DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

Los desafíos del uso de la fuerza en el ciberespacio

The Challenges of the Use of Force in Cyberspace

María Pilar **Llorens***

Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can only be achieved through international cooperation, and the foundation of this cooperation must be international law and the principles of the UN Charter.
Secretario general de las Naciones Unidas - A/70/174

* Abogada; doctorando en Derecho y Ciencias Sociales, Fac. Derecho, UNC; becaria doctoral CONICET; profesora ayudante A, Derecho Internacional Público, Cátedra B, Fac. Der., U. Nacional de Córdoba.

Artículo recibido el 8 de julio de 2016
Aprobado para publicación el 22 de septiembre de 2016

Anuario Mexicano de Derecho Internacional, vol. XVII, 2017, pp. 785-816
México, D. F., ISSN 1870-4654

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

RESUMEN: La mayor dependencia de los Estados de las tecnologías de la información y de la comunicación y consecuentemente su mayor vulnerabilidad ha provocado que la ciberseguridad se convierta en uno de los principales tópicos de debate de la comunidad internacional. En este aspecto, es de trascendental importancia la determinación del modo en que las normas del *ius ad bellum*, es decir, el conjunto de normas que regulan la utilización de la fuerza en el contexto internacional, se aplican en el ámbito del ciberespacio. En el presente trabajo se exploran las principales aristas que presenta esta problemática.

Palabras clave: uso de la fuerza, ciberespacio, legítima defensa, ciberoperaciones, Manual de Tallinn.

ABSTRACT: Cyber-security has become one of the most important issues for the international community since States' dependence on information and communication technologies and consequently its vulnerability has increased. Therefore, to determine how the ius ad bellum, this is the norms that regulate the use of force in the international context, is applied to cyberspace is essential. In this work different aspects of this issue are explored.

Key words: use of force, cyberspace, self-defence, cyber-operations, Tallin Manual.

RÉSUMÉ: La très grande dépendance des États aux technologies de l'information et de la communication, et, en conséquence, leur plus grande vulnérabilité, ont fait de la cybersécurité un des thèmes les plus débattus dans la communauté internationale. Aussi est-il extrêmement important de déterminer le mode d'application des normes propres au jus ad bellum, c'est-à-dire l'ensemble des règles appliquées pour une utilisation régulée de la force dans le contexte international, mais ici dans le domaine du cyberespace. Avec ce travail, les principaux problèmes que présente cette problématique sont examinés.

Mots-clés: usage de la force, cyberespace, légitime défense, cyberopérations, Manuel de Tallinn.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

I. Introducción

La enorme expansión de las tecnologías de la información y del conocimiento ha provocado que la dependencia de ellas de una sociedad completamente interconectada (tanto en el ámbito de las estructuras civiles como en el de las estructuras de las fuerzas armadas) sea cada vez mayor.[1] Como resultado de ello, la seguridad del ciberespacio[2] se ha convertido en una preocupación principal de la comunidad internacional, ya que mientras más digitalizado sea un Estado mayor será su vulnerabilidad.

De este modo, la cuestión de la ciberseguridad es de fundamental trascendencia para los Estados debido a que se encuentra íntimamente ligada a la protección de sus intereses nacionales. Ello implica que paulatinamente los Estados otorgarán mayor valor al acceso y a la capacidad de explotar el ciberespacio y como consecuencia tendrán más interés en proteger las infraestructuras y las actividades cibernéticas de las que dependen.[3]

En este ámbito, uno de los aspectos[4] que ha atraído la atención de los juristas es el de la aplicabilidad del *ius ad bellum*, es decir, el conjunto de

[1] Roscini, M., *Cyber Operations and the Use of Force in International Law,* Oxford, Oxford University Press, 2014, pp. 1 y 2.

[2] El ciberespacio puede ser definido como el ambiente formado por componentes físicos y no físicos, caracterizado por la utilización de computadoras y del espectro electromagnético a los fines de almacenar, modificar e intercambiar información usando redes de computadoras. *Cfr.* Schmitt, M. N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge Universtity Press, Cambridge, 2013, p. 278 (traducción propia).

Sin embargo, es necesario destacar que la anterior no es la única definición existente sobre el ciberespacio. Así, por ejemplo, puede consultarse: Raboin, B., "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Journal of the National Association of Administrative Law Judiciary,* 31, 2, 2011, pp. 602-648; o bien, Ottis, R. y Lorents, P., "Cyberspace: Definition and Implications", *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, pp. 267-270.

[3] Schmitt, M. N., "The Law of Cyber Warfare: *Quo vadis*?", *Standford Law & Policy Review,* 25, 2, 2014, pp. 269-300, p. 274.

[4] Otro de los aspectos, y que ha dado lugar a numerosos estudios, está vinculado con la aplicabilidad de las normas del *ius in bello*, es decir, del derecho internacional humanitario. Sin embargo, esta cuestión, a pesar de las numerosas e interesantes aristas que presenta, no será abordado en el presente trabajo.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

normas que regulan la utilización de la fuerza en el contexto de las relaciones internacionales. Particularmente, porque tal como lo señalan Schmitt[5] y Roscini,[6] los ciberataques[7] pueden ser concebidos como un fin en sí mismos[8] o bien pueden formar parte de un maniobra militar de mayor escala dentro de un conflicto armado.[9] Debiéndose señalar que lejos de reducirse estas operaciones cibernéticas[10] se han ido incrementando año a año.[11]

A raíz de este paulatino incremento de las operaciones cibernéticas así como de la falta de consenso doctrinario acerca de la aplicabilidad de las normas existentes a estas situaciones, el Centro de Excelencia para la Ciberdefensa Cooperativa asociado a la Organización del Tratado del Atlánti-

[5] Schmitt, M. N., *op. cit.*, p. 269.

[6] Roscini, M., "World Wide Warfare - Jus ad bellum and the Use of Cyber Force", en *Max Planck Yearbook of United Nations Law*, 14, 2010, pp. 85-130, pp. 88 y 89

[7] Los ciberataques son una especie dentro de las operaciones cibernéticas y pueden ser definidos como una operación cibernética, ya sea ofensiva o defensiva, de la que razonablemente se espera que cause daños o la muerte de una/s persona/s o daño o destrucción de bienes. *Cfr*. Regla 30 del Manual de Tallin, Schmitt, M. N. (ed.), *op. cit.*, p. 106. (traducción propia).

[8] La mayoría de los estudios señalan como ejemplo del primero, el ataque sufrido en el abril de 2007 por Estonia que provocó que numerosos sitios gubernamentales, diarios, estaciones televisivas, bancos y otros objetivos quedaran fuera de línea.

[9] Dichos estudios consideran que los ataques que sufrió Georgia en el periodo de julio-agosto de 2008 por parte de la Federación Rusa y que provocaron que varios sitios gubernamentales quedaran fuera de línea y que se redujera la velocidad del servicio de internet, constituyeron parte de la ofensiva bélica que enfrentaba a ambos Estados.

[10] Se entiende por operación cibernética el empleo de capacidades cibernéticas con el objetivo primordial de alcanzar ciertos objetivos en o empleando el ciberespacio. *Cfr*. Schmitt, M. N. (ed.), *op. cit.*, p. 258.

[11] Por ejemplo, la oficina de inteligencia británica GCHQ (Cuartel General de Comunicaciones del Gobierno) ha detectado que en el término de un año se han duplicado los ataques que afectan la seguridad nacional del Reino Unido. Whitehead, T., "Cyber Attacks Threatening National Security Double in Past Year, GCHQ Reveals", The Telegraph, 9 de noviembre de 2015, disponible en: *http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11984217/Cyber-attacks-threatening-national-security-double-in-past-year-GCHQ-reveals.html* (fecha de consulta: 19 de septiembre de 2016). Por su parte, el Informe del Pew Research Center: "Cyber Attacks Likely to Increase", que se realizó sobre la base de un sondeo a expertos del mundo informático, resalta que éstos consideran que en la próxima década se va a producir un aumento en el número de ataques que comprometan la seguridad nacional. Pew Research Center, *Cyber Attacks Likely to Increase*, 2014, disponible en: *http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/* (fecha de consulta: 19 de septiembre de 2016).

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

co Norte patrocinó un proyecto de investigación destinado a determinar las implicancias del *ius ad bellum* y del *ius in bello* en relación con los conflictos armados cibernéticos. Su resultado fue el *Manual de Tallin sobre el Derecho Internacional Aplicable a los Conflictos Armados Cibernéticos* (en adelante, el Manual de Tallin o Manual) que fue publicado en el año 2013.[12] En este Manual, que no es vinculante para los Estados, se realiza un examen de *lege lata* del ordenamiento jurídico internacional relevante para la regulación de las operaciones cibernéticas; por lo cual, se constituye en un marco de análisis de esta clase de operaciones. Sin embargo, hay que reconocer que parte de la doctrina coincide en la necesidad de actualizar las normas jurídicas internacionales para adecuarlas a las particularidades del ciberespacio.[13]

Ahora bien, en el presente trabajo, de carácter exploratorio y que no pretende agotar la temática, se examinan cuáles son las particularidades del uso de la fuerza en el ámbito del ciberespacio. Para ello, en primer lugar, se analizan las características y desafíos que las operaciones cibernéticas presentan para el derecho internacional, señalándose algunos debates que tienen lugar en la actualidad en el ámbito de la comunidad internacional y que son relevantes para el tratamiento de la cuestión del uso de la fuerza en el ciberespacio, como ser la problemática de la atribución/responsabilidad y la cuestión de la soberanía/jurisdicción. En segundo término se aborda el asunto del uso de la fuerza a nivel general para luego y en tercer lugar examinar la materia del uso de la fuerza en el contexto específico del ciberespacio distinguiendo en esta evaluación la cuestión del uso de la fuerza y la legítima defensa.

[12] La versión electrónica del Manual, en inglés, puede consultarse en el siguiente sitio web: *https://issuu.com/nato_ccd_coe/docs/Tallinnnmanual/1?e=0/1803379* (fecha de consulta: 12 de febrero de 2016).

[13] Véase, entre otros, Yoo, C. S., "Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures", *Penn Law: Legal Scholarship Repository*, 2015; Eichensehr, K. I., "Cyberwar & International Law Step Zero", *Texas International Law Journal,* 50, Symposium Issue 2, 2015, pp. 355-377; Walker, P. A., "Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace", en Maybaum, M., Osula, A.-M. y Linström, L., *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, NATO CCD CDE Publications, Tallin, 2015, pp. 93-104; Schmitt, M. N., *op. cit.,* nota 4.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

II. Las operaciones cibernéticas en el derecho internacional

Dado el auge y la dependencia de los Estados en las computadoras, la posibilidad de utilizar herramientas informáticas como mecanismos de defensa y ataque en las relaciones interestatales se ha convertido en una de las alternativas más viables con las que cuentan los Estados. Ello se debe, en parte, a que las operaciones cibernéticas son relativamente accesibles para cualquier Estado, independientemente de su grado de desarrollo, ya que no requieren de grandes infraestructuras para ser llevadas a cabo.

Además de su relativo bajo costo, existen otras dos características que las hacen atractivas para la estrategia militar y, por ende, incrementan la asiduidad con las que son utilizadas: el anonimato y la versatilidad. El primero supone, en términos prácticos, la existencia de una dificultad real para rastrear en forma fehaciente la fuente donde se originó la ciberoperación. En tanto, el segundo permite la utilización de operaciones cibernéticas en una gran variedad de situaciones ya sea que involucren objetivos civiles o militares; ello porque por un lado, se reduce la posibilidad de provocar daños colaterales[14] y por el otro, tienen la aptitud de que sus efectos sean potencialmente devastadores especialmente sobre estructuras críticas de los Estados.

Las operaciones cibernéticas ofensivas o defensivas pueden llevarse a cabo a través de dos mecanismos: los físicos, que permiten llevar adelante una ciberoperación, tales como computadoras, módems o cables, y por otro lado, lo que Raboin[15] identifica como el componente cibernético, es decir, aquellos mecanismos que sólo funcionan en el ciberespacio tales como programas de computadoras o virus.

Ante estas circunstancias, el auge en la utilización de las operaciones cibernéticas presenta ciertas particularidades ya que es necesario determinar si el ordenamiento jurídico internacional tiene la capacidad de regular el recurso a nuevas tecnologías, especialmente cuando éstas son utilizadas como mecanismos de ataque o de defensa en el marco de las relaciones interestatales. Así, los debates estatales y académicos han centrado su aten-

[14] Hollis, D. B.: "Why States Need an International Law for Information Operations", *Lewis & Clark Law Review,* 11, 4, 2007, pp. 1023-1061 y 1032.

[15] Raboin, B., *op. cit.,* nota 2, p. 610.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

ción en el hecho de precisar si la aparición de estas nuevas tecnologías justifica un tratamiento normativo diferenciado que suponga la elaboración de un conjunto de normas particulares y que se encuentre motivado en las diferencias con las tecnologías preexistentes.[16] Un ejemplo interesante lo fue en su momento la aparición de las armas nucleares.[17] Sin embargo, lo cierto es que el ciberespacio, por sus propias características, requiere la fijación de pautas normativas claras que permitan solucionar las problemáticas que se plantean. Particularmente, teniendo en cuenta que la utilización de herramientas cibernéticas para la realización de operaciones militares será cada día más habitual.[18]

[16] El mejor ejemplo de estos debates se traduce en la presentación del proyecto del Código Internacional de Conducta para la Seguridad de la Información por parte de China, Rusia, Kazajstán, Kirguistán, Tayikistán y Uzbekistán en las Naciones Unidas (A/69/723) ya que este proyecto si bien reconoce que los Estados se encontrarían obligados a cumplir con las normas de la Carta de las Naciones Unidas, no reconoce ninguno de los entendimientos logrados por los Grupos de Expertos Gubernamentales, que se referían a la aplicabilidad de las normas del derecho internacional al ciberespacio. De este modo, la postura de estos Estados no es clara en esta materia y se opone a la de otros Estados (v.g. Estados Unidos, Australia) que se han mostrado favorables a la aplicación de las normas del *ius ad bellum* y de las normas del *ius in bello* en el contexto del ciberespacio. Sobre este punto además de consultarse el informe del segundo Grupo de Expertos Gubernamentales (A/68/98) puede verse el trabajo de Eichensehr, K., *op. cit.*, nota 13, pp. 361-366, quien desarrolla en extenso esta cuestión.

[17] En este caso existe un consenso mayoritario con la Opinión Consultiva de la Corte Internacional de Justicia sobre la legalidad de la amenaza o el uso de las armas nucleares del año 1996 (en adelante, Opinión consultiva sobre Armas Nucleares), donde en términos generales la Corte señaló que ni las normas convencionales ni las normas consuetudinarias se referían a un tipo de armas específico; por lo que su uso iba a ser ilegal en tanto y en cuanto se contravinieran las normas sobre el uso de la fuerza vigentes en el derecho internacional. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996*, p. 226. El documento en español puede consultarse en: A/51/218. Sin embargo, hay autores que señalan serias preocupaciones en relación con las conclusiones a las que arribó la Corte y mantienen que este tribunal no pudo traducir los principios generales en una prohibición sustantiva del uso de armas nucleraes. *Cfr*. McCormack, T.: "A *non liquet* on Nuclear Weapons. The ICJ Avoids the Application of General Principles of International Humanitarian Law", *International Review of the Red Cross,* 316, 1997, pp. 76-91.

[18] Véase, por ejemplo, el recuento de ciberoperaciones desde el año 2008 en Schmitt, M. N., "Rewired Warfare: Rethinking the Law of Cyber Attack", *International Review of the Red Cross,* 96, 893, 2014, pp. 189-206, o el que realiza Roscini, M., *op. cit.*, nota 6, pp. 4-10.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

1. *Desafíos de las operaciones cibernéticas*

Las operaciones militares cibernéticas plantean ciertos retos al derecho internacional, particularmente en dos aspectos: soberanía/jurisdicción, atribución/responsabilidad. El estudio de estos desafíos es necesario a los efectos de establecer ciertos lineamientos esenciales para responder los interrogantes que se plantean en el marco de la aplicación de las normas del uso de la fuerza.

A. *Soberanía/jurisdicción*

¿Qué es el ciberespacio y dónde se encuentra ubicado? Son dos preguntas que se encuentran íntimamente ligadas y que generan un interesante reto para el derecho internacional ya que existirá un sinfín de posibles soluciones tanto como Estados o doctrinarios hayan tratado de responder estas preguntas.

El ciberespacio se encuentra en todas y en ninguna parte al mismo tiempo; tal como lo señala Zekos, el ciberespacio es un espacio amorfo que no ocupa un determinado lugar físico o geográfico.[19] La mayoría de las definiciones que circulan sobre el ciberespacio concuerdan en que el núcleo del ciberespacio está compuesto por las redes de *hardware*, *software* y datos interconectadas globalmente junto con la interacción humana con dichas redes.[20] En este contexto, el interrogante que se plantea para el derecho internacional es cómo compatibilizar los conceptos tradicionales de soberanía con el ciberespacio.[21]

La soberanía, entendida como la *falta de sometimiento del Estado a una autoridad o poder superior*,[22] constituye uno de los principios fundamentales del

[19] Zekos, G. I.: "State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction" en *International Journal of Law and Information Technologies*, 15, 1, 2007, pp. 1-37.

[20] Ottis, R., y Lorents, P., *op. cit.,* nota 2, p. 268.

[21] Sobre este aspecto pueden consultarse entre otros: Jensen, E. T., "Cyber Sovereignty: The Way Ahead", *Texas International Law Journal*, 50, 2, 2015, pp. 275-304; Von Heinegg, W. H., "Territorial Sovereignty and Neutrality in Cyberspace" en *International Law Studies*, 89, 2013, pp. 123-156; Scassa, T y Currie, R. J., "New First Principles? Assesing the Internet's Challenges to Jurisdiction", *Georgetown Journal of International Law,* 42, 4, 2011, pp. 1017-1082; Zekos, G. I., *op. cit.*

[22] Pagliari, A. S.: *Curso de Derecho Internacional Público,* 2a. ed., Córdoba (Argentina), Advocatus, 2013, p. 257.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

derecho internacional. Tan es así que la Carta de las Naciones Unidas dispone en su artículo 2(1) que "[l]a Organización está basada en el principio de igualdad soberana de todos sus Miembros".

Este principio que implica una igualdad en el plano jurídico y no en términos de poder real, garantiza que todos los Estados ejerzan de manera plena y exclusiva sus competencias sobre su territorio. De este modo, se puede señalar que la soberanía se encuentra íntimamente ligada a la existencia de este espacio físico y es por ello que en el ámbito del ciberespacio su aplicación no es tan clara.

Las características propias de este espacio, particularmente su intangibilidad, hacen imposible su apropiación y como resultado de ello imposibilitan que un Estado ejerza soberanía en este ámbito.[23] Sin embargo, a pesar de que el Estado no tiene soberanía sobre el ciberespacio *per se*, sí la tiene respecto de las infraestructuras cibernéticas[24] y sobre cualquier actividad que esté relacionada con estas infraestructuras,[25] ya que éstas se encuentran indubitablemente sobre su territorio.

De este modo, el Estado va a tener competencias sobre diversos ámbitos vinculados al ciberespacio. Así, por ejemplo, podrá restringir el acceso a Internet sin perjuicio de la normativa internacional convencional o consuetudinaria —*v. g.* las normas de derechos humanos o las telecomunicaciones—[26] tanto para defenderse como para prevenir ataques cibernéticos.[27]

Otra competencia fundamental del Estado, derivada de su soberanía, se vincula con el ejercicio de jurisdicción sobre las actividades que tienen lugar en el ciberespacio, tales como la comisión de delitos cibernéticos. El

[23] Tan es así que algunos autores han señalado que el ciberespacio debería ser equiparado a un patrimonio común de la humanidad y por ende debería aplicársele una regulación específica como la de los fondos marinos y oceánicos. Véase los autores citados por Jensen, E. T., *op. cit.,* nota 21, p. 296.

[24] Una estructura cibernética puede ser definida como los recursos de comunicación, almacenamiento y computación sobre los que opera un sistema de información. Cfme. Schmitt, M. N. (ed.), *op. cit.* en nota 2, p. 258.

[25] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 15. Regla 1, traducción propia. En idéntico sentido Kanuck, S., "Sovereign Discourse on Cyber Conflict Under International Law", en *Texas Law Review,* 88, 7, 2010, p. 1575.

[26] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 17.

[27] Diez de Velasco, señala que: "…existe una estrecha relación entre el derecho exclusivo del Estado a ejercer las actividades estatales (con exclusión, pues de cualquier otro Estado) y la obligación de proteger, dentro del propio territorio, los derechos de los restantes Estados…". *Instituciones de derecho internacional público*, 16a. ed., Madrid, Tecnos, 2007, p. 276.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

ejercicio de jurisdicción sobre este tipo de actividades es especialmente relevante ya que permite determinar cuál es el Estado responsable y competente para perseguir y sancionar a los agresores cibernéticos.[28]

En este punto se presenta un interesante debate doctrinario ya que existen dos cuestiones que deben ser resueltas: por un lado, si los criterios tradicionales de atribución de jurisdicción territorial —*v. g.* apropiación, cesión, prescripción— son susceptibles de ser aplicados al ciberespacio y, por el otro lado, si los criterios de atribución de jurisdicción penal —subjetivo, territorial o universal— son susceptibles de ser aplicados a las actividades que se llevan a cabo en el ciberespacio. Sin embargo, las respuestas a estas cuestiones no son sencillas ya que van a depender de cómo entendamos el ciberespacio y las actividades que en él se desarrollan.[29]

B. *Atribución / responsabilidad*

La posibilidad de enmascarar el origen de una operación cibernética genera una de problemática de especial trascendencia ya que esta dificultad técnica de determinar quiénes son los autores de una ciberoperación afecta la atribución de responsabilidad del Estado. La determinación de qué hechos pueden ser atribuidos a un Estado es relevante en dos aspectos: primero, porque permite una adecuada respuesta del Estado que ha sido víctima de un ataque cibernético contra el responsable del ataque, y segundo, porque el derecho de legítima defensa depende de que el atacante pueda ser efectivamente identificado.[30]

En esta materia son de aplicación las normas del derecho consuetudinario que establecen el marco normativo de la responsabilidad internacional de los Estados por hechos ilícitos y que han sido recogidas en el Proyecto de

[28] Raboin, B., *op. cit.* en nota 2, p. 647. Sin embargo, tal como lo señala Kanuck, S., *op. cit.,* nota 25, pp. 1590-1592, los Estados no necesariamente cuentan con las capacidades para disuadir, prevenir o algunas veces ni para detectar actividad no deseada que se produzca en sus redes y consecuentemente constituye un obstáculo para aplicar el principio de responsabilidad del Estado.

[29] Un análisis detallado de este debate puede verse en Raboin, B., *op. cit.*, nota 2, pp. 647-653 y los autores allí citados.

[30] Raboin, B., *op. cit.,* nota 2, p. 640-641. Tal como lo señala Schmitt, las dificultades técnicas en determinar de manera confiable la atribución de un hecho —encontrar al culpable— limita la capacidad del Estado de actuar. Schmitt, M. N., "In Defense of Due Diligence in Cyberspace", *TheYale Law Journal Forum,* 125, 2015, pp. 74 y 75.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

Artículos sobre Responsabilidad Internacional de los Estados por Hechos Ilícitos[31] (en adelante, proyecto de artículos) elaborado por la Comisión de Derecho Internacional en 2001. Siendo esta cuestión de particular importancia ya que en la era digital existen más posibilidades de que actores no estatales utilicen operaciones cibernéticas en contra de un Estado,[32] haciéndose necesario por ende, determinar si dichas conductas pueden ser atribuidas a un Estado en particular.

En este marco la doctrina distingue dos tipos de actos por los que puede ser responsable un Estado. Por un lado, actos positivos o comisivos y, por otro lado, actos negativos u omisivos.[33]

Con respecto a los actos comisivos son dos las posibilidades: la primera tiene lugar cuando la operación cibernética es llevada adelante por un órgano del Estado, como, por ejemplo, un miembro que forme parte de un cuerpo o división cibernética de las fuerzas armadas de ese Estado o bien por un miembro de una empresa privada o una entidad paraestatal contratada por el Estado para llevar adelante actividades que impliquen el ejercicio de atribuciones de poder público. En ambos casos la cuestión no presenta demasiados problemas ya que ambas conductas serán atribuidas al Estado conforme lo establece el proyecto en sus artículos 4o.[34] y 5o.[35]

[31] Comisión De Derecho Internacional. *Anuario de la Comisión de Derecho Internacional 2001. Vol. II. Segunda Parte.* Naciones Unidas. A/CN.4/SER.A/2001/Add.1 (Part 2), p. 120.

[32] Roscini, M., *op. cit.,* nota 6, p. 97; Raboin, B., *op. cit.,* nota 2, pp. 642-646. Para mayor abundamiento puede revisarse Schmitt, M. N. y Vihul, L., "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", *Fletcher Security Review,* 1, 1, 2014, pp. 54-73. En este artículo los autores analizan toda la problemática de la atribución de responsabilidad por actos llevados a cabo por actores no estatales.

[33] Entre otros, Schmitt, M. N., *op. cit.*, sobre la obligación de diligencia debida; Schmitt, M. N. y Vihul, L., *op. cit.*; Schmitt, M. N., *op. cit.*; Goldsmith, J. I.: "How Cyber Changes the Laws of War", *European Journal of International Law,* 24, 1, 2013, pp. 131-135; Schmitt, M. N., "Cyber Operations and the *Jus ad bellum* Revisited", *Villanova Law Review,* 56, 2011, pp. 578-581; Raboin, B., *op. cit.*, nota 2, p. 642-646; Roscini, M., *op. cit.*, nota 6, p. 97-102.

[34] Artículo 4o. *Comportamiento de los órganos del Estado*. 1. Se considerará hecho del Estado según el derecho internacional el comportamiento de todo órgano del Estado, ya sea que ejerza funciones legislativas, ejecutivas, judiciales o de otra índole, cualquiera que sea su posición en la organización del Estado y tanto si pertenece al gobierno central como a una división territorial del Estado. 2. Se entenderá que órgano incluye toda persona o entidad que tenga esa condición según el derecho interno del Estado. Comisión de Derecho Internacional, *op. cit.,* nota 31, p. 41.

[35] Artículo 5o. *Comportamiento de una persona o entidad que ejerce atribuciones del poder público*. Se considerará hecho del Estado según el derecho internacional el comportamiento de una

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

La segunda posibilidad tiene lugar cuando una persona o grupo de personas son contratadas por el Estado a fin de que lleven adelante un ataque cibernético. En este caso nos encontraríamos, en principio, frente a conductas reguladas por el artículo 8o. del proyecto de artículos que dispone: "Se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o bajo la dirección o el control de ese Estado al observar ese comportamiento".

Ante esta situación es necesario preguntarse hasta qué grado se requiere que exista un control por parte del Estado para que le pueda ser atribuida la conducta de estos particulares. Dos son las respuestas posibles: el criterio del control efectivo desarrollado por la Corte Internacional de Justicia en el *caso de las Actividades Militares y Paramilitares en y contra de Nicaragua (en adelante caso de las Actividades Militares o Paramilitares)*[36] o bien el criterio del control global desarrollado por el Tribunal Internacional para la Ex Yugoslavia en el *asunto Tadic*.[37] A pesar de que no existe consenso en la doctrina acerca de cuál es el criterio que debe aplicarse en el contexto de las operaciones cibernéticas, sí existe un entendimiento de que es preferible el criterio del control efectivo porque de lo contrario el Estado sería responsable por un sinnúmero de actividades.[38]

Finalmente, otra de las situaciones posibles se da cuando el territorio de un Estado es utilizado por un individuo o grupo de personas para llevar adelante operaciones cibernéticas contra un tercer Estado sin que exista ninguna clase de envolvimiento por parte del Estado. En este caso, los actos

persona o entidad que no sea órgano del Estado según el artículo 4 pero esté facultada por el derecho de ese Estado para ejercer atribuciones del poder público, siempre que, en el caso de que se trate, la persona o entidad actúe en esa capacidad. Comisión De Derecho Internacional, *op. cit.*, nota 27, p. 44.

[36] *Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment*. I.C.J. Reports 1986, p. 14.

[37] ICTY, *Prosecutor vs. Dusko Tadic,* Case number: IT-94-1-A-AR77, 27 February 2001.

[38] Véase Raboin, B., *op. cit.,* nota 2, pp. 344-345 y Roscini, M., *op. cit.,* nota 6, p. 100. Ambos discuten las ventajas de utilizar el test del control efectivo. Es interesante señalar que, por ejemplo, Gervais, M.: "Cyber Attacks and the Laws of War", en *Berkeley Journal of International Law,* 30, 2, 2012, pp. 525-579, p. 548, distingue entre las acciones de aquellos individuos que forman parte de un grupo organizado jerárquicamente a los que se les aplicará el estándar del control global y las acciones de grupos no organizados o de individuos en cuyo caso se aplicará el estándar del control efectivo.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

de los particulares no pueden ser imputados al Estado, sin embargo, éste podrá ser igualmente responsable no ya por el ataque cibernético en sí mismo, sino por la violación de otra obligación internacional: la obligación de no permitir que el territorio sea utilizado para que se lleven a cabo actos contrarios a los derechos de otros Estados.[39]

En este sentido, la doctrina señala que los Estados tienen un deber de diligencia debida orientado a impedir que operaciones cibernéticas que afecten los derechos de otros Estados sean iniciadas en su territorio.[40] Así, el Manual de Tallin dispone: "Un Estado no deberá permitir que la infraestructura cibernética localizada en su territorio o que se encuentra bajo control gubernamental exclusivo sea utilizada para llevar a cabo actos que ilegítimamente afecten los derechos de otros Estados".[41]

Esta obligación se fundamenta en el principio de igualdad soberana de los Estados ya que todos éstos tienen el deber de respetar la soberanía de los demás Estados.[42] Consecuentemente, los Estados tienen la obligación de adoptar todas las medidas pertinentes para evitar que los derechos de terceros Estados se vean afectados.

III. La "ciberguerra" y el *ius ad bellum*

Uno de los debates más interesantes que se plantea en relación con las operaciones cibernéticas se da en el marco de la aplicabilidad de las normas del

[39] Esta obligación fue identificada por la Corte Internacional en el *Caso del Canal de Corfú - Corfu Channel case, Judgment of April 9th,* 1949: *I.C.J. Reports* 1949, p. 4. - cuando señaló, p. 22: "…and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".

[40] Schmitt, M. N. y Vihul, L., *op. cit.,* nota 32. Algunos autores señalan que la obligación de diligencia debida se extiende no sólo a los casos en los que la operación cibernética se origina en el territorio del Estado sino también a aquellos casos en los que un ataque cibernético se transmite a través del territorio del Estado. En este sentido, véase Shackelford, S. J. *et al.*, *Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector – Research Kelley School of Business Research Paper No. 15-41*, Kelley School of Business, 2015, pp. 1-30, pp. 11-12, disponible en: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594323* (fecha de consulta: 10 de marzo de 2016).

[41] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 26, regla 5 (traducción propia).

[42] Schmitt, M. N., *op. cit.,* nota 30, pp. 71-76; Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 26.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

ius ad bellum, es decir, el conjunto de normas que regulan el uso de la fuerza en las relaciones interestatales.

Este conjunto de normas tiene tanto fuente convencional como consuetudinaria. La fuente convencional por excelencia es el artículo 2o., apartado 4, de la Carta de las Naciones Unidas (en adelante la Carta) que dispone: "Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas".

Esta norma es considerada tanto por la doctrina como por la jurisprudencia, como la piedra angular de la Carta de las Naciones Unidas.[43] Tal es su importancia que existe acuerdo acerca de que esta norma tiene la naturaleza de *ius cogens*.[44]

Además de estar recogida en normas convencionales, la prohibición de la amenaza y el uso de la fuerza se encuentran reguladas por normas consuetudinarias. En este aspecto, la Corte Internacional de Justicia (en adelante también la Corte) en el *caso de las Actividades Militares y Paramilitares* señaló: "Los principios relativos al uso de la fuerza incorporados en la Carta de las Naciones Unidas se corresponden, en lo esencial, con aquellos que se encuentran en el derecho internacional consuetudinario".[45]

[43] Entre otros, Värk, R., "The Legal Framework of the Use of Armed Force Revisited", *Baltic Security & Defence Review,* 15, 1, 2013, pp. 56-94; Simma, B. *et al.*, *The Charter of the United Nations. A commentary, vol.* I, 3a. ed., Oxford, Oxford University Press, pp. 200 y ss.; Jiménez de Aréchaga, E., "International Law in the Past Third of a Century", *Recueil des cours,* 159, 1978, pp. 1-344; Waldock, C. H. M., "The Regulation of the Use of Force by Individual States in International Law", *Recueil des cours,* 81, 1952, pp. 455-517. *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005*, p. 168; p. 223, párrafo 148 (en adelante, Actividades armadas en el Congo).

[44] Baste señalar, por ejemplo, que la Comisión de Derecho Internacional en su comentario al Proyecto de la Convención de Viena sobre Derechos de los Tratados sostuvo que la prohibición del uso de la fuerza constituye un ejemplo conspicuo ("a conspicuous example") de normas de *ius cogens.* International Law Commision. *Yearbook of the International Law Commision. 1966.Vol. II.* United Nations. A/CN.4/191, p. 247.

Posición que fuera reiterada en el Proyecto de Artículos sobre Responsabilidad de los Estados por Hechos Ilícitos cuando la Comisión señaló: "Se conviene generalmente que… la prohibición de la agresión ha de considerarse imperativa". Comisión de Derecho Internacional, *op. cit.*, nota 31, p. 120.

[45] *Caso de las Actividades Militares y Paramilitares*, nota 36, p. 99, párrafo 188 (traducción propia).

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

Con ello, la Corte reconoció la existencia de una norma que prohíbe la utilización de la amenaza y el uso de la fuerza en el derecho internacional consuetudinario que no necesariamente coincide de manera exacta con las provisiones de la Carta. Sin embargo, esto importa que en el derecho internacional contemporáneo la prohibición de la amenaza y el uso de la fuerza son absolutas sólo aceptando las excepciones previstas en la propia Carta: *a*) el derecho de legítima defensa —individual o colectivo— y *b*) las medidas coercitivas adoptadas por el Consejo de Seguridad de las Naciones Unidas al amparo del capítulo VII de la Carta.[46]

La legítima defensa, al igual que la prohibición de la amenaza y el uso de la fuerza, tiene una regulación convencional y consuetudinaria. La regulación convencional se encuentra en el artículo 51 de la Carta que dispone:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales.

La doctrina y la Corte entienden que esta norma es un reflejo del derecho internacional consuetudinario.[47] En este sentido la Corte señaló:

> …Este tratado [la Carta de las Naciones Unidas] se refiere a una norma internacional consuetudinaria preexistente; esta referencia al derecho consuetudinario se encuentra en el texto actual del artículo 51, que menciona el "derecho inmanente" (en el texto en Francés el "droit natural") a la legítima defensa individual o colectiva al cual "ninguna disposición de esta Carta menoscabará" y que se aplica en el caso de la existencia de un ataque armado. Consecuentemente la Corte entiende que el artículo 51 de la Carta sólo tiene sentido sobre la base que existe un derecho

[46] Entre otros, Värk, R., *op. cit.*, nota 43, p. 67; Dinstein, Y., *War, Agression and Self Defence,* Fifth, Cambridge University Press, 2011, p. 91.

[47] Véase, entre otros, Dinstein, Y., *op. cit.,* p. 282.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

> a la legítima defensa "natural" o "inmanente", y es difícil entender que la naturaleza de éste sea distinta de la consuetudinaria [...Tampoco] puede sostenerse que el artículo 51 es una disposición que "subsume o sobreviene" al derecho internacional consuetudinario. Sólo demuestra que en el campo en cuestión... el derecho internacional consuetudinario coexiste con el derecho convencional. Las áreas reguladas por las dos fuentes de derecho no se superponen exactamente, y las reglas no tienen el mismo contenido...[48]

La legítima defensa, por tanto, constituye un derecho que poseen los Estados de recurrir legalmente al uso de la fuerza en caso de ser objeto de un ataque armado.[49] A estos efectos se requiere que la respuesta armada del Estado afectado sea inmediata, necesaria y proporcional al ataque sufrido.

Otro requisito para el ejercicio de la legítima defensa lo constituye la notificación inmediata al Consejo de Seguridad de las acciones que se han tomado. Sin embargo, cabe destacar que, tal como lo señalara la Corte en el *caso de las Actividades Militares y Paramilitares,*[50] esta notificación no es obligatoria si se está actuando en el marco del derecho consuetudinario, ya que la notificación es una condición específica regulada por la Carta de las Naciones Unidas.

Por su parte, las medidas coercitivas adoptadas por el Consejo de Seguridad en ejercicio de sus atribuciones en el marco del capítulo VII de la Carta suponen la autorización de este órgano de Naciones Unidas a los efectos de que un Estado o un grupo de ellos utilice los medios necesarios, incluso la fuerza, a los fines de mantener o restablecer la paz y la seguridad internacionales, toda vez que con antelación se haya determinado la existencia de una amenaza a la paz, un quebrantamiento de la paz o un acto de agresión. Las medidas coercitivas consecuentemente son el resultado de un complejo sistema[51] ideado por la Carta que tiene por objetivo que la Organización de

[48] *Caso de las Actividades Militares y Paramilitares*, nota 36, p. 94, párrafo 176 (traducción propia).

[49] Entre otros, Värk, R., *op. cit.*, nota 43, p. 67; Dinstein, Y., *op. cit.,* nota 46, p. 187.

[50] *Caso de las Actividades Militares y Paramilitares*, nota 36, p. 105, párrafo 200.

[51] Este sistema, previsto entre los artículos 39 a 42 de la Carta, supone un procedimiento consistente en la determinación de la existencia de una situación que constituya una amenaza a la paz, un quebrantamiento a la paz o un acto de agresión (artículo 39), determinar medidas provisionales e instar a las partes a que las cumplan (artículo 40) o bien realizar recomendaciones y disponer medidas que no impliquen el uso de la fuerza (artículo 41).

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

las Naciones Unidas (en adelante ONU) pueda alcanzar su propósito principal: el mantenimiento de la paz y la seguridad internacionales.[52]

La interpretación de estas normas presenta algunas particularidades conn relación a qué fuerza se entiende prohibida y cuándo existe un ataque armado que dé lugar al ejercicio del derecho de legítima defensa. Evidentemente estas particularidades sumadas a las características propias de las operaciones cibernéticas darán lugar a un complejo panorama que requiere ser analizado.

1. *Uso de la fuerza y ciberoperaciones*

A. *Uso de la fuerza*

Establecer cuándo una operación cibernética viola la prohibición del uso de la fuerza contenida en el artículo 2o. apartado 4 de la Carta de Naciones Unidas supone un problema de interpretación. Ello debido a que en primer lugar es necesario determinar el alcance del término fuerza con el objeto de identificar cuál es la fuerza que se encuentra prohibida y en segundo lugar precisar cuándo una operación cibernética alcanza los estándares fijados por el derecho internacional[53] para configurar una violación de este tipo.

El problema de la delimitación del alcance del término fuerza se vincula con la redacción del artículo 2 (4) de la Carta. Esta disposición señala que

Finalmente, cuando el Consejo considere que todas estas medidas resultan inadecuadas podrá utilizar la fuerza para hacer cumplir sus decisiones (artículo 42); dado que aún no se han firmado los acuerdos que le permitan al Consejo de Seguridad disponer de una fuerza militar (artículo 43) en la práctica las competencias del Consejo del artículo 42 se traducen en una autorización para que los Estados adopten todas las medidas necesarias —lo que incluye el uso de la fuerza— a los fines de asegurar el mantenimiento de la paz y la seguridad internacionales. Para mayor abundamiento sobre este procedimiento ver entre otros, Värk, *op. cit.*, nota 43, pp. 81-83; Dinstein, Y., *op. cit.*, nota 46, pp. 308-338; Jiménez De Arechaga, E., *op. cit.,* nota 43, pp. 116-126.

[52] *Caso de las Actividades Militares y Paramilitares*, *cit.*, nota 36, p. 99, párrafo 188.

[53] Tal como lo señalan Gervais, M., *op. cit.,* nota 38, p. 536 y Roscini, M., *op. cit.,* nota 6, pp. 102-103, si bien no todas las operaciones cibernéticas alcanzan a configurar una violación al artículo 2 (4), no necesariamente significa que sean legales ya que pueden estar en contradicción con otras normas del derecho internacional, como, por ejemplo, el principio de no intervención.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

los Estados *se abstendrán de recurrir la amenaza o al uso de la fuerza*, sin embargo en ningún lugar de la Carta se define qué es el uso de la fuerza.

La doctrina mayoritaria entiende que el uso de la fuerza que está prohibido es el de la fuerza armada.[54] En apoyo de esta interpretación se señala que en primer lugar, las demás disposiciones de la Carta utilizan la expresión "fuerza armada", así lo hacen el Preámbulo, el artículo 41 y el artículo 46. En segundo lugar los trabajos preparatorios de la Carta, ya que una propuesta de la delegación de Brasil[55] para incluir una referencia a las presiones económicas fue dejada de lado; y en tercer lugar, diversas disposiciones de la resolución 2625 (XXV) hacen referencia al uso de la fuerza armada.[56] Consecuentemente, esta interpretación determina que cualquier tipo de coerción política o económica quedarán excluidas de la prohibición del uso de la fuerza, aunque podrán verse cubiertas por el principio de no intervención.[57]

Ahora bien, cabe preguntarse si las operaciones cibernéticas pueden ser consideradas como fuerza armada, y en su caso si se encuentran comprendidas por la prohibición del artículo 2 (4) de la Carta. A estos efectos, es necesario señalar que la Corte Internacional de Justicia en la Opinión Consultiva sobre Armas nucleares señaló que ninguna de las disposiciones de la Carta de las Naciones Unidas hace referencia a un tipo de arma específico y consecuentemente se aplican a cualquier uso de la fuerza[58] independientemente del arma empleada. Ello implica que cualquier operación cibernética que sea considerada un uso de la fuerza armada quedará sujeta a la prohibición del artículo 2 (4) de la Carta.[59] Así también ha sido recogido en la regla 10 del Manual de Tallin: "Una operación cibernética que constituya una amenaza o un uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o es en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas es ilegal".

[54] Véase, entre otros, Värk, R., *op. cit.*, nota 43, pp. 61-62; Dinstein, Y., *op. cit.*, nota 46, pp. 87 y 88.

[55] Brownlie, I., *International Law and the Use of Force by States,* Oxford, Oxford University Press, 2002, pp. 266-267.

[56] Värk, R., *op. cit.,* nota 39, p. 61; Roscini, M., *op. cit.,* nota 6.

[57] Roscini, M., *op. cit.,* nota 6, p. 106; Benatar, M., "The Use of Cyber Force: Need for Legal Justification?", *Goettingen Journal of International Law,* 1, 3, 2009, pp. 375-396, p. 385.

[58] Opinión consultiva sobre Armas nucleares, p. 244, párrafo 39.

[59] Roscini, M., *op. cit.,* nota 6, p. 106, señala que ello se debe a que no necesariamente se requiere que un arma tenga efectos explosivos o bien que haya sido creada con fines ofensivos y menciona como ejemplos los agentes químicos o biológicos.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

Establecer en qué circunstancias una operación cibernética puede ser un uso de la fuerza no es sencillo, en primer lugar, porque la Carta no establece ningún criterio para definir cuándo un acto implica un uso de la fuerza;[60] asimismo, la versatilidad y variabilidad que las operaciones cibernéticas presentan provocan que no se pueda dar una respuesta única acerca de si su uso implica o no una violación de la prohibición, particularmente porque sus efectos pueden abarcar un rango tan diverso como el de crear simples inconvenientes, o bien, provocar destrucción física o la muerte.

A estos efectos la doctrina ha elaborado diversos criterios con los cuales evaluar si una operación cibernética alcanza los estándares para ser considerada como un uso de la fuerza.[61] Entre ellos se destacan: *a*) el criterio instrumental (*instrumentality approach*); *b*) el criterio basado en el objetivo (*target-based approach*); *c*) el criterio de las consecuencias (*consequentiality approach*). El primer criterio —instrumental— tendrá en cuenta los medios empleados en el acto (armados, económicos o políticos) más que sus consecuencias dañosas; de esta manera una operación cibernética normalmente no será considerada como una fuerza armada porque carece de las características típicas de coerción militar y los efectos físicos o cinéticos. Por su parte, el criterio basado en el objetivo (*target-based approach*) considerará que una operación cibernética constituye un uso de la fuerza en tanto y en cuanto afecte una infraestructura crítica de un Estado, aun cuando no hubiere destrucción o heridos significativos. Finalmente, el criterio de las consecuencias (*consequentiality approach*), analizará los efectos de una operación cibernética y entenderá que ésta ha alcanzado los parámetros para ser considerada un uso de la fuerza toda vez que sus consecuencias sean equivalentes a los de una operación militar tradicional. Es decir, toda vez que se cause destrucción de propiedad y muertes existirá un uso de la fuerza contrario a la prohibición del artículo 2 (4) de la Carta.

Dentro de este último criterio es posible ubicar el modelo de análisis que propone Michael N. Schmitt;[62] este autor plantea que en los ca-

[60] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 45.

[61] Para mayor abundamiento sobre estos criterios, particularmente sobre las desventajas que presentan pueden verse los siguientes autores: Gervais, M., *op. cit.,* nota 38, pp. 538 y 539; Raboin, B., *op. cit.,* nota 2, pp. 655 y 656; benatar, M., *op. cit.*, nota 57, pp. 387-392; Hollis, D. B.: *op. cit.,* nota 14, pp. 1041 y 1042.

[62] Para mayor abundamiento sobre este modelo de análisis véase: Schmitt, M. N., *op. cit.,* nota 33, pp. 575-578; Schmitt, M. N.: "Computer Network Attack and the Use of Force in

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

sos en los que no sea indubitable que una operación cibernética sea un uso de la fuerza será necesario examinar si las consecuencias previsibles de esta operación se asemejan a las de una operación militar tradicional. Para ello, se señalan una serie factores[63] que deberán tenerse en cuenta: *a*) severidad,[64] *b*) inmediatez,[65] *c*) vinculación directa (directness),[66] *d*) intrusión (*invasiveness*),[67] *e*) medida de los efectos (measurability of effects),[68] *f*) carácter militar,[69] *g*) participación estatal,[70] *h*) presunta legalidad.[71] Di-

International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law,* 37, 2, 1999, pp. 885-937.

[63] Para el análisis de los factores se han seguido el Manual de Tallin (Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 48-50); así como los siguientes trabajos: Schmitt, M. N., *op. cit.,* nota 33, p. 576-577; Benatar, M., *op. cit.,* nota 55, p. 391; Schmitt, M. N., *op. cit.,* nota 62, p. 914-915

[64] A través de este criterio se determinará que todas aquellas operaciones cibernéticas que produzcan daño físico ya sea a los individuos o a la propiedad serán consideradas como uso de la fuerza

[65] Cuanto más inmediatos sean los efectos de un acto de coerción armada mayores son las probabilidades de que sea caracterizado como un uso de la fuerza. Como resultado de ello, las operaciones cibernéticas cuyas consecuencias se manifiesten de inmediato serán probablemente calificadas como un uso de la fuerza.

[66] Este criterio busca analizar la vinculación entre el acto y las consecuencias.; por ende analiza la cadena de causalidad. Mientras mayor sea el vínculo entre la ciberoperación y las consecuencias, mayores serán las probabilidades de que sea caracterizada como un uso de la fuerza.

[67] La intrusión se refiere al grado en el que una ciberoperación se inmiscuye en el Estado atacado o en sus sistemas cibernéticos en contra de los intereses de ese Estado. Además, se debe tener en cuenta que mientras mayor sea la seguridad del sistema atacado, mayor será la percepción de intrusión. Asimismo está percepción de intrusión se elevará cuando el objetivo del ataque sea un único Estado.

[68] Este factor determinará que los Estados sean más propensos a caracterizar una acción como un uso de la fuerza cuando sus efectos sean aparentes. Esto implica que mientras más fácil sean de cuantificar e identificar las consecuencias de una ciberoperación mayor será la probabilidad de que sea caracterizada como un uso de la fuerza.

[69] La existencia de un nexo entre la operación cibernética y una operación militar hará más probable la caracterización de esa ciberoperación como un uso de la fuerza. Cabe destacar que a diferencia de los anteriores, este factor sólo ha sido desarrollado en Manual de Tallin y no en los modelos previos presentados por Schmitt.

[70] Este factor supone que cuanto más visible sea el nexo entre un Estado y una operación cibernética mayor será la probabilidad de que sea clasificada como un uso de la fuerza, ya que es más probable que el Estado continúe involucrado en el desarrollo de la operación.

[71] A través de este factor se pone de relieve que en general en el Derecho Internacional los actos que no están prohibidos están permitidos; por lo que cualquier acto, incluyendo las

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

chos factores no son exhaustivos y buscan brindar herramientas a los Estados que les permitan determinar si una operación cibernética ha alcanzado los parámetros para ser considerada un uso de la fuerza.

El criterio de las consecuencias junto con el criterio de Schmitt han sido adoptados por el Manual de Tallin en la regla 11[72] a fin de definir cuándo existe un uso de la fuerza en el ámbito de las operaciones cibernéticas. Si bien el criterio de Schmitt no se encuentra explícitamente incluido en la regla 11, el Grupo de Expertos recomienda que sea utilizado a la hora de analizar aquellas operaciones que no pueden ser clasificadas de manera indubitable como un uso de la fuerza.[73]

B. *Amenaza del uso de la fuerza*

Cabe recordar que el artículo 2(4) de la Carta no sólo prohíbe el uso de la fuerza sino también la amenaza del uso de la fuerza. Tal como lo señala Roscini, puede entenderse que una amenaza del uso de la fuerza es una acción o una declaración que conlleva una promesa implícita o explícita de un uso futuro e ilegal de la fuerza armada en contra de uno o más Estados, cuya realización depende enteramente de la voluntad de quien la emite.[74]

En el ámbito de las operaciones cibernéticas se distinguen dos supuestos vinculados con la amenaza del uso de la fuerza: por un lado, cuando una operación cibernética es utilizada para comunicar una amenaza de uso de la fuerza ya sea cinética o cibernética, y por otro lado, cuando se realiza una amenaza por cualquier medio de llevar adelante una operación cibernética que califique como un uso de la fuerza. Ahora bien, para establecer si se

ciberoperaciones, que no esté expresamente prohibido por una regla consuetudinaria o por un tratado será presuntamente legal. Y por lo tanto menos propenso a ser considerado por un Estado como un uso de la fuerza.

[72] Una operación cibernética constituye un uso de la fuerza cuando su escala y efectos son comparables a los de operaciones no cibernéticas que alcanzan el nivel de un uso de la fuerza.

[73] Schmitt, M. N. (ed.), *op. cit.,* nota 2, pp. 47-52. Sin embargo, es necesario señalar que la aplicación de este criterio no es aceptado pacíficamente por toda la doctrina, en este sentido, por ejemplo, véase Boer, L. J. M., "«Restating the Law» «As It Is»: On the Tallin Manual and the Use of Force in Cyberspace", *Amsterdam Law Forum,* 5, 3, 2013, pp. 4-18; Kessler, O. y Wener, W.: "Expertise, Uncertainty, and International Law: a Study of the Tallinn Manual on Cyberwarfare", *Leiden Journal of International Law*, 26, 4, 2013, pp. 793-810.

[74] Roscini, M., *op. cit.,* nota 6, p. 104. En el mismo sentido Dinstein, Y., *op. cit.,* nota 46, pp. 88 y 89.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

trata de una amenaza contraria al artículo 2 (4), será necesario determinar si el uso de la fuerza amenazado es ilegal o no. Es decir, que la amenaza será legal si la acción amenazada es en sí misma legal.[75]

Así lo ha señalado la Corte Internacional de Justicia en la Opinión Consultiva sobre la Licitud de la Amenaza o el Uso de Armas Nucleares:[76]

> …Si el uso previsto de la fuerza es en sí ilegítimo, la afirmación de estar dispuesto a recurrir a ella sería una amenaza prohibida en virtud del párrafo 4 del Artículo 2… Los conceptos de "amenaza" y "uso" de la fuerza con arreglo al párrafo 4 del Artículo 2 de la Carta van unidos en el sentido de que, si el mismo uso de la fuerza en ciertos casos es ilícito, cualquiera que sea la razón, la amenaza de recurrir a esa fuerza será igualmente ilícita. En resumidas cuentas, para que se considere legítimo, el anuncio por un Estado de que está dispuesto a recurrir a la fuerza debe referirse a un uso de la fuerza que esté de conformidad con la Carta…

En este sentido, la regla 12 del Manual de Tallin dispone que se considerará una amenaza de uso de la fuerza ilícita cuando la acción amenazada (una operación cibernética o la amenaza de una operación cibernética), si es llevada a cabo, sería un uso de la fuerza ilícito.[77]

2. *Legítima defensa y operaciones cibernéticas*

En el marco de las operaciones cibernéticas existe otra cuestión legal que debe ser considerada y es la relativa a la compatibilidad de las operaciones con el derecho de legítima defensa. Es decir, determinar cuándo los Estados podrán recurrir legalmente al uso de la fuerza para responder a una operación cibernética.

En este caso el concepto fundamental que debe ser analizado es el de "ataque armado". La primera cuestión que ha de tenerse en cuenta es que este concepto no se encuentra definido en la Carta,[78] por lo que en este ámbito coexisten las normas convencionales con las consuetudinarias. En segundo lugar, es necesario señalar que el concepto de uso de la fuerza

[75] Opinión consultiva sobre Armas Nucleares, p. 246, párrafo 47.

[76] *Idem*.

[77] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 52. Traducción propia.

[78] *Caso de las Actividades Militares y Paramilitares*, nota 36, p. 94, párrafo 176.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

difiere del de ataque armado; tal como lo señaló la Corte en el *Caso de las Actividades Militares y Paramilitares* es necesario *distinguir las formas más graves del uso de la fuerza (aquellas que constituyen un ataque armado) de aquellas formas menos graves*.[79] Como resultado de ello, todo ataque armado será un uso de la fuerza contrario a la prohibición, mientras que no todo uso de la fuerza será un ataque armado. Ello a su vez implicará que no todo Estado que sea afectado por un uso de la fuerza ilegal tendrá derecho a ejercer el derecho a la legítima defensa.

Para distinguir las formas graves de las formas menos graves del uso de la fuerza la Corte utiliza el criterio de "escala y efectos". Roscini, señala que la doctrina ha tratado de definir este criterio en los siguientes términos:

> Un ataque armado es, "un acto o el comienzo de una serie de actos de fuerza armada de considerable magnitud e intensidad (escala) que tienen como consecuencia (efectos) la producción de una destrucción sustancial sobre elementos importantes del Estado atacado, como por ejemplo, la población, infraestructuras económicas y de seguridad, destrucción de aspectos de la autoridad gubernamental, esto es su independencia política, así como el daño a o la privación de su elemento físico, también denominado su territorio".[80]

Como resultado de ello, y tal como lo recoge la regla 13 del Manual de Tallin,[81] toda ciberoperación que suponga un ataque armado dará lugar al ejercicio del derecho de legítima defensa. La utilización de este criterio permite equiparar los efectos de una operación cibernética con los de una operación cinética. De este modo toda ciberoperación que produzca una destrucción significativa de elementos de trascendencia del Estado atacado puede dar lugar al ejercicio del derecho de legítima defensa.[82]

Si una operación militar convencional —*v. g.* bombardeos, ataques armados navales o aéreos— tiene como resultado la destrucción de bienes o

[79] Caso de las *Actividades Militares y Paramilitares*, nota 36, p. 101, párrafo. 191. En idéntico sentido *Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment*, I. C. J. Reports 2003, p. 161, párrafos 51, 63, 64 y 72.

[80] Constantinou, A., *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter*, 2000, pp. 63-65 citado por Roscini, M., *op. cit.*, nota 6, p. 115, traducción propia.

[81] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 54.

[82] Gervais, M., *op. cit.,* nota 38, p. 543.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

la pérdida de vidas, entonces es calificada como un ataque armado. En el mismo sentido, cualquier operación cibernética que produzca lesiones o la muerte de una/s persona/s o que produzca daños o la destrucción de bienes satisfará el requisito de la escala y efectos y por ende será considerado un ataque armado.[83]

El ejercicio del derecho de legítima defensa puede ser individual o colectivo. La legítima defensa colectiva supone la ayuda que un Estado le brinda a otro a los efectos de repeler un ataque del cual este último ha sido víctima. A los efectos del ejercicio de este derecho se requiere que exista una solicitud por parte del Estado atacado a los fines de repeler el ataque; consecuentemente la ausencia de esta solicitud impide el ejercicio de la legítima defensa colectiva.

En este sentido la Corte ha dispuesto que los Estados no pueden ejercer el derecho de legítima defensa sólo sobre la base de su propio análisis de la situación. Es necesario que el Estado que ha sido víctima de un ataque armado declarare que ha sido atacado,[84] y consecuentemente solicite la asistencia de otro/s Estado/s.[85]

En el contexto del ejercicio del derecho de legítima defensa en relación con operaciones cibernéticas existen una serie de cuestiones controversiales. Entre ellas se destacan: en primer término, la determinación de si un ataque a infraestructuras cibernéticas civiles puede ser considerado como un ataque armado que dé lugar al ejercicio del derecho de legítima defensa; en este caso, la doctrina entiende que si la infraestructura afectada por una operación cibernética es una infraestructura crítica el Estado entonces esa operación, en tanto alcance los estándares de escala y efectos, será considerada como un ataque armado y por lo tanto dará lugar al ejercicio del derecho de legítima defensa.[86] En segundo término, la determinación de si aquellas operaciones que no causen un daño físico pero sí generen severas consecuencias no destructivas o dañosas pueden ser consideradas un ataque

[83] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 55; Gervais, M., *op. cit.,* nota 38, p. 543. , p. 288

[84] *Caso de las Actividades Militares y Paramilitares*, nota 36, p. 104, párrafo 195.

[85] *Caso de las Actividades Militares y Paramilitares*, nota 36, p. 105, párrafo 199. Este requisito ha sido reiterado por la Corte en el Caso de las *Plataformas petrolíferas* en nota 79, pp. 186-187, párrafo 51; y en el Caso de las *Actividades armadas en el Congo,* nota 43, p. 218, párrafo 121.

[86] Roscini, M., *op. cit.,* nota 6, pp. 116-118; Benatar, M., *op. cit.*, nota 55, p. 394. Aunque la utilización de este criterio no es tan sencilla ya que no existe acuerdo sobre el modo de determinar cuáles son las infraestructuras críticas del Estado.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

armado; en este caso existe consenso acerca de que las operaciones cibernéticas que no produzcan daños no pueden ser consideradas como ataques armados y consecuentemente en estos casos no podrá ejercerse el derecho de legítima defensa.[87] Y, finalmente, si las ciberoperaciones llevadas a cabo por actores no estatales pueden dar lugar al ejercicio del derecho de legítima defensa; esta cuestión en la actualidad se rige por las normas de la responsabilidad de los Estados. Consecuentemente sólo aquellos casos en los que las actividades de los actores no estatales puedan ser atribuidas a un Estado particular[88] será posible el ejercicio de legítima defensa.[89]

A. *Requisitos para ejercicio del uso de la fuerza*

El ejercicio del derecho de legítima defensa en el contexto de las operaciones cibernéticas también está sujeto a las condiciones de necesidad, proporcionalidad e inmediatez.[90] El Manual de Tallin refleja estos requisitos en los siguientes términos:

Un uso de la fuerza que implique ciberoperaciones llevadas a cabo por un Estado en el ejercicio del derecho de legítima defensa debe ser necesario y proporcionado.[91]

Existe el derecho de usar la fuerza en legítima defensa si un ataque armado cibernético ocurre o es inminente. También está sujeto al requisito de la inmediatez.[92]

a. Necesidad

El requisito de necesidad hace referencia al hecho que el uso de la fuerza, aun de operaciones cibernéticas, sea necesario para repeler en forma satis-

[87] Schmitt, M. N., *op. cit.,* nota 4, pp. 282-283; Schmitt, M. N. (ed.), *op. cit.,* nota 2, 55.

[88] Véase apartado II.1.2. del presente trabajo.

[89] Schmitt, M. N., *op. cit.,* nota 4, pp. 286-288.

[90] Las condiciones de necesidad y proporcionalidad para el ejercicio del derecho de legítima defensa se encuentran establecidas en el derecho internacional consuetudinario, tal como lo señaló la Corte Internacional de Justicia en el caso de las Plataformas Petrolíferas en nota 79, p. 198, párrafo 76, y lo reafirmó en el caso de las Acciones Armadas en el Congo en nota 43, p. 223, párrafo 147.

[91] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 61, regla 14, traducción propia

[92] Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 63, regla 15, traducción propia.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

factoria un ataque que está teniendo lugar. Ello debido a que las medidas que no impliquen el uso de la fuerza han fallado o es muy probable que vayan a fallar.

Uno de los elementos centrales de este requisito es la atribución del ataque. Dinstein[93] señala que el Estado que pretende invocar el derecho de legítima defensa debe determinar de manera inequívoca que un ataque armado fue lanzado por un Estado particular y no por otro. Sin embargo, como se señaló anteriormente, la identificación del agresor en el contexto cibernético no es sencilla.[94]

b. Proporcionalidad

La proporcionalidad busca determinar cuánta fuerza es necesaria a los efectos de responder a un ataque armado. Como señala Dinstein.[95] Se trata de un estándar de razonabilidad en la respuesta a un uso de la fuerza por medio de la fuerza.

El requisito de la proporcionalidad limita la escala, el alcance, la duración y la intensidad de la respuesta necesaria para poner fin a un acto que dio lugar al ejercicio de la legítima defensa. Se debe señalar que no es necesario que la fuerza empleada en la defensa sea de la misma naturaleza que la empleada en el ataque armado. Ello implica que ante un ataque armado cibernético puede responderse tanto con operaciones cibernéticas como con operaciones cinéticas o convencionales.

c. Inmediatez

El requisito de la inmediatez permite distinguir entre los actos de defensa y las represalias; con ello se pone de manifiesto que el objetivo de la legítima defensa es repeler el ataque armado y no castigar al responsable del mismo. La inmediatez supone que no debe existir un lapso de tiempo excesivo entre el ataque armado y el ejercicio de la legítima defensa. Este requisito debe ser interpretado razonablemente, ya que entre otros elementos deben considerarse: la proximidad temporal entre el ataque y la respuesta, el

93 Dinstein, Y., *op. cit.* en nota 46, pp. 231-232

94 Véase apartado II.1.2. de este trabajo. Roscini, M., *op. cit.* nota 6, p. 119-120

95 Dinstein, Y., *op. cit.* en nota 46, pp. 232 y 233.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

periodo necesario para identificar al atacante, y el tiempo necesario para preparar la respuesta.

La flexibilidad en la interpretación de este requisito en el marco de las operaciones cibernéticas es esencial ya que muchas veces puede ocurrir que la existencia de un ataque armado no sea aparente durante un tiempo; o bien puede ocurrir que un ciberataque se componga de numerosas olas de operaciones cibernéticas y que el Estado víctima considere que se trata de una "campaña cibernética" y que consecuentemente el ejercicio de la legítima defensa no se agote con la finalización de cada ola de ciberoperaciones sino que se mantenga a lo largo de la campaña. También puede ocurrir que la identificación del agresor se demore dada la posibilidad de enmascarar las direcciones de IP.[96]

Cabe señalar que las discusiones que se presentan en torno a la posibilidad de utilizar la legítima defensa en forma preventiva es más marcada en el campo de las operaciones cibernéticas. Gran parte de los autores considera que dadas las características que tienen las ciberoperaciones es necesario prever la posibilidad de actuar en forma preventiva.[97]

IV. Consideraciones finales

El ciberespacio constituye un nuevo dominio sobre el que los Estados se están aventurando y explorando a pasos agigantados impulsados por el incesante avance tecnