, pp. 314-315.

[41] PICTET (ed.), *Commentary on the Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field* (reimpreso en 2006), 1952, p. 32 ("No importa cuánto dura el conflicto ni cuántas muertes ocurren").

[42] SCHMITT, «Wired warfare», *IRRC*, (84), 2002, p. 373.

[43] Sobre dicho criterio combinado, DROEGE, *IRRC*, (94), 2012, pp. 547-548.

[44] Cfr. Tadic Jurisdictional Decision [70]; incorporado en el art. 8 (2) (f) Estatuto CPI (aprobado el 17 de julio de 1998, entrada en vigor el 1 de julio de 2002, 2187 UNTS 3); ver también SCHMITT, *Int'l L. Stud*, (87), 2011, p. 106.

[45] Cfr. DROEGE, *IRRC*, (94), 2012, p. 551.

[46] MELZER, *Cyberwarfare,* 2011, pp. 24-25 (quien sostiene que aún no se ha definido el umbral preciso); HARRISON DINNISS, *Cyber Warfare*, 2012, p. 131. Para HATHAWAY et al., *Cal.L. Rev.* (110), 2012, p. 850 y GEISS, «Cyber Warfare: Implications for Non-international Armed Conflict», *Int'l L. Stud*, (89), 2013, pp. 633-634, en la práctica todavía no se ha alcanzado el umbral necesario mediante un ataque informático aislado. KESSLER/ WERNER, *LJIL*, (26), 2013, p. 800 generalmente señalan que, aparte del caso Stuxnet, "no ha habido ningún incidente de guerra cibernética que infligiera una devastación y daño generalizado usualmente asociado con la 'guerra'".

exige una intención específica de causar daño y destrucción, y si estas consecuencias deben ser previsibles[47]. Aunque esta "subjetivización" restringiría aun más el criterio con base en los efectos, y en particular evitaría una valoración meramente cuantitativa[48], lo cierto es que parece confundir el requisito *per se* objetivo del conflicto/ataque armado con los requisitos de la responsabilidad penal individual y, en consecuencia, sería teóricamente incoherente. Además de ello traería graves problemas probatorios.

El segundo requisito –la atribución del ataque informático a una de las partes en conflicto- puede ser más difícil de alcanzar. La atribución es prácticamente imposible si el atacante no puede ser identificado, i.e., el ataque se realiza en el anonimato de Internet y no puede ser rastreado a un usuario específico perteneciente a una de las partes en conflicto[49]. Pero, incluso, cuando el ataque es realizado por individuos o grupos identificables se plantea la cuestión de si esto los califica como partes de un conflicto, o si sus actos pueden ser atribuidos a una de las partes en conflicto, en particular a un Estado. Con relación a la primera pregunta, la respuesta dependerá del grado suficiente de organización de estos grupos, i.e., que cumplan con los requisitos de comando, control, disciplina y jerarquía característicos para los grupos armados del derecho internacional humanitario[50]. Aquellos grupos de personas ("hackers") con una existencia meramente virtual normalmente carecen de estas características[51], y tampoco satisface el requisito de la organización un ataque colectivo espontáneo (como un ataque de denegación de servicio) que va aumentando sus seguidores *online*[52]. En cuanto a la posible atribución de los actos de estos grupos a un Estado, las reglas de la Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos ("Responsibility of States for Internationally Wrongful Acts")[53] brinda una guía de utilidad[54]. Por consiguiente, en este contexto es irrelevante que un Estado culpe a los hackers privados por los ataques informáticos desde su territorio con el fin de eludir su responsabilidad estatal[55], puesto que la existencia de un conflicto armado con las respectivas partes se determinará objetivamente.

---

[47] En este sentido, SCHMITT, *IRRC*, (84), 2002, p. 374 ("con el objetivo de causar tanto la muerte, lesiones, daño o destrucción… o bien esas consecuencias sean previsibles"); también SCHMITT, *Int'l L. Stud*, (87), 2011, pp. 94-95; también enfatiza la intención del atacante, HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 132-133.

[48] En este sentido, MELZER, *Cyberwarfare,* 2011, p. 16.

[49] Cfr. DROEGE, *IRRC*, (94), 2012, los problemas de atribución a la luz del carácter anónimo del atacante (pp. 541, 543-545); ver también GOLDSMITH, *EJIL*, (24), 2013, pp. 131-132, 134; HINKLE, *YJIL Online*, (37), 2011, pp. 17-18; HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 99-102; KESSLER/WERNER, *LJIL*, (26), 2013, p. 799.

[50] Para una definición, ver AMBOS, *Treatise of ICL II*, 2014, pp. 125-126; en nuestro contexto SCHMITT, *Int'l L. Stud*, (87), 2011, pp. 105-106; GEISS, *Int'l L. Stud*, (89), 2013, p. 634; HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 124-125.

[51] DROEGE, *IRRC*, (94), 2012, pp. 550-551; GEISS, *Int'l L. Stud*, (89), 2013, pp. 635-636; MELZER, *Cyberwarfare,* 2011, p. 24; aparentemente con una visión distinta, M. SCHMITT, «Classification of cyber conflict», *J.C.& S.L.*, (17), 2012, p. 256 (quien sostiene que "esos grupos pueden actuar en forma coordinada contra el gobierno… seguir órdenes de un líder virtual y ser altamente organizados").

[52] GEISS, *Int'l L. Stud*, (89), 2013, p. 635.

[53] Cfr. CDI, Artículos sobre responsabilidad del Estado por hechos internacionalmente ilícitos, con comentarios (2001) Informe de la Comisión de Derecho Internacional, 53° período de sesiones (23 de abril a 1° de junio y 2 de julio a 10 de agosto de 2001) UN Doc A/56/10 (2001), p. 20, arts. 4-9 (en donde se establecen las reglas de atribución de los actos de órganos estatales o de grupos o agentes privados al Estado). Sobre el test del control efectivo vs. el control general (CIJ Nicaragua vs. TPIY Tadic) en este contexto, ver SCHMITT, *Int'l L. Stud*, (87), 2011, pp. 104-105. Discute posibles contramedidas ("recíprocas"), HATHAWAY et al., «Cyber-Attack», *Cal.L. Rev.* (110), 2012, pp. 857-859; HINKLE, *YJIL Online*, (37), 2011, pp. 14 y ss.; con relación al *ius in bello*, HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 75 y ss.

[54] DROEGE, *IRRC*, (94), 2012, p. 544.

[55] Cfr. GOLDSMITH, *EJIL*, (24), 2013, p. 135.

b) Alcance geográfico del conflicto armado

En un conflicto armado internacional entre dos o más Estados, normalmente las hostilidades tienen lugar en el territorio de estos Estados, o al menos en uno de ellos (por ejemplo, en el caso de la invasión a un Estado). Con respecto a un conflicto armado que no sea de índole internacional, el art. 3 común a los cuatro Convenios de Ginebra exige que el conflicto ocurra "en el territorio de una de las Altas Partes Contratantes". Otras normas[56] y la jurisprudencia internacional confirman que debe haber algún vínculo territorial, o nexo de algún tipo. En este sentido, la decisión sobre la jurisdicción en el caso "Tadic" se refirió a la violencia armada "dentro de un Estado"[57], y la Sala de Cuestiones Preliminares de la CPI en el caso "Bemba" hizo mención a "los límites territoriales de un Estado"[58].

Sin embargo, los ataques cibernéticos desafían todos los límites geográficos o fronteras impuestas por los territorios estatales[59]. Ello es así porque se pueden originar en un dispositivo móvil que se esté desplazando entre diferentes Estados, pasar a través de uno o más servidores ubicados en otros Estados y finalmente alcanzar su objetivo inclusive en otro Estado mas. Si cada dispositivo o red involucrada en el ciberataque se convierte en un objetivo militar pasible de ser atacado, entonces se llegaría a una suerte de "guerra cibernética total", con lo cual se romperían todos los límites geográficos del campo de batalla[60] produciendo "graves efectos desestabilizadores en las relaciones entre los Estados"[61]. De todos modos, con la focalización en los efectos de los ataques informáticos no se reduce el riesgo de una propagación semejante de la violencia cibernética[62] por cuanto los contra-ataques siempre se dirigirán contra las computadoras, dispositivos o redes, probablemente desperdigados a lo largo de diferentes territorios, que causaron los efectos mencionados. Sólo sería posible una limitación si el ataque cibernético pudiese ser rastreado hasta la computadora o dispositivo en donde se originó, y sólo si éste pudiese ser un objetivo legítimo de un contra-ataque.

c) Nexo entre un ataque a la red informática y el conflicto armado

Según el derecho internacional humanitario convencional, el crimen de guerra respectivo debe tener relación con el conflicto armado[63]. De todas formas, este llamado requisito del nexo ha sido interpretado en forma amplia, i.e., es suficiente una relación funcional entre los respectivos actos y el conflicto, pero no es suficiente que los crímenes en cuestión hayan sido cometidos

[56] Cfr. art 1 Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la Protección de las Víctimas de los Conflictos Armados no Internacionales (aprobado el 8 de junio de 1977, entrada en vigor el 7 de diciembre de 1978) 1125 UNTS 609 (PA II), art. 8(2) (f) Estatuto CPI.
[57] Supra nota 16 y texto principal. Ver también *Prosecutor v Blaskić* (Judgement) ICTY-95-14-T (3 de marzo de 2000) [63]- [64]; *Prosecutor v Hadžihasanović and Kubura* (Judgement) ICTY-01-47-T (15 de marzo de 2006) [14]; *Prosecutor v Limaj et al.*(Judgement) ICTY-03-66-T (30 de noviembre de 2005) [84]; *Prosecutor v Milutinović et al.* (Judgement) ICTY-05-87-T (26 de febrero de 2009) [127]; *Prosecutor v Perišić* (Judgement) ICTY-04-81-T (6 de septiembre de 2011) [72].
[58] *Prosecutor v Bemba* (Confirmation of Charges) ICC-01/05-01/08 (15 de junio de 2009) [231].
[59] GEISS, *Int'l L. Stud*, (89), 2013, p. 637; GOLDSMITH, *EJIL*, (24), 2013, p. 131.
[60] DROEGE, *IRRC*, (94), 2012, pp. 565-566.
[61] GEISS, *Int'l L. Stud*, (89), 2013, p. 640.
[62] HARRISON DINNISS, *Cyber Warfare*, 2012, p. 135.
[63] Tadic Jurisdictional Decision [70]; *Prosecutor v. Aleksovski* (Judgement) ICTY-95-14/1-T (25 de junio de 1999) [45]; *Prosecutor v. Musovic et. al.* (Judgement) ICTY -96-21-T (16 de noviembre de 1998) [193]; ver también, WERLE/JESSBERGER, *Principles of ICL*, 3ª ed., 2014, nm. 1109 y ss. (con más referencias).

únicamente en ocasión del conflicto armado aprovechando el caos resultante[64]. Además, para determinar el nexo deben tenerse en cuenta una serie de factores[65].

Sin lugar a dudas un ataque informático requiere un nexo con un conflicto armado que se esté llevando a cabo[66]. Se puede considerar que ese nexo está presente si, al igual que lo exige el derecho internacional humanitario convencional[67], el autor no hubiese podido realizar el ataque sin el conflicto armado.

d) Agente responsable

Cualquier persona, incluyendo un contratista privado que actúe en nombre de una de las partes del conflicto, puede cometer un crimen de guerra[68]. En el contexto cibernético la participación de los civiles tiene una relevancia particular, puesto que en esta área es indispensable el recurso y la dependencia en los conocimientos civiles especializados[69]. Estos civiles pueden ser miembros formales de las fuerzas armadas, incluyendo las fuerzas irregulares en el sentido del art. 4 (A) (2) del III Convenio de Ginebra, y como tales poseen estatus como combatientes[70] y prisioneros de guerra[71]. Lo mismo se aplica a los miembros de los grupos armados[72] y a los intervinientes de un "levantamiento masivo"[73]. Aunque también el personal contratista puede ser asimilado a los mercenarios que no tienen estatus como combatientes, ni como prisioneros de guerra[74].

En todos los otros casos los civiles pierden la inmunidad de ataque si "participan directamente en las hostilidades"[75]. Por lo general, este es el caso cuando cumplen con los siguientes tres requisitos mínimos[76]: (1) el acto en cuestión debe afectar negativamente la capacidad militar del

64 AMBOS, *Treatise of ICL II*, 2014 , p. 141.
65 *Prosecutor v Kunarac, Kovac & Vokovic* (Appeals Judgement) ICTY-96-23 & ICTY-96-23/1-A 12 de junio de 2002 [59] ("…toma en cuenta, *inter alia*, los siguientes factores: que el perpetrador sea un combatiente, que la víctima no sea un combatiente, que la víctima sea un miembro de un partido de la oposición, que se pueda decir que el acto sirve al fin último de la campaña militar, y que el delito sea cometido como parte o en el contexto del ejercicio de las funciones oficiales del agente"). Coincidente: *Prosecutor v Katanga & Ngudjolo Chi* (Confirmation of Charges) ICC-01/04-01/07-717 (30 de septiembre de 2008) [382].
66 Manual de Tallinn, *Tallinn Manual,* 2013, p. 76; también MELZER, *Cyberwarfare,* 2011, p. 23.
67 En este sentido, ver WERLE/JESSBERGER, *Principles of ICL*, 3ª ed., 2014, nm. 1111.
68 PICTET (ed.), *Commentary on the Geneva Convention relative to the Protection of Civilian Persons in Time of War* (reimpreso en 1994), 1958, p. 212; WERLE/JESSBERGER, *Principles of ICL*, 3ª ed., 2014, nm. 1113; Manual de Tallinn , *Tallinn Manual,* 2013, p. 77.
69 TURNS, *J.C. & S. L.*, (17), 2012, pp. 289-290 (con una distinción útil sobre las funciones a cumplir); HATHAWAY et al., «Cyber-Attack», *Cal.L. Rev.* (110), 2012, p. 854; LÜLF, «IHL», *Humanitäres Völkerrecht*, 2013, p. 79.
70 Esto funciona en ambos sentidos: se beneficiarían del privilegio de los combatientes (inmunidad de persecución por actos ilícitos de guerra) pero también serían objetivos legítimos, i.e., perderían la inmunidad civil.
71 En el caso del art. 4 A (2) CG III deben satisfacer los cuatro requisitos allí indicados; ver generalmente, MELZER, *Cyberwarfare,* 2011, p. 34; TURNS, *J.C. & S. L.*, (17), 2012, p. 290; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 140 y ss.
72 MELZER, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 2009, p. 31; conc. SCHMITT, *Int'l L. Stud*, (87), 2011, p. 98. Sobre los criterios ver supra nota 48 con el texto principal.
73 Cfr. art. 4 A (6) CG III.
74 Cfr. art. 47 (2) PA I ; ver también, HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 172-175; TURNS, *J.C. & S. L.*, (17), 2012, p. 294.
75 Cfr. arts. 3 CG I-IV, 51 (3) PA I, 13 (3) PA II y regla 35 del Manual de Tallinn, *Tallinn Manual,* 2013,
76 Estos criterios resultaron del proceso de consultas del Comité Internacional de la Cruz Roja, cfr. MELZER, *Interpretive Guidance*, 2009, p. 46; conc. SCHMITT, *Int'l L. Stud*, (87), 2011, p. 101; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 165-166; ver también AMBOS, *Treatise of ICL II*, 2014 , p. 156; TURNS, *J.C. & S. L.*, (17), 2012, p. 286.

adversario o causarle un daño sustantivo (límite del daño); (2) existe una relación directa entre el acto y el daño causado (causalidad directa); (3) el acto debe estar relacionado con las hostilidades (nexo de beligerancia)[77]. Estos criterios también pueden ser aplicados en el contexto cibernético, aunque allí hay algunos cuestionamientos específicos de esta área, por ejemplo, en cuanto al modo para distinguir a los civiles que han realizado alguna actividad cibernética de aquellos civiles ordinarios[78]. Por supuesto que para determinar si un civil toma parte directa habrá que considerar las circunstancias de cada caso específico[79], en donde un claro ejemplo sería el del civil que prepara y activa un virus para ser enviado a una red informática de otro Estado, puesto que en este caso el civil estaría realizando un ataque cibernético[80]. Además, por lo general habría una participación directa si el ataque no hubiese sido posible sin los conocimientos especiales del civil[81]. Por el contrario, no habría participación directa si el civil sólo brindara una función de soporte meramente inferior[82], o si solo pusiera un virus a disposición en Internet[83].

Aquí surge de nuevo el interrogante, ya discutido anteriormente con respecto al requisito de la atribución, sobre cómo tratar a un grupo de hackers que organiza una actividad de resistencia espontánea y ataca los sistemas informáticos de una fuerza ocupante. ¿Puede considerarse a este grupo de personas como un grupo armado organizado en los términos definidos más arriba[84], y podría ser atacado por ese motivo[85]? ¿Podrían atribuirse sus actos a una de las partes del conflicto? ¿Equivale esa actividad a un "levantamiento masivo" mencionado previamente? Esto llevaría a considerar a las computadoras o al software de los hackers como "armas" que son llevadas "a la vista" (art. 4 (A) (6), III Convención de Ginebra), y a su conducta como un acto espontáneo de resistencia[86].

Finalmente, y con respecto a la duración de la participación ("mientras dure") y el retiro (definitivo) de un interviniente cibernético, los problemas tradicionales[87] incluso se ven

---

También han sido adoptadas por el Manual de Tallinn, *Tallinn Manual,* 2013, pp. 119-120. Para un tratamiento más profundo, ver HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 161 y ss.

[77] Este último criterio descarta la conducta puramente delictiva, cfr. Manual de Tallinn, *Tallinn Manual,* 2013, p. 120.

[78] Cfr. MELZER, *Cyberwarfare,* 2011, pp. 29-30; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 145 y ss. (con referencias especiales al art. 44 (3) PA I).

[79] Sobre la discusión al respecto, ver TURNS, *J.C. & S. L.*, (17), 2012, pp. 286-289, 294-295 (quien demuestra la incertidumbre de estos criterios y presenta un cuadro útil con posibles ejemplos).

[80] Manual de Tallinn, *Tallinn Manual,* 2013, p. 120 con más ejemplos; ver también LIN, *IRRC,* (94), 2012, , p. 526; Harrison Dinniss, *Cyber Warfare*, 2012, p. 167.

[81] Cfr. MELZER, *Interpretive Guidance*, 2009, p. 53 ("…en donde el conocimiento de un civil particular fuese de un valor muy excepcional y que puede ser decisivo para el resultado de un conflicto armado").

[82] DOSWALD-BECK, «Some Thoughts on Computer Network Attack», *Int'l L. Stud.*, (76), 2002, p. 171 (sostiene que los técnicos que "efectivamente realizaron los ataques" serían considerados civiles que toman intervención directa en las hostilidades y en consecuencia estarían sujetos al contraataque sin el derecho al estatus de prisionero de guerra según el art 4 (4) CG III); conc. DÖRMANN, «Additional Protocols», 2004, p. 9 ("ejecución" de un ataque informático versus el mero mantenimiento de la red informática); TURNS, *J.C. & S. L.*, (17), 2012, p. 293; para un enfoque más equilibrado, ver HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 167-172 (quien excluye solamente "el mantenimiento de los sistemas de rutina").

[83] Manual de Tallinn, *Tallinn Manual,* 2013, p. 120.

[84] Supra nota 47.

[85] Sobre la discusión al respecto, ver SCHMITT, *Int'l L. Stud*, (87), 2011, pp. 98-101 (quien identifica como casos difíciles aquellos de personas que actúan con un propósito común).

[86] Bastante escéptico TURNS, *J.C. & S. L.*, (17), 2012, p. 293; ver también MELZER, *Cyberwarfare,* 2011, p. 34 (quien cuestiona el modo en que debe interpretarse el requisito del "portar armas a la vista").

[87] Cfr. AMBOS, , *Treatise of ICL II*, 2014 , pp. 157 y ss.

magnificados en el contexto cibernético. Si se considerara suficiente que un partícipe cibernético interrumpiera su actividad por un momento –haciendo un paralelo con un retiro (temporal) del campo de batalla- sería prácticamente imposible contra-atacarlo puesto que el ataque cibernético dura sólo algunos minutos y el campo de batalla virtual, en cualquier caso, sería la computadora privada del hacker en su domicilio. Por este motivo, la duración de la participación debería prolongarse en la medida en que el partícipe realice repetidas operaciones cibernéticas[88].

3. Principios del derecho internacional humanitario

La comisión de un crimen de guerra concreto depende, en gran medida, de la interpretación que se efectúe de los principios tradicionales del derecho internacional humanitario, i.e., los principios que regulan el desarrollo de las hostilidades[89], en particular, los principios de distinción, proporcionalidad y precaución[90]. Esto no difiere con relación a los ataques cibernéticos o, en términos más amplios, con las operaciones cibernéticas[91] que se califican como "hostilidades" en este sentido[92]. Así, por ejemplo, a fin de poder determinar si se ha cometido el crimen de guerra de ataque intencional contra bienes civiles (art. 8 (2) (b) (ii), Estatuto CPI) a través de un ataque informático, deben distinguirse los objetivos civiles de los militares. Igualmente, para poder establecer si un ataque informático causa un daño colateral desproporcionado debe precisarse cuál es el sentido de la proporcionalidad en este contexto.

3.1. Principio de distinción

La distinción, por un lado, entre civiles y combatientes, y por el otro, entre objetivos civiles y militares, constituye la esencia del derecho internacional humanitario y está consagrada en el art. 48, PA I[93]. Es "parte del derecho internacional consuetudinario aplicable tanto a los conflictos armados internacionales como a los no internacionales"[94]. Con frecuencia este principio es

[88] SCHMITT, *Int'l L. Stud*, (87), 2011, p. 102; la cuestión fue controversial en el grupo de expertos de Tallin, cfr. Manual de Tallinn, *Tallinn Manual,* 2013, pp. 121-122.

[89] Según el Comité Internacional de la Cruz Roja, "el concepto de 'hostilidades' se refiere al recurso (colectivo) de las partes del conflicto a los medios y métodos para causar daño al enemigo, y puede ser descripto como la suma total de todos los actos hostiles llevados a cabo por individuos que participan directamente en las hostilidades" (MELZER, *lnterpretive Guidance*, 2009, pp. 43, 44).

[90] Sobre la prohibición de la perfidia (art. 37 PA I) y la difícil delimitación de los ardides legales en nuestro contexto, ver DOSWALD-BECK, *Int'l L. Stud.*, (76), 2002, p. 171; DÖRMANN, «Additional Protocols», 2004, pp. 10-12; MELZER, *Cyberwarfare,* 2011, pp. 32-3; más recientemente HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 261-265, 278; BOOTHBY, *Int'l L. Stud.*, (89), 2013, p. 404.

[91] Estos principios se aplican no sólo en el contexto de los "ataques" (en el sentido del art. 49 (1) PA I) sino también en el contexto más amplio de las "operaciones militares" tal como se desprende claramente del art. 51 (1) y 57 (1) PA I que se refiere explícitamente al último (Cfr. HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 196 y ss.; en el mismo sentido DROEGE, *IRRC*, (94), 2012, pp. 555-6; MELZER, *Cyberwarfare,* 2011, p. 27; sin embargo, señala la diferencia, SCHMITT, *Int'l L. Stud*, (87), 2011, p. 91-3 (quien sostiene que la "operación" del art. 48 PA I debe ser entendida como "ataque"); LUBELL, *Int'l L.Stud.*, (89), 2013, p. 261; en el mismo sentido la mayoría de los redactores del Manual de Tallinn, *Tallinn Manual,* 2013, p. 177 [con respecto al art 58 (c) PA I]).

[92] El umbral es más bajo que el que se exige para el "ataque" (art. 49 (1) PA I, supra nota 26 y texto principal), cfr. MELZER, *Cyberwarfare,* 2011, pp. 28-9.

[93] El art 48 PA I dice: "A fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, 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".

[94] HENCKAERTS/DOSWALD-BECK, *ICRC Study on Customary International Humanitarian Law, Volume I: Rules*, 2005, p. 25; ver también ibíd. regla 1-10 con pp. 3 y ss.

decisivo para determinar si los ataques a personas o bienes pueden ser calificados como crímenes de guerra, o actos ilícitos, en un conflicto armado. También se aplica a los ataques cibernéticos[95], en donde el término "ataque" debe ser precisado de acuerdo al criterio basado en los efectos discutido anteriormente[96]. Con respecto a los civiles que no son miembros formales de las fuerzas armadas ni de un grupo armado organizado, surge la cuestión de la "participación directa" recientemente tratada que los convierte, eventualmente, en objetivos militares.

Con relación a la distinción entre bienes civiles y objetivos militares existen problemas particulares de delimitación[97]. El término "bienes de carácter civil" es definido en el art. 52 (1) PA I en forma negativa, i.e., "todos los bienes que no son objetivos militares". 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*"[98]. Este examen doble con base en los términos "eficazmente" y "definida" es sumamente controvertido. El Comité Internacional de la Cruz Roja define al requisito de la "contribución eficaz" en forma bastante estrecha y lo limita a los objetivos puramente militares, con lo cual excluye a aquellos que producen una ventaja incierta[99]. Una visión más amplia, defendida en particular por Estados Unidos, incluye a los ataques contra objetivos que limitan las capacidades de combate y sustentación del enemigo[100]. En última instancia, la decisión debe ser tomada de acuerdo a la naturaleza, ubicación, propósito o uso del objetivo[101], de modo que exprese un nexo cercano entre el bien en cuestión y la acción militar[102]. En consecuencia, la decisión siempre será contextualizada y con base en un análisis caso por caso. Por ejemplo, si se produce un combate en un área civil, pero en donde los edificios civiles, como las escuelas o iglesias, son tomadas como protección por parte de los combatientes o insurgentes, entonces esos edificios se convierten en objetivos militares[103]. Por supuesto que siempre deben respetarse aquellas prohibiciones absolutas[104], como las referidas a los establecimientos médicos.[105]

Otro problema que surge en este contexto es el de si la información puede ser considerada como un bien protegido. La postura mayoritaria de que el término "bienes" sólo se refiere a los objetos tangibles y visibles, mas no a la información en sí misma[106], se basa en un criterio demasiado

---

[95] Manual de Tallinn, *Tallinn Manual,* 2013, regla 31 y 110.
[96] Supra nota 27 con texto principal.
[97] Ver, en general, con respecto a la distinción entre civiles (personas protegidas) y combatientes (de facto), AMBOS, *Treatise of ICL II*, 2014 , pp. 146 y ss.
[98] Art. 52 (2) PA I (énfasis agregado); puede verse su análisis en HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 184 y ss.; ver también SCHMITT, *Int'l L. Stud*, (87), 2011, p. 380; GEISS, *Int'l L. Stud*, (89), 2013, pp. 639-640.
[99] PILLOUD et al., *Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, 1987, p. 636.
[100] Cfr. art. 52 (2) PA I; ver también SCHMITT, *IRRC*, (84), 2002, p. 381; crit. DROEGE, *IRRC*, (94), 2012, pp. 567-568; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 188-189.
[101] OETER, «Methods and Means of Combat», en FLECK (ed.), *The Handbook of International Humanitarian Law*, 2ª ed., 2008, nm. 442 ("La fórmula usada constituye un criterio general cuya existencia puede ser valorada *in abstracto*").
[102] Cfr. DROEGE, *IRRC*, (94), 2012, p. 562.
[103] DÖRMANN, «§ 11 VStGB», en JOECKS/MIEBACH, *Münchener Kommentar zum Strafgesetzbuch*, vol. 8, 2ª ed, 2013, nm. 54.
[104] Para un debate más amplio sobre esas prohibiciones en nuestro contexto, ver HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 220 y ss.; ver también DÖRMANN, «Additional Protocols», 2004, pp. 6 y ss.
[105] Cfr. art. 19 CG I, art. 18 CG IV, art. 12 PA I; ver también art. 54-56 PA I.
[106] Manual de Tallinn, *Tallinn Manual,* 2013, p. 127.

tradicional que reposa en la antigua interpretación de la regla que se desarrolló cuando la posibilidad de los ataques cibernéticos no era más que un tema de ciencia ficción. Desde una perspectiva moderna, la diferencia entre los bienes físicos y virtuales resulta, al menos en el contexto cibernético, difusa; por lo tanto, en principio, la información debería ser cubierta por la protección[107]. En todo caso, de acuerdo al criterio con base en los efectos debe considerarse el daño causado en forma general, en vez de aquel causado en forma aislada[108].

El principal problema de la aplicación del principio de distinción es la *interconectividad* entre los sistemas informáticos militares y civiles, y, en gran medida, el doble uso que tiene la infraestructura cibernética[109]. Los bienes de doble uso son aquellos que sirven tanto a los propósitos civiles como militares, pero, con arreglo al derecho de los conflictos armados (i.e. una consecuencia del principio de distinción), un bien es de naturaleza civil o militar[110]. De hecho, como regla, los bienes de doble uso son calificados como objetivos militares puesto que normalmente contribuyen a propósitos militares, i.e., el primer requisito de la definición del art. 52 (2) PA I se encuentra satisfecho[111]. Sin embargo, la contribución militar no puede ser presumida sino que debe ser efectivamente demostrada[112].

Dado que no existe una separación clara entre los sistemas informáticos civiles y militares, i.e., cualquier sistema informático puede ser utilizado tanto para propósitos civiles como militares al mismo tiempo o de manera intercambiable, la distinción es "prácticamente imposible" y, por lo tanto, la protección ofrecida por el principio de distinción sería de importancia práctica limitada[113]. Por supuesto que esto también depende de una comprensión más amplia o estrecha del principio, así como de las circunstancias particulares del caso. Por lo general, parece bastante

---

107 En sentido similar, LUBELL, *Int'l L.Stud.*, (89), 2013, pp. 267-268, 271; MELZER, *Disarmament Forum*, (4), 2011, p. 11; ídem., *Cyberwarfare*, 2011, p. 31 (ambos consideran a los datos como "bienes"); HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 184-185 (quien se centra en el objeto y propósito de la operación).

108 En el mismo sentido, SCHMITT, *Int'l L. Stud*, (87), 2011, p. 96.

109 MELZER, *Cyberwarfare,* 2011, p. 30; DROEGE, *IRRC*, (94), 2012, pp. 539, 541; Manual de Tallinn, *Tallinn Manual,* 2013, p. 169; TURNS, *J.C. & S. L.*, (17), 2012, pp. 296-297; HATHAWAY et al., *Cal.L. Rev.,* (110), 2012, pp. 852-853; GOLDSMITH, *EJIL*, (24), 2013, p. 134; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 193-195.

110 Cfr. Manual de Tallinn, *Tallinn Manual,* 2013, regla 39 y p. 134 ("Como cuestión de puro derecho no pueden coexistir el estatus de bien de carácter civil y de carácter militar; es uno o el otro").

111 Cfr. Manual de Tallinn, *Tallinn Manual,* 2013, regla 39 y p. 134 ('…confirma que todos los bienes e instalaciones de doble uso son bienes de carácter militar, sin calificación"); en el mismo sentido, DROEGE, *IRRC,* (94), 2012, pp. 562-563.

112 STEIGER, «Civilian Objects», en WOLFRUM (ed.), *Max-Planck-Encyclopedia of Public International Law*, 2013, nm. 12 ("En la mayoría de los casos, los bienes de doble uso deben ser considerados objetivos militares. Sin embargo, esto sólo es cierto siempre y cuando el bien realice una contribución efectiva a la acción militar por su naturaleza, ubicación, finalidad y uso, y cuando su destrucción ofrezca una clara ventaja militar en las circunstancias del caso"); *ICRC Study 2005*, p. 32 ("En lo que se refiere a las instalaciones de doble uso ... la práctica considera que la clasificación de estos objetos depende, en última instancia, de la aplicación del concepto de objetivo militar"); FENRICK, «Targeting and Proportionality during the NATO Bombing Campaign against Yugoslavia», *EJIL*, (12), 2001, pp. 489, 494 ("En la situación de dependencia. ... los bienes [de doble uso] pueden convertirse en objetivos militares en ciertos conflictos en función de diversos factores, entre los que se incluyen los objetivos estratégicos de las partes en el conflicto y el grado en que el conflicto se acerca a la guerra total"). Para un criterio más equilibrado, ver también GEIß/LAHMANN, «Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space», *Isr.L.Rev.*, (45), 2012, pp. 381, 389 (quienes sostienen que, en el mundo físico, la mayoría de los bienes civiles no tienen ningún tipo de potencial militar significativo y por ende no pueden ser utilizados de manera militarmente propicia).

113 GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, pp. 383, 384-390; en el mismo sentido, DERVAN, «Information Warfare and Civilian Population: How the Law addresses a fear of the Unknown», *GoJIL*, (3), 2011, pp. 373, 388; DROEGE, *IRRC*, (94), 2012, pp. 541, 562-566.

plausible sostener que un sistema computarizado que es en sí mismo civil pierde este estatus si es utilizado como soporte de objetivos militares[114]. Por ejemplo, si una de las partes del conflicto utiliza un sistema informático –per se civil- de un hospital para lanzar ataques cibernéticos, estos sistemas se convierten en objetivos militares[115]. Es más difícil trazar la línea si uno se refiere a toda una infraestructura cibernética, incluyendo a Internet. Como los militares se basan en gran medida en la infraestructura civil para todas sus operaciones[116], incluyendo la preparación y ejecución de un ataque, se puede afirmar que esta infraestructura en sí misma –que comprende a las compañías de tecnología informática que las proveen y las mantienen, o hasta las redes sociales como Facebook o Twitter[117]- realizan una contribución efectiva al esfuerzo militar y por ende su destrucción significa una ventaja militar definida[118]. Una postura aun más amplia podría sostener que semejante uso militar de la infraestructura cibernética civil contamina a esa infraestructura en un grado tal que la convierte en un objetivo militar. En este sentido, el grupo de expertos de Tallinn sostiene que en este tipo de casos en los que no queda claro qué conexiones de Internet se utilizan para las transmisiones militares, entonces toda la Red se califica como un objetivo militar[119]. Si uno va más allá y considera suficiente –en forma contraria a la postura que aquí se defiende[120]- la intención de utilizar una infraestructura cibernética civil con fines militares, entonces en el futuro todo el ciberespacio civil podría constituir un objetivo militar legítimo[121].

Otra consecuencia del principio de distinción es la prohibición de ataques indiscriminados[122], aunque estos difieren de los ataques directos contra bienes civiles en el sentido de que el daño causado al bien que se protege es completamente indistinto para el atacante. Es dudoso sostener que sea posible cumplir con esta prohibición en el caso de los ataques cibernéticos del mismo modo en que ocurre con los ataques tradicionales. Si se considera que no es posible trazar una separación clara entre la infraestructura civil y militar, como se hizo más arriba, un ataque contra una infraestructura cibernética no puede ser considerado claramente como un ataque dirigido "contra un objetivo militar concreto" (art. 51 (4), PA I), ni contra un bien estrictamente civil. Aparte de ello, los medios utilizados en un ataque cibernético, por ejemplo un virus como el Stuxnet dirigido contra las instalaciones militares iraníes, puede no ser lo suficientemente controlable, i.e., por definición sus efectos no pueden ser razonablemente limitados y por ende no puede discriminar[123]. Si este es el caso, entonces el ataque cibernético en cuestión califica como

114 Manual de Tallinn, *Tallinn Manual,* 2013, p. 28.
115 Cfr. LIN, *IRRC* (94), 2012, p. 526.
116 Según DERVAN, *GoJIL,* (3), 2011, p. 388, "se estima que el 98% de todas las comunicaciones gubernamentales clasificadas y el 95% de todas las comunicaciones militares en los EE.UU. se transmiten a través de sistemas de comunicación civiles, y no redes militares específicas".
117 Cfr. Manual de Tallinn, *Tallinn Manual,* 2013, p. 135-137; crit. DROEGE, *IRRC,* (94), 2012, pp. 566-569.
118 GEISS/LAHMANN, *Isr.L.Rev*, 2012, pp. 386, 388-389.
119 Manual de Tallinn, *Tallinn Manual,* 2013, p. 135; cfr. GEISS/LAHMANN, *Isr.L.Rev*, (45), 2012, pp. 388 y ss.
120 Supra nota 46 y texto principal.
121 GEISS/LAHMANN, *Isr.L.Rev*, (45), 2012, p. 386; PILLOUD et al., *Commentary*, 1987, p. 636.
122 Cfr. art 51 (4) PA I: "Se prohíben los ataques indiscriminados. Son ataques indiscriminados: a) los que no están dirigidos contra un objetivo militar concreto; b) los que emplean métodos o medios de combate que no pueden dirigirse contra un objetivo militar concreto; o c) los que emplean métodos o medios de combate cuyos efectos no sea posible limitar conforme a lo exigido por el presente Protocolo; y que, en consecuencia, en cualquiera de tales casos, pueden alcanzar indistintamente a objetivos militares y a personas civiles o a bienes de carácter civil". Ver, en general, *ICRC Study 2005*, reglas 11-13 con p. 37 y ss.
123 BOOTHBY, *Int'l L. Stud.*, (89), 2013, p. 393-4. DOSWALD-BECK, *Int'l L. Stud.*, (76), 2002, p. 169, sostuvo hace más de diez años que el control limitado con respecto a los efectos de un ataque informático era "el problema más serio";

uno de los "métodos o medios de combate cuyos efectos no sea posible limitar"[124]. De hecho, y tal como sostiene correctamente Droege, las partes de un conflicto tienen una doble carga: por un lado, no pueden emplear armas cibernéticas que por su naturaleza sean indiscriminadas y no puedan ser suficientemente controladas; por el otro, en cada caso de un ataque la parte tiene que verificar si el arma utilizada puede ser, y de hecho es, dirigida contra un objetivo militar concreto[125].

En definitiva, el principio de distinción sólo podrá tener un papel más importante si fuese posible separar en forma más clara los bienes civiles de los militares, por ejemplo, con la creación de "refugios digitales", en forma análoga a lo que ocurre con las áreas desmilitarizadas contempladas en el art. 60, PA I[126]. En el estado actual del derecho, los principios de proporcionalidad y precaución, que serán tratados a continuación, parecen ser más útiles para limitar los ataques cibernéticos[127].

3.2. Principio de proporcionalidad

Este principio es parte del derecho internacional consuetudinario tanto para los conflictos armados internacionales como los no internacionales[128]. El mismo establece límites al uso de los medios y métodos de guerra y, en particular, prohíbe aquellos que causen "males superfluos o sufrimientos innecesarios" [129] y "daños extensos, duraderos y graves al medio ambiente natural"[130]. Define a los ataques indiscriminados, más allá del art. 51 (4), PA I, como ataques que causan pérdidas de vidas civiles y daños a los bienes civiles que son "excesivos en relación con la ventaja militar concreta y directa prevista"[131]. En consecuencia, un ataque que produzca ese daño colateral no es ilícito en sí mismo, sino sólo cuando el daño sea excesivo con respecto a la ventaja militar.

---

conc. DÖRMANN, «Additional Protocols», 2004, p. 5; ver también HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 256-257 (discute la cuestión bajo el concepto de las "armas indiscriminadas").

[124] Cfr. art. 51(4) (c) PA I.

[125] DROEGE, *IRRC*, (94), 2012, p. 571.

[126] Para una discusión crítica sobre ésta y otras posibilidades, ver GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, pp. 383, 390-5; ver también DROEGE, «Cyber Warfare» *IRRC*, (94), 2012,. 576-577.

[127] Ver también Manual de Tallinn, *Tallinn Manual,* 2013, regla 39 y pp. 134-135 ("Un ataque a un objetivo militar que también se utiliza para fines civiles está sujeto al principio de proporcionalidad y a la necesidad de tomar precauciones en el ataque"); en el mismo sentido, DERVAN, *GoJIL*, (3), 2011, p. 388.

[128] *ICRC Study 2005,* regla 14 con p. 46-50; Manual de Tallinn, *Tallinn Manual,* 2013, p. 159. Ver también OLÁSOLO, *Unlawful attacks in combat situations: from the ICTY's case law to the Rome Statute*, 2008, pp. 155 y ss., 226 y ss., 256 y ss.; KELLER/FOROWICZ, «A Tightrope Walk between Legality and Legitimacy: An Analysis of the Israeli Supreme Court's Judgment on Targeted Killing», *LJIL*, (21), 2008, pp. 189, 213 y ss.; HANKEL, *Das Tötungsverbot im Krieg: Eine Intervention*, 2011, pp. 22 y ss.; WRIGHT, «'Excessive' ambiguity: analysing and refining the proportionality standard», *IRRC*, (94), 2012, pp. 819, 838 y ss. (se focaliza especialmente en el término ambiguo "excesivo").

[129] Cfr. art. 22 y 23 (e) Anexo a la Convención de la Haya relativa a las leyes y costumbres de la Guerra terrestre y su anexo: regulaciones relativas a las leyes y costumbres de la guerra terrestre (18 de octubre de 1907, entrada en vigor el 26 de enero de 1910); art. 35 (1) y (2) PA I. Ver también HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 252-256. Sobre un posible crimen de guerra, ver art. 8 (2)(b)(iii), (x), (xx) (xxv) y (e)(xi).

[130] Art. 35 (3) PA I; ver también art. 55 PA I (en relación a los objetos protegidos) y BOOTHBY, *Int'l L. Stud.*, (89), 2013, p. 394. Para un posible crimen de guerra, ver art. 8 (2)(b)(iv).

[131] Art. 51 (5)(b) y 57 (2)(a) (iii) y (b) PA I. Para un posible crimen de guerra, ver art. 8 (2)(b)(iv).

El principio también se aplica a los ataques cibernéticos que causan un daño colateral excesivo[132], quizá equivalentes a "males superfluos o sufrimientos innecesarios"[133], ya sea durante la utilización transitoria de la infraestructura civil, o bien a través del ataque mismo[134]. Por el momento, brinda más protección que el principio de distinción, que es estático y menos flexible[135]. De hecho, si se siguiera la postura estricta de que cualquier uso militar potencial de un bien de carácter civil lo transforma en un objetivo militar, el bien en cuestión sería un objetivo lícito y sólo el estándar de la proporcionalidad excesiva brindaría límites posibles a los ataques cibernéticos. Tómese, por ejemplo, el caso de una infraestructura en sí misma de carácter civil, como la red de energía eléctrica de una gran ciudad, que es utilizada sólo en forma limitada para un fin militar, pero que por esta misma razón sería considerada como de doble uso y, por lo tanto, un objetivo lícito. Un ataque informático a esa infraestructura probablemente causaría un impacto civil serio al cortar el suministro eléctrico a los hogares y otros sitios de carácter civil. Si bien este daño "colateral" de carácter civil no es contrario al principio de distinción, debería ser equilibrado con la ventaja militar prevista[136].

Por supuesto que el test de la proporcionalidad sólo podría contrarrestar los efectos adversos de una interpretación estricta del principio de distinción si el daño colateral, o incidental, causado por un ataque a la red informática en sí mismo lícito, i.e., "muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas"[137], fuese interpretado en forma amplia[138]. Por lo tanto, el daño colateral debería abarcar tanto a los efectos directos de un ataque cibernético, como a los indirectos, i.e., las "consecuencias inmediatas, de primer orden" del ataque y las "consecuencias mediatas y/o desplazadas de segundo, tercer y mayor grado… causadas a través de mecanismos o eventos intermedios"[139]. En particular, respecto a los "daños a bienes de carácter civil" incidentales, debe adoptarse una interpretación amplia y dinámica, que incluya en la ecuación de proporcionalidad la mera pérdida de funcionalidad del bien de carácter civil atacado[140]. Para esta evaluación sobre el exceso hay que intentar determinar de la manera más precisa posible los efectos adversos de un ataque informático a la red sobre las actividades cibernéticas civiles, y relacionarlos con la ventaja militar prevista: "La cuestión consiste en si el daño que debe esperarse es excesivo en relación a la ventaja militar prevista de acuerdo a las circunstancias existentes en el momento"[141]. La ventaja militar debe determinarse de un modo

[132] Manual de Tallinn, *Tallinn Manual,* 2013, regla 51 ("Se prohíbe un ataque cibernético que se puede prever que causará pérdidas incidentales de vidas civiles, lesiones a civiles, daños a bienes de carácter civil, o una combinación de ellas, que serían excesivos en relación con la ventaja militar concreta y directa prevista"); ver también GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, p. 395.
[133] BOOTHBY, *Int'l L. Stud.*, (89), 2013, p. 391-2.
[134] Manual de Tallinn, *Tallinn Manual,* 2013, p. 160.
[135] GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, pp. 395-398, 398; ver también DERVAN, *GoJIL*, (3), 2011, p. 389.
[136] Ver también el Manual de Tallinn, *Tallinn Manual,* 2013, p. 160, con el ejemplo del ataque contra el GPS.
[137] Cfr. art. 51 (5)(b) y 57 (2)(a) (iii) y (b) PA I, así como el Manual de Tallinn, *Tallinn Manual,* 2013, regla 51, citado en la nota 132.
[138] GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, pp. 396-397.
[139] Manual de Tallinn, *Tallinn Manual,* 2013, p. 160; ver también GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, p. 396; DROEGE, *IRRC*, (94), 2012, pp. 572-573; BOOTHBY, *Int'l L. Stud.*, (89), 2013, pp. 390, 395, 397-398, 401.
[140] En este sentido GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, pp. 397-398; GEISS, *Int'l L. Stud*, (89), 2013, pp. 644-645. Los expertos del Manual de Tallinn también concuerdan en que una "afectación de la funcionalidad" puede, en ciertas circunstancias, ser incluida (p. 160), aunque explícitamente excluyen a los "daños *de minimis*" (*Tallinn Manual,* 2013, regla 30 con p. 107).
[141] Manual de Tallinn, *Tallinn Manual,* 2013, p. 161; ver también BOOTHBY, *Int'l L. Stud.*, (89), 2013, p. 392.

igualmente preciso ("concreta y directa")[142], tomando en cuenta el ataque como un todo[143] y de forma prospectiva ("anticipada")[144], i.e., el respectivo comandante tiene, por un lado, un "amplio margen de decisión"[145], también con respecto al posible daño colateral, pero, por el otro, enfrenta un test de razonabilidad, i.e., su decisión debe superar un análisis de razonabilidad que considere como estándar relevante el de "una persona razonablemente bien informada en las circunstancias del autor concreto"[146]. Por supuesto, la incertidumbre de los efectos indirectos de segundo, tercer, etc., orden de los ataques cibernéticos hace que sea difícil, sino imposible, para un comandante anticiparse correctamente a las consecuencias del ataque[147]. Sigue siendo controvertido, al igual que en el derecho internacional humanitario tradicional, si una ventaja militar especialmente grande puede superar a un daño particularmente serio o extenso, i.e., si un cierto grado de daño puede significar un límite absoluto en la ecuación de la proporcionalidad[148].

3.3. Principio de precaución

El objetivo general de este principio es el de minimizar los daños civiles en la mayor medida posible, sin perjuicio de cualquier consideración de proporcionalidad como ocurre con el principio recientemente discutido. Este principio tiene dos componentes, i.e., se refiere a las precauciones en el ataque (art. 57, PA I) y a las precauciones contra los efectos de los ataques (art. 58, PA I)[149]. La omisión de adoptar estas precauciones puede convertir en un crimen de guerra lo que de otro modo sería un ataque permitido contra una persona o bien de carácter civil. Respecto a las precauciones en el ataque, el art. 57 (2) PA I, enumera una serie de medidas activas que las partes en un conflicto deben adoptar para preservar a las personas civiles y a los bienes de carácter civil. En el contexto cibernético se debe adoptar un "cuidado constante"[150], verificar los objetivos[151], limitar los posibles efectos incidentales en la mayor medida posible[152] y dar aviso con la debida antelación de que los ataques cibernéticos pueden afectar a la población civil[153]. Los deberes de verificación y limitación pueden implicar, por ejemplo, que antes de atacar a una red informática del adversario haya que evaluarla, y que el ataque, en la medida de lo posible, deba

142 Manual de Tallinn, *Tallinn Manual,* 2013, regla 51, citado supra nota 132, y p. 161-2 ("ventaja… sustancial y relativamente cerca", en relación al Comité Internacional de la Cruz Roja, Comentario PA, [2209]).
143 Cfr. Manual de Tallinn, *Tallinn Manual,* 2013, p. 162.
144 Manual de Tallinn, *Tallinn Manual,* 2013, regla 51, citada supra nota 132, y p. 162-3 ("que la evaluación de la razonabilidad de la decisión al momento del ataque... no se aplique con el beneficio de la retrospectiva").
145 Manual de Tallinn, *Tallinn Manual,* 2013, p. 163, en relación al Comité Internacional de la Cruz Roja, Comentario PA, párr. 2210.
146 *Prosecutor v Galic* (Judgment) ICTY-98-29-T (5 de diciembre de 2003) [58]; ver también *Tallinn Manual*, *Tallinn Manual,* 2013, p. 163 y DOSWALD-BECK, *Int'l L. Stud.*, (76), 2002, p. 167 (ventaja militar "clara y obvia" para el atacante).
147 Sobre la falta de certeza con las consecuencias, ver también HATHAWAY et al., *Cal.L. Rev.* (110), 2012, p. 851; HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 207-208.
148 En este sentido PILLOUD et al., *Commentary*, 1987, [1980]; contra *Tallinn Manual*, *Tallinn Manual,* 2013, p. 161.
149 Sobre su estatus como derecho consuetudinario, ver *ICRC Study 2005*, reglas 15-24 con p. 51 y ss.; ver también DROEGE, *IRRC*, (94), 2012, pp. 573 y ss.; para una perspectiva norteamericana, WRIGHT, *IRRC*, (94), 2012, pp. 830-832.
150 Manual de Tallinn, *Tallinn Manual,* 2013, regla 52.
151 Manual de Tallinn, *Tallinn Manual,* 2013, regla 53; resalta que éste es el principal problema, DOSWALD-BECK, *Int'l L. Stud.*, (76), 2002, pp. 170-171; ver también HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 211-212.
152 Manual de Tallinn, *Tallinn Manual,* 2013, regla 54 ("elección de los medios y métodos de guerra... con el fin de evitar y, en todo caso minimizar, lesiones incidentales a civiles…") y regla 56 (elección de los objetivos con el fin de "que causen el menor peligro para las personas civiles y bienes de carácter civil"). Ver como norma primaria, art. 57 (3) PA I; sobre esta provisión, HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 216-217.
153 Manual de Tallinn, *Tallinn Manual,* 2013, regla 58.

limitarse a sus componentes militares[154]. Incluso, si uno va más allá se puede considerar que estos límites en el ataque están previstos para evitar cualquier efecto incidental (colateral) con miras a la infraestructura cibernética civil[155]. Todo esto exige conocimiento técnico[156]. Sin embargo, está controvertido hasta dónde llegan las obligaciones de precaución. Si bien el estándar normal es el de la "posibilidad"[157], i.e., hacer lo que sea "practicable o prácticamente posible teniendo en cuenta todas las circunstancias"[158], en el caso de las operaciones militares en el mar o en el aire es suficiente las "precauciones razonables" (art. 57 (4) PA I), i.e., se exige menos que la posibilidad[159]. En consecuencia, en el ejemplo de un buque de guerra atacado mediante una operación cibernética existen dos abordajes: una mirada estricta exigiría una evaluación de toda la infraestructura cibernética de este buque a fin de poder anticipar los efectos (incidentales) del ataque; mientras que una mirada más amplia sostendría que esa evaluación no sería razonable puesto que la operación se focaliza en un objetivo que no está en tierra[160].

En cuanto al deber de precaución pasivo de "alejar" a los bienes de carácter civil de los objetivos militares (art. 58 (a) PA I), el problema de la interconectividad anteriormente mencionado hace que sea difícil de cumplir en el ámbito del ciberespacio: si la infraestructura civil y militar están íntimamente conectadas o –peor aun- el ciberespacio es una clásica estructura de doble uso, entonces es prácticamente imposible cumplir con esta obligación, i.e., no es "posible"[161] en el contexto cibernético[162]. El art. 58 (c) PA I exige que se tomen "las demás precauciones necesarias" las cuales dependen, por supuesto, de las posibilidades prácticas ("en la mayor medida posible"[163]). Por lo tanto, el art. 58 (c) es una disposición de "carácter general"[164] que intenta asegurar la protección de la infraestructura cibernética civil a través de otros medios que la separación estricta, i.e., "para asegurar la funcionalidad continua cibernética" con respecto a la infraestructura civil crítica, por ejemplo, brindando copias de seguridad a las redes eléctricas[165].

4. Ataques cibernéticos y el crimen de agresión

Algunos autores sostienen que el hecho de librar un ataque informático puede constituir una violación del *ius ad bellum* y, por lo tanto, generar responsabilidad penal por el crimen de

[154] DROEGE, *IRRC*, (94), 2012, pp. 573-574.
[155] Ver Manual de Tallinn, *Tallinn Manual,* 2013, pp. 169-170, con el ejemplo de la inserción de programas maliciosos en una red militar cerrada como una manera de minimizar los daños colaterales.
[156] DROEGE, *IRRC*, (94), 2012, pp. 574; Manual de Tallinn, *Tallinn Manual,* 2013, p. 166.
[157] Manual de Tallinn, *Tallinn Manual,* 2013, p. 164; ver también art 58 PA I ("en la máxima medida posible") y HARRISON DINNISS, *Cyber Warfare*, 2012, p. 211.
[158] Cfr. Manual de Tallinn, *Tallinn Manual,* 2013, p. 169, con más referencias en la nota 186.
[159] PILLOUD et al., *Commentary*, 1987, p. 2230 ("se deben tomar 'todas las precauciones razonables' lo cual es, sin duda, un poco diferente y tiene menos alcance que la expresión 'tomar todas las precauciones factibles'").
[160] Manual de Tallinn, *Tallinn Manual,* 2013, p. 165, según el cual la mayoría de los expertos tomó la postura más amplia; ver también HARRISON DINNISS, *Cyber Warfare*, 2012, pp. 217-219.
[161] Art. 58 PA I: "hasta donde sea factible".
[162] Cfr. GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, pp. 392-394, concluye que en consecuencia de esta norma no se puede deducir una obligación de distinción; en el mismo sentido, DROEGE, *IRRC*, (94), 2012, p. 575 ("poco realista").
[163] Ver también Manual de Tallinn, *Tallinn Manual,* 2013, regla 59; con una discusión que tiene limitaciones prácticas ("factibilidad") ibíd., pp. 177-178.
[164] Manual de Tallinn, *Tallinn Manual,* 2013, p. 177.
[165] GEIß/LAHMANN, *Isr.L.Rev*, (45), 2012, p. 395; en el mismo sentido, DROEGE, *IRRC*, (94), 2012, p. 576.

agresión según el art. 8 bis (1), Estatuto CPI[166]. Este criterio se basa, por supuesto, en la hipótesis en que el ataque en cuestión es realizado por un Estado ya que el art. 8 bis no incluye la conducta de actores no estatales[167]. En todo caso, es difícil prever un ataque informático que encuadre en el art. 8 bis. Si bien en circunstancias especiales un ataque semejante puede ser equiparado a un "acto de agresión" en el sentido del art. 8 bis (2) lit. (d) Estatuto CPI, lo cierto es que difícilmente pueda ser equiparado a una "violación manifiesta" de la Carta de la ONU tal como lo exige el art. 8 bis (1) Estatuto CPI. Además, y de acuerdo a la llamada cláusula de liderazgo, sólo podría haber responsabilidad penal con respecto a una persona que esté "en condiciones de controlar o dirigir efectivamente la acción política o militar de un Estado" (art. 8 bis (1)). Esto significa que las personas que lleven a cabo efectivamente el ataque informático no serán penalmente responsables de acuerdo al art. 8 bis, sino que, en el mejor de los casos, lo serán sus superiores si pertenecen al nivel de la conducción y pueden ser considerados responsables por los actos de los "soldados informáticos" concretos.

4.1. ¿"Acto de agresión" de acuerdo al art. 8 bis (2) lit. (a)-(g), Estatuto CPI?

El párrafo 2 del art. 8 bis Estatuto CPI exige un análisis en dos etapas. Primero, hay que examinar si un ataque informático es uno de los actos de agresión allí enumerados. Segundo, si ello no fuere así, la pregunta que surge es si la enumeración del párrafo 2 es exhaustiva o no.

Los actos enumerados en el párrafo 2 se basan en el "uso de la fuerza armada" tal como explícitamente se exige al comienzo de su redacción[168]. Según los trabajos preparatorios, el término "fuerza armada" debe ser entendido en sentido estricto, en referencia al empleo de fuerza cinética a través de las armas tradicionales[169]. Si bien durante las negociaciones se sugirió un concepto más amplio que incluyera a los ataques cibernéticos[170], lo cierto es que finalmente fue rechazado para evitar que se afectara "la estabilidad política o económica, o el ejercicio del derecho a la auto-determinación, o que se violara la seguridad, defensa o integridad territorial de uno o más Estados"[171]. Por lo tanto, si bien desde el principio los negociadores aparentemente

---

166 Esta es la posición que representa OPHARDT, «Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield», *Duke Law and Technology Review*, (3), 2010, 3, 35; WEISSBRODT, «Conceptualizing Aggression», *Duke Journal of Comparative and International Law*, (20), 2009, p. 1; WEISBORD, «Judging Aggression», *Colum. J. of Trans. L.*, (50), 2011, p. 82; WEISSBRODT, «Cyber-Crime», *Minnesota J. Intl L*, (22), 2013, p. 369; en igual sentido, CAMMACK, «The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression», *Tulane J. of Intl. & Comp. L.*, (20), 2010, p. 303.

167 Crit. AMBOS , *Treatise of ICL II*, 2014 , pp. 203-204.

168 Esto se corresponde más con el "ataque armado" en el sentido del art. 51 de la Carta de la ONU que con el genérico "uso de la fuerza" en el sentido del art. 2 (4) de la Carta de la ONU (para una comparación, MELZER, *Cyberwarfare,* 2011, pp. 11-12).

169 Cfr. GILLET, «The anatomy of an international crime: Aggression at the ICC», *ICLR*, (13), 2013, pp. 829, 838 (explícitamente excluye a la "guerra cibernética").

170 Cfr. S. S. BARRIGA, «Against the Odds: The Results of the Special Working Group on the Crime of Aggression», en S. BARRIGA/W. DANSPECKGRUBER/C. WENAWESSER (eds.), *The Princeton Process on the Crime of Aggression – Materials of the Special Working Group on the Crime of Aggression*, 2003-2009, 2009, p. 10 ("Se hicieron sugerencias para incluir medios de agresión no convencionales más allá del uso de la fuerza armada, como los ataques cibernéticos o embargos económicos").

171 Cfr. SWGCA, June 2008 Report (junio de 2008), en Assembly of States Parties to the Rome Statute of the International Criminal Court, Official Records, Resumed 6th sess (2-6 junio de 2008) ICC-ASP/6/20/Add.1, Annex II <http://www.icc-cpi.int/iccdocs/asp_docs/ICC-ASP-6-20-Add.1%20English.pdf> consultado el 24 de octubre de 2013, párr. 35). Ver también BARRIGA, en S. BARRIGA *The Princeton Process,* 2003-2009, p. 10 ("…no había

prefirieron un concepto estrecho que excluyera a los ataques cibernéticos, lo cierto es que una interpretación más amplia puede ser defendida según el criterio con base en los efectos aplicado anteriormente con relación a los crímenes de guerra[172]. De hecho, y tal como sostuvo correctamente uno de los principales negociadores, una "interpretación contemporánea del término fuerza armada podría incluir, bajo ciertas circunstancias, el uso de las redes informáticas como armas"[173]. El criterio general de que las disposiciones relevantes de la Carta de la ONU, i.e., que el art. 2 (4) que se refiere al "uso de la fuerza" y el art. 51 que se refiere a un "ataque armado"[174], sólo abarcan sanciones militares, mas no políticas o económicas[175], no contradice esta interpretación amplia puesto que esta interpretación supone que un ataque informático puede ser equiparado, bajo ciertas circunstancias, a un ataque militar.

En cuanto a los actos enumerados por la norma, sólo aquellos contemplados en los apartados (b) y (d) pueden ser llevados a cabo a través de un ataque informático. El supuesto del apartado (b) exige, en su segunda alternativa, el "empleo de cualesquiera armas" contra el territorio de otro Estado. Si se define a las "armas" en sentido tradicional, como sugeriría el requisito de que sea dirigido "contra el territorio de otro Estado", entonces no incluiría a las herramientas típicas que se utilizan para realizar un ataque cibernético (e.g. mediante gusanos o virus informáticos). Sin embargo, un abordaje tan estricto iría en contra de la interpretación más flexible de la CIJ en su Opinión sobre Armas Nucleares citada anteriormente[176], y en rigor de verdad no hay ningún motivo convincente para excluir de la provisión a los ataques cibernéticos si causan un daño igual o similar que las armas convencionales[177]. En todo caso, el apartado (d), que exige un "ataque por las fuerzas armadas", permite una interpretación más amplia que abarque a los ataques cibernéticos llevados a cabo por miembros de las fuerzas armadas contra las fuerzas de otro Estado. De hecho, un ataque cibernético en un país desarrollado, que se basa fuertemente en

---

ningún deseo de abrir la caja de Pandora, y la gran mayoría de las delegaciones consideró que la limitación al uso de la fuerza armada era apropiada a los fines de la justicia penal individual").

172 Supra nota 27 y texto principal.

173 BARRIGA, en S. BARRIGA *The Princeton Process,* 2003-2009, p. 10, nota al pie 44. Con relación al umbral del art. 2 (4), ver SCHMITT, *Int'l L. Stud*, (87), 2011, pp. 914-915; EL MISMO, «Cyber Operations and the Jus Ad Bellum Revisited», *Vill.L.Rev.*, (56), 2011, pp. 569, 576-577 (propone un test con siete elementos que incluyen la gravedad, la inmediatez, la franqueza, la invasión, la medición, la legitimidad y la presunta responsabilidad); ver también MELZER, *Cyberwarfare,* 2011, pp. 6 y ss.; BENATAR, «The Use of Cyber Force: Need for Legal Justification?», *GoJIL*, (11), 2009, p. 376; WAXMAN, «Cyber Attacks and the use of Force», *YJIL*, (36), 2011, p. 421; GERVAIS, «Cyber Attack and the Laws of War», *J.L. & Cyber Warfare*, (8), 2012, p. 29; crit. HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 63-65. Este test también ha sido adoptado por el Manual de Tallinn, *Tallinn Manual,* 2013, p. 48-51; crit. en este sentido, KESSLER/WERNER, *LJIL*, (26), 2013, pp. 808-809 (sostienen que esto "marca las incertidumbres que rodean el alcance de la prohibición en el contexto de los ataques cibernéticos").

174 Para un análisis profundo y en general de estricta lectura, HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 37 y ss., 75 y ss.

175 En términos generales, RANDELZHOFER/DOERR, «Art. 2 (4)», en SIMMA et al. (eds), *The Charter of the United Nations - A Commentary*, 3ª ed., vol. 1, 2012, nm. 16-20; en nuestro contexto, ver SCHMITT, «Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework», *Columbia Journal of Transnational Law*, (37), 1999, pp. 885, 905-908; SILVER, «Computer Network Attack as a Use of Force under Article 2(4) of the Un Charter (2002)», *Int'l L. Stud*, (76), 2002, pp. 73, 80 y ss.; HATHAWAY et al., *Cal.L. Rev.* (110), 2012, p. 842; WEISSBRODT, *Minnesota J. Intl L*, (22), 2013, pp. 358-360; GOLDSMITH, *EJIL*, (24), 2013, p. 133; sobre las distintas interpretaciones de la doctrina, ver HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 58 y ss.

176 Supra nota 26.

177 Cfr. CAMMACK, «The Stuxnet Worm», *Tulane J. of Intl. & Comp. L.*, (20), 2010, pp. 322-323 (quien sostiene que "muchos de los objetivos por los que en el pasado se utilizaba la fuerza armada actualmente se alcanzan a través de presiones no forzadas ni militares"; con respecto al ataque con el virus Stuxnet contra Irán sostiene que de acuerdo al subpárr. (b) "la admisión de cualquier arma utilizada contra un territorio calificará" de acuerdo al "daño o destrucción causados").

su redes computarizadas para operar su infraestructura (e.g. control del tráfico, suministro del agua y de la electricidad) y sus fuerzas armadas (e.g. sistemas de defensa aéreos, jets de combate modernos, equipos de comunicación o drones) puede llevar a la inoperabilidad completa o parcial del sistema respectivo. Por cierto, en términos del resultado es indistinto si las fuerzas armadas resultan inoperables por los ataques "convencionales" de otras fuerzas armadas o por ataques cibernéticos[178].

En cuanto a la segunda pregunta, i.e., si la enumeración es exhaustiva, se ha sostenido en otro lugar que efectivamente ello es así[179]. Por supuesto que la cuestión ha sido controvertida durante las negociaciones[180], y siempre hay posturas –a veces invocando el art. 4 de la Resolución 3314[181]- que sostienen una enumeración abierta[182] o semi-abierta que incluya actos de la misma naturaleza (*eiusdem generis*)[183]. No obstante, una interpretación semejante no es compatible con los requisitos de previsibilidad y certeza que demanda el principio de legalidad (*nullum crimen sine lege*) consagrado en los arts. 22-24 Estatuto CPI. Consecuentemente, no puede atribuirse una responsabilidad penal *ex post facto* y las definiciones de los delitos deben construirse en forma estricta y precisa (*leges stricta* y *certa*)[184]. Si los redactores hubiesen querido aplicar la doctrina del *eiusdem generis*, podrían haber adoptado el art. 4 de la Resolución 3314, o incluido un párrafo respectivo similar al del art. 7 (1) (k) Estatuto CPI. Sin embargo, ni siquiera le han dado al Consejo de Seguridad de la ONU –contrariamente al art. 4 de la Res. 3314- la facultad de extender o enmendar la enumeración del art. 8 bis (2) si lo considera apropiado[185].

---

178 La única diferencia es la alta probabilidad de heridos en casos de ataques convencionales (aunque un ataque cibernético también puede producir fatalidades, e.g. cuando provoca la falla total del sistema informático de un avión en vuelo).

179 *Aggression* (Intersentia 2010), p. 236; SATZGER, *International and European Criminal Law*, 2012, p. 273; SCHMALENBACH, «Das Verbrechen der Aggression vor dem Internationalen Strafgerichtshof: Ein politischer Erfolg mit rechtlichen Untiefen», *Juristenzeitung*, (65), 2010, pp. 745, 748; STRAPATSAS, «Aggression» en SCHABAS/BERNAZ (eds), *The Routledge Handbook of International Criminal Law*, 2011, pp. 155, 160; cfr. WERLE, *Völkerstrafrecht,* 3ª ed., 2012, nm. 1473 ; deja abierta la cuestión, PAULUS, «Second Thoughts on the Crime of Aggression», *EJIL*, (20), 2009, pp. 1117, 1120 ('…queda por dilucidar si la lista pretende ser exhaustiva...").

180 Special Working Group on the Crime of Aggression, 'June 2008 Report' (junio de 2008) ICC-ASP/6/20/Add. 1, Anexo II, impreso en: BARRIGA/KREß (eds.), *The Travaux Preparatoires of the Crime of Aggression*, 2012, pp. 602-614, 608; cfr. HEINSCH, «The Crime of Aggression After Kampala: Success or Burden for the Future?», *GoJIL*, (2), 2010, pp. 713, 723-724.

181 Asamblea General de la ONU Res 3314 (14 de diciembre de 1974) A/RES/3314, art. 4 (explícitamente declara que la lista no es exhaustiva y autoriza al Consejo de Seguridad a expandirla).

182 SAFFERLING, *Internationales Strafrecht*, 2011, nm. 183.

183 CLARK, «Negotiating Provisions Defining the Crime of Aggression, its Elements and the Conditions for ICC Exercise of Jurisdiction Over It», *EJIL*, (20), 2009, pp. 1103, 1105; ídem., «Amendments to the Rome Statute of the International Criminal Court Considered at the first Review Conference on the Court, Kampala, 31 May-11 June 2010», *GoJIL*, (2), 2010, pp. 689, 696; más ambiguo, KREß, «Time for Decision: Some Thoughts on the Immediate Future of the Crime of Aggression: A Reply to Andreas Paulus», *EJIL*, (20), 2009, pp. 1129, 1137 (como mucho "semi-abierto"); KOSTIC, «Whose Crime is it Anyway? The International Criminal Court and the Crime of Aggression», *Duke Journal of Comparative and International Law*, (22), 2011, pp. 109, 129-130; OPHARDT, «Cyber Warfare», *DLTR*, 2010, [66]; ver también HEINSCH, *GoJIL*, (2), 2010, pp. 713, 723-726; WEISBORD, «Judging Aggression», *Colum. J. of Trans. L.*, (50), 2011, p. 40.

184 Sobre el principio *nullum crimen*, ver AMBOS, *Treatise of ICL I*, 2013, pp. 88-93. Ver también BARRIGA, in: S. BARRIGA *The Princeton Process,* 2003-2009, p. 12; id., "Negotiating the Amendments", en BARRIGA/KREß, *Travaux Preparatoires*, 2012, pp. 30-31.

185 SCHMALENBACH, «*Das Verbrechen*», JZ, 2010, pp. 747-748; igualmente: WERLE, *Völkerstrafrecht,* 3ª ed., 2012 nm. 1473; diferente: WEISBORD, *Colum. J. of Trans. L.*, (50), 2011, p. 40.

4.2. ¿Violación manifiesta de la Carta de la ONU (art. 8 bis (1) Estatuto CPI)?

La cláusula del umbral del art. 8 bis (1) exige un "acto de agresión que por sus características, gravedad y escala constituya una violación manifiesta de la Carta de las Naciones Unidas". La misma expresa la diferencia cualitativa que existe entre un "acto" de agresión, que implica una responsabilidad colectiva, y el "crimen" de agresión, que da lugar a una responsabilidad (penal) individual[186]. Su finalidad es excluir de la criminalización a los incidentes menores (e.g. escaramuzas fronterizas) o casos legalmente controvertidos (e.g. una intervención humanitaria)[187]. Así, por ejemplo, la invasión de Irak en 2003 liderada por los Estados Unidos, que si bien ha sido considerada por muchos iusinternacionalistas como un *acto* ilícito de agresión[188], lo cierto es que puede no constituir un *crimen* de agresión debido a la falta de una "violación manifiesta" –i.e. cuantitativa y cualitativamente seria desde una perspectiva objetiva[189]- de la Carta de la ONU puesto que existía una postura, académicamente respetable, según la cual la invasión estaba justificada, especialmente sobre la base de la Resolución 678 del Consejo de Seguridad del 29 de noviembre de 1990[190]. Con respecto a los ataques cibernéticos, esto significa que es difícil pensar en un ataque que sea lo suficientemente grave y de gran escala como para ser considerado equivalente a una violación manifiesta de la Carta. Por cierto, como se explicó en la sección previa, incluso es discutible en primer lugar si los ataques cibernéticos constituyen una violación simple a la prohibición de la Carta sobre el uso de la fuerza (art. 2 (4))[191], especialmente porque el criterio con base en los efectos no puede ser utilizado sin más ni más.

Conforme al Manual de Tallinn una operación cibernética constituye el uso de la fuerza "cuando su escala y efectos son comparables a las operaciones no cibernéticas que alcanzan el nivel del uso de la fuerza"[192]. La "escala y efectos" dependen, a su vez, de una serie de factores que deben tenerse en cuenta[193]. De ello parece desprenderse con claridad que una operación cibernética que "genera daño, destrucción, heridos o muerte es altamente probable que sea considerada como uso de la fuerza"[194], i.e., se exige más que una mera coerción económica o política[195]. Por ende, si se define al ataque informático como aquél que causa muerte, heridos o una seria destrucción de los bienes, entonces es equivalente al uso de la fuerza. Sin embargo, establecer si este ataque

---

186 Cfr. AMBOS, *Treatise of ICL II*, 2014 , p. 199; crit. sobre la distinción, CORREDOR, *El Crimen de Agresión en Derecho Penal Internacional*, 2012, pp. 88-89.

187 Ver SWGCA, 'June 2005 Report' (junio de 2005) ICC-ASP/4/32, Discussion Paper 3, No. 3, reimpreso en S. BARRIGA/W. DANSPECKGRUBER/C. WENAWESSER, *The Princeton Process,* 2003-2009, p. 197; ver también BARRIGA, in: S. BARRIGA *The Princeton Process,* 2003-2009, p. 8; BARRIGA, en S. BARRIGA *The Princeton Process,* 2003-2009, p. 29; CLARK, «Alleged Aggression in Utopia», en SCHABAS et al. (eds.), *The Ashgate Research Companion to International Criminal Law*, 2013, p. 66.

188 Ver KREß, «Strafrecht und Angriffskrieg im Licht des 'Falles Irak'», *ZStW*, (115), 2003, pp. 294, 313 y ss., con mayores referencias.

189 Ciertamente el término es ambiguo, cfr. PAULUS, *EJIL*, (20), 2009, p. 1121; para una explicación –no del todo convincente– ver KREß, «Time for Decision», *EJIL*, (20), 2009, p. 1137 y ss. La perspectiva objetiva está determinada por el Elemento 3 de la Introducción a los Elementos de los Crímenes del art. 8bis del Estatuto CPI.

190 KREß, «Strafrecht und Angriffskrieg», *ZStW*, (115), 2003, p. 331; críticamente, PAULUS, *EJIL*, (20), 2009, p. 1123.

191 Ver referencias en nota 173.

192 Manual de Tallinn, regla 11 en p. 45.

193 Cfr. Manual de Tallinn, *Tallinn Manual,* 2013, p. 48-50 (la gravedad, la inmediatez, la franqueza, la invasividad, la mensurabilidad de los efectos, el carácter militar, la participación del Estado y la presunta legalidad).

194 Manual de Tallinn, *Tallinn Manual,* 2013, p. 48.

195 Ver también Manual de Tallinn, *Tallinn Manual,* 2013, p. 46.

constituye, además, una violación manifiesta a la Carta es una pregunta abierta y depende de las circunstancias específicas del caso.

5. Ataques cibernéticos y crímenes contra la humanidad

Los crímenes contra la humanidad exigen que la conducta efectivamente constitutiva del delito, e.g. asesinato, tortura, violación, privación de la libertad, hayan sido cometidos "como parte de un ataque generalizado o sistemático contra una población civil…" (art. 7 (1) Estatuto CPI). Esto es lo que se conoce como el elemento de contexto de los crímenes contra la humanidad. Mientras que el requisito de un ataque "contra una población civil" tiene su origen en el derecho de la guerra, y por lo tanto se reduce a la distinción entre combatientes y civiles ya discutida anteriormente con respecto a los crímenes de guerra[196], el "ataque generalizado o sistemático" es la característica particular de los crímenes contra la humanidad. La redacción del art. 7 (2) (a) Estatuto CPI sugiere que este requisito debe ser entendido cualitativamente, i.e. el "ataque" siempre debe basarse –sin perjuicio de su carácter predominante de "generalizado" o "sistemático"- en una determinada política ("de conformidad con o para promover")[197].

Con respecto a los ataques cibernéticos esto significa, en primer término, que deben ser realizados de conformidad con una determinada política y, además, ser generalizados o sistemáticos. El elemento político presupone que estos ataques son planificados, organizados, coordinados o al menos tolerados por un Estado o una organización en el sentido del art. 7 (2)(a) Estatuto CPI. En este caso, el ataque normalmente también se calificaría como "sistemático"[198]. Si bien un grupo de hackers con poca organización que actúe autónomamente no alcanzaría el requisito de la organización, lo cierto es que aquellos grupos armados organizados en el sentido del derecho internacional humanitario que recurran a los métodos de la guerra cibernética ciertamente sí[199]. Y si, además, los ataques cibernéticos realizados por un Estado o un grupo suficientemente organizado causaran un daño grave y extenso, en el sentido de los ejemplos dados anteriormente, entonces el ataque probablemente también se calificaría como "generalizado". Estos ataques cibernéticos generalizados o sistemáticos pueden resultar, finalmente, en el asesinato o exterminio de poblaciones civiles, o incluso en una de las conductas establecidas en el art. 7 Estatuto CPI. Por supuesto que en última instancia la verificación de los elementos de un crimen contra la humanidad va a depender de las circunstancias del caso concreto.

6. Conclusiones

En el caso de los ataques cibernéticos es más probable que pueda atribuirse una responsabilidad penal individual por crímenes de guerra que por el crimen de agresión. Librar una "guerra cibernética" en violación del *ius ad bellum* difícilmente puede dar lugar a una responsabilidad

196 Sin embargo, para una interpretación más restrictiva de este elemento, AMBOS, *Treatise of ICL II*, 2014 , pp. 63 y ss.
197 Cfr. AMBOS, *Treatise of ICL II*, 2014 , pp. 63, 67 y ss.
198 Cfr. AMBOS, *Treatise of ICL II*, 2014 , pp. 59-61.
199 Sobre la correspondiente disputa en la decisión de la CPI en relación a Kenia, ver AMBOS, *Treatise of ICL II*, 2014, pp. 72 y ss.

penal por agresión bajo el art. 8 bis Estatuto CPI, puesto que es bastante difícil pensar que un ataque cibernético sea equiparable a un acto de agresión en el sentido del art. 8 bis (2) Estatuto CPI, y mucho menos a una violación manifiesta en el sentido del art. 8 bis (1) Estatuto CPI.

El derecho internacional humanitario se aplica a los ataques cibernéticos sin más preámbulos si esos ataques son parte de un conflicto en curso. Ante la ausencia de tal conflicto, los ataques cibernéticos deben ser, por sí mismos, lo suficientemente serios como para superar el umbral del conflicto armado. Este sería el caso si un ataque cibernético causara, siguiendo el criterio con base en los efectos, considerable daño humano o de otro tipo, que vaya más allá de meros incidentes esporádicos y aislados, es decir, que no sean simples inconvenientes o la caída temporaria de los sistemas informáticos. Los ataques cibernéticos que producen estos efectos también se califican como ataques armados en el sentido del art. 49 (1) PA I. Para que un ataque cibernético se califique como un crimen de guerra debe estar relacionado con un conflicto armado en curso. En esos casos, la atribución de responsabilidad será posible si el atacante puede ser identificado y actúa en nombre de una de las partes del conflicto en el sentido del derecho internacional humanitario, i.e., tanto un Estado o un grupo armado organizado. De todos modos, los ataques cibernéticos de aquellos grupos de individuos menos organizados que no son calificados como una parte en el conflicto, también pueden ser atribuidos a esa parte conforme a las reglas de la responsabilidad estatal[200]. Para aquellos intervinientes cibernéticos "puramente" civiles se aplican las reglas sobre la participación directa en las hostilidades.

Según los principios del derecho internacional humanitario que regulan las hostilidades, el principio de proporcionalidad parece tener la mayor capacidad para limitar el daño a las personas civiles y a los bienes de carácter civil. Por el contrario, el principio de distinción tiene poca relevancia práctica teniendo en cuenta la alta interconectividad entre los sistemas computarizados militares y civiles, y el predominante doble uso que tiene la infraestructura cibernética. El principio de precaución también guía la conducta de las operaciones cibernéticas pero se encuentra limitado por consideraciones de posibilidad o razonabilidad. Por eso, el derecho internacional humanitario parece ser lo suficientemente amplio y flexible como para acomodar los nuevos desarrollos con respecto a la guerra cibernética[201]. Sin embargo, y como la eficacia de las reglas frecuentemente depende de su interpretación amplia o restrictiva, podría ser necesario contar con "normas más precisas"[202].

Los ataques cibernéticos que superan el umbral del conflicto armado también pueden constituir ataques generalizados o sistemáticos en el sentido del art. 7 Estatuto CPI. En todo caso, deben ser realizados conforme a una política de Estado o de una organización en el sentido del art. 7 (2) (a) Estatuto CPI.

[200] Supra nota 51.
[201] En el mismo sentido HARRISSON DINNISS, *Cyber Warfare*, 2012, pp. 28-29, 279.
[202] En el mismo sentido DROEGE, *IRRC*, (94), 2012, pp. 540, 578.

7. Bibliografía

ALDRICH (1996), «The International Legal Implications of Information Warfare», *Airpower Journal*, vol. 10, pp. 99 y ss.

AMBOS (2014), *Treatise of International Criminal Law. Volume II: The Crimes and Sentencing*, OUP, Oxford.

- EL MISMO (2013), *Treatise on International Criminal Law. Volume I: Foundations and General Part*, OUP, Oxford.

BARRIGA/KREß (eds.) (2012), *The Travaux Preparatoires of the Crime of Aggression*, CUP, Cambridge.

S. BARRIGA (2009), «Against the Odds: The Results of the Special Working Group on the Crime of Aggression», en S. BARRIGA/W. DANSPECKGRUBER/C. WENAWESSER (eds.), *The Princeton Process on the Crime of Aggression – Materials of the Special Working Group on the Crime of Aggression*, 2003-2009, Lynne Rienner Publishers, Princeton, pp. 10 y ss.

BENATAR (2009), «The Use of Cyber Force: Need for Legal Justification?», *GoJIL*, vol. 11, pp. 376 y ss.

BOOTHBY (2013), «Methods and Means of Cyber Warfare», *Int'l L.Stud.*, vol. 89, pp. 387 y ss.

CAMMACK (2010), «The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression», *Tulane J. of Intl. & Comp. L.*, vol. 20, pp. 303 y ss.

CASSESE et al. (2013), *Cassese's International Criminal Law*, 3ª ed., OUP, Oxford.

CLARK (2013), «Alleged Aggression in Utopia», en SCHABAS et al. (eds.), *The Ashgate Research Companion to International Criminal Law*, Ashgate, Farnham, pp. 66 y ss.

EL MISMO (2010), «Amendments to the Rome Statute of the International Criminal Court Considered at the first Review Conference on the Court, Kampala, 31 May-11 June 2010», *GoJIL*, vol. 2, pp. 689 y ss.

EL MISMO (2009), «Negotiating Provisions Defining the Crime of Aggression, its Elements and the Conditions for ICC Exercise of Jurisdiction Over It», *EJIL*, vol. 20, pp. 1103 y ss.

CORREDOR (2012), *El Crimen de Agresión en Derecho Penal Internacional*, Universidad del Rosario, Bogotá.

DERVAN (2011), «Information Warfare and Civilian Population: How the Law addresses a fear of the Unknown», *GoJIL*, vol. 3, pp. 373 y ss.

DINSTEIN (2002), «Computer Network Attacks and Self-Defense», *Int'l L. Stud*, vol. 76, pp. 99 y ss.

DÖRMANN (2013), «§ 11 VStGB», en JOECKS/MIEBACH, *Münchener Kommentar zum Strafgesetzbuch*, vol. 8, 2a ed, C.H. Beck, Múnich.

- EL MISMO (2004), «Applicability of the Additional Protocols to Computer Network Attacks», 19 de noviembre de 2004, disponible en: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm

DOSWALD-BECK (2002), «Some Thoughts on Computer Network Attack», *Int'l L. Stud.*, vol. 76, pp. 163 y ss.

DROEGE (2012), «Get off my Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians», *IRRC*, vol. 94, pp. 533 y ss.

FENRICK (2001), «Targeting and Proportionality during the NATO Bombing Campaign against Yugoslavia», *EJIL*, vol. 12, pp. 489 y ss.

GEISS (2013), «Cyber Warfare: Implications for Non-international Armed Conflict», *Int'l L. Stud*, vol. 89, pp. 627 y ss.

GEIß/LAHMANN (2012), «Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space», *Isr.L.Rev.*, vol. 45, pp. 381 y ss.

GERVAIS (2012), «Cyber Attack and the Laws of War», *J.L. & Cyber Warfare*, vol. 8, pp. 29 y ss.

GILLET (2013), «The anatomy of an international crime: Aggression at the ICC», *ICLR*, vol. 13, pp. 829 y ss.

GOLDSMITH (2013), «How Cyber Changes the Laws of War», *EJIL*, vol. 24, pp. 129 y ss.

HANKEL (2011), *Das Tötungsverbot im Krieg: Eine Intervention*, Hamburger Edition, Hamburgo.

HARRISSON DINNISS (2012), *Cyber Warfare and the Laws of War*, CUP, Cambridge.

HASLAM (2000), «Information Warfare: Technological Changes and International Law», *J.C.& S.L*, pp. 157 y ss.

HATHAWAY et al (2012), «The Law of Cyber-Attack», *Cal.L. Rev.*, vol. 110, pp. 817 y ss.

HEINSCH (2010), «The Crime of Aggression After Kampala: Success or Burden for the Future?», *GoJIL*, vol. 2, pp. 713 y ss.

HENCKAERTS/DOSWALD-BECK (2005), *ICRC Study on Customary International Humanitarian Law, Volume I: Rules*, CUP, Cambridge.

HINKLE (2011), «Countermeasures in the Cyber Context: One More Thing to Worry About», *YJIL Online*, vol. 37, pp. 11 y ss.

KELLER/FOROWICZ (2008), «A Tightrope Walk between Legality and Legitimacy: An Analysis of the Israeli Supreme Court's Judgment on Targeted Killing», *LJIL*, vol. 21, pp. 189 y ss.

KESSLER/WERNER (2013), «Expertise, Uncertainty, and International Law: A Study on the Tallinn Manual on Cyberwarfare», *LJIL*, vol. 26, pp. 793 y ss.

KOSTIC (2011), «Whose Crime is it Anyway? The International Criminal Court and the Crime of Aggression», *Duke Journal of Comparative and International Law*, vol. 22, pp. 109 y ss.

KREß (2003), «Strafrecht und Angriffskrieg im Licht des 'Falles Irak'», *Zeitschrift für die Gesamte Strafrechtswissenschaft*, vol. 115, pp. 294 y ss.

- EL MISMO (2009), «Time for Decision: Some Thoughts on the Immediate Future of the Crime of Aggression: A Reply to Andreas Paulus», *EJIL*, vol. 20, pp. 1129 y ss.

LIN (2012), «Cyber Conflict and International Humanitarian Law», *IRRC*, vol. 94, pp. 515 y ss.

LUBELL (2013), «Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?», *Int'l L.Stud.*, vol. 89, pp. 252 y ss.

LÜLF (2013), «International Humanitarian Law in Times of Contemporary Warfare – The New Challenge of Cyber Attacks and Civilian Participation», *Humanitäres Völkerrecht – Informationsschriften*, vol. 26, pp. 74 y ss.

MCCLURE (2012), «International Adjudication Options in Response to State-Sponsored Cyber-Attacks Against Outer-Space Satellites», *New England J. of Intl & Comparative L.*, vol. 18, pp. 431 y ss.

MELZER (2011), «Cyber Operations and Ius in Bello», *Disarmament Forum*, vol. 4, pp. 3 y ss.

- EL MISMO (2011), *Cyberwarfare and International Law*, UNDIR Resources, Ginebra.

- EL MISMO (2009), *lnterpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC, Ginebra.

O'CONNELL (2008), «Historical Developments and Legal Basis», en FLECK (ed.), *The Handbook of International Humanitarian Law*, 2ª ed., OUP, Oxford, pp. 1 y ss.

O'DONNELL/KRASKA (2003), «Humanitarian Law: Developing International Rules for the Digital Battlefield», *J.C.& S.L.*, vol. 8, pp. 133 y ss.

OETER (2008), «Methods and Means of Combat», en FLECK (ed.), *The Handbook of International Humanitarian Law*, 2ª ed., OUP, Oxford, pp. 115 y ss.

OLÁSOLO (2008), *Unlawful attacks in combat situations: from the ICTY's case law to the Rome Statute*, Nijhoff, Leiden.

OPHARDT (2010), «Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield», *Duke Law and Technology Review*, vol. 3, pp. 3 y ss.

PAULUS (2009), «Second Thoughts on the Crime of Aggression», *EJIL*, vol. 20, pp. 1117 y ss.

PICTET (ed.) (1952), *Commentary on the Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field* (reimpreso en 2006), ICRC, Ginebra.

- EL MISMO (ed.) (1958), *Commentary on the Geneva Convention relative to the Protection of Civilian Persons in Time of War* (reimpreso en 1994), ICRC, Ginebra.

PILLOUD et al. (1987), *Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Nijhoff, Ginebra.

RANDELZHOFER/DOERR (2012), «Art. 2 (4)», en SIMMA et al. (eds), *The Charter of the United Nations - A Commentary*, 3a ed., vol. 1, OUP, Oxford.

SAFFERLING (2011), *Internationales Strafrecht*, Springer, Berlín.

SATZGER (2012), *International and European Criminal Law*, C.H. Beck, Múnich.

SCHMALENBACH (2010), «Das Verbrechen der Aggression vor dem Internationalen Strafgerichtshof: Ein politischer Erfolg mit rechtlichen Untiefen», *Juristenzeitung*, vol. 65, pp. 745 y ss.

SCHMITT (ed.) (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, CUP, Cambridge.

- EL MISMO (2012), «Classification of Cyber Conflict», *J.C.& S.L.*, vol. 17, pp. 245 y ss.

- EL MISMO (2011), «Cyber Operations and the Jus Ad Bellum Revisited», *Vill.L.Rev.*, vol. 56, pp. 569 y ss.

- EL MISMO (2011), «Cyber Operations and the Jus in Bello: Key Issues», *Int'l L. Stud*, vol. 87, pp. 89 y ss.

- EL MISMO (2002), «Wired warfare: Computer Network Attack and Ius in Bello», *IRRC*, vol. 84, pp. 365 y ss.

- EL MISMO (1999), «Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework», *Columbia Journal of Transnational Law*, vol. 37, pp. 885 y ss.

M. SCHMITT (2012), «Classification of cyber conflict», *J.C.& S.L.*, vol. 17, pp. 245 y ss.

SILVER (2002), «Computer Network Attack as a Use of Force under Article 2(4) of the Un Charter (2002)», *Int'l L. Stud*, vol. 76, pp. 73 y ss.

STEIGER (2013), «Civilian Objects», en WOLFRUM (ed.), *Max-Planck-Encyclopedia of Public International Law*, OUP, Oxford.

STRAPATSAS (2011), «Aggression» en SCHABAS/BERNAZ (eds), *The Routledge Handbook of International Criminal Law*, Routledge, Londres, pp. 155 y ss.

SWANSON (2010), «The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict», *Loyola L.A.Int'l & Comp.L.J.*, vol. 32, pp. 303 y ss.

TURNS (2012), «Cyber Warfare and the Notion of Direct Participation in Hostilities», *J.C. & S. L.*, vol. 17, pp. 280 y ss.

WAXMAN (2011), «Cyber Attacks and the use of Force», *YJIL*, vol. 36, pp. 421 y ss.

WEISBORD (2011), «Judging Aggression», *Colum. J. of Trans. L.*, vol. 50, pp. 82 y ss.

WEISSBRODT (2009), «Conceptualizing Aggression», *Duke Journal of Comparative and International Law*, vol. 20, pp. 1 y ss.

-EL MISMO (2013), «Cyber-Conflict, Cyber-Crime, and Cyber Espionage», *Minnesota J. Intl L*, vol. 22, pp. 345 y ss.

WERLE (2012), *Völkerstrafrecht*, 3ª ed., Mohr Siebeck, Tübingen.

WERLE/JESSBERGER (2014), *Principles of International Criminal Law*, 3ª ed., Oxford University Press, La Haya.

WRIGHT (2012), «'Excessive' ambiguity: analysing and refining the proportionality standard», *IRRC*, vol. 94, pp. 819 y ss.

8. Tabla de Jurisprudencia citada

Tribunal, Sala y Fecha	*Ar.*	*Magistrado Ponente*	*Partes*
ICC, Sala de Cuestiones Preliminares II, 15 de junio de 2009	ICC-01/05-01/08-424 Confirmation of Charges	Trendafilova, Presidente Kaul Tarfusser	The Prosecutor v. Jean-Pierre Bemba Gombo
ICTY, Sala de Primera Instancia, 3 de marzo de 2000	ICTY-95-14-T Judgement	Jorda, Presidente Rodrigues Shahabuddeen	Prosecutor v Blaski
ICTY, Sala de Primera Instancia, 15 de marzo de 2006	ICTY-01-47-T Judgement	Antonetti Rasoazanany Swart	Prosecutor v Hadzihasanovic and Kubura
ICC, Sala de Cuestiones Preliminares I, 30 de septiembre de 2008	ICC-01/04-01/07-717 Confirmation of Charges	Kuenyehia, Presidente Usacka Steiner	Prosecutor v Katanga & Ngudjolo Chi
ICTY, Sala de Apelaciones, 12 de junio de 2002	ICTY-96-23 & ICTY-96-23/1-A 12 Appeals Judgement	Jorda, Presidente Shahabuddeen Schomburg Güney Meron	Prosecutor v Kunarac, Kovac & Vokovic
ICTY, Sala de Primera Instancia II, 30 de noviembre de 2005	ICTY-03-66-T Judgement	Parker, Presidente Thelin Van Den Wyngaert	Prosecutor v Limaj et al.
ICC, Sala de Cuestiones Preliminares I, 29 de enero de 2007	ICC-01/04-01/06 Confirmation of Charges	Jorda, Presidente Kuenyehia Steiner	Prosecutor v Lubanga
ICTY, Sala de Primera Instancia, 26 de febrero de 2009	ICTY-05-87-T Judgement	Bonomy, Presidente Chowhan Kamenova Nosworthy, Reserve Juez	Prosecutor v Milutinović et al.
ICTY, Sala de Primera Instancia I, 6 de septiembre de 2011	ICTY-04-81-T Judgement	Moloto, Presidente David Picard	Prosecutor v Perišić
TPIY, Sala de Apelaciones, 2 de octubre de 1995	ICTY-94-1-AR Jurisdiction	Cassese, Presidente Li Deschênes Abi-Saab Sidhwa	Prosecutor v Tadić
ICTY, Sala de Primera Instancia, 25 de junio de 1999	ICTY-95-14/1-T Judgement	Rodrigues, Presidente Vohrah Nieto-Navia	Prosecutor v. Aleksovskia
ICTY, Sala de Primera Instancia, 16 de noviembre de 1998	ICTY -96-21-T Judgement	Karibi-Whyte, Presidente Benito Saood Jan	Prosecutor v. Musovic et. al.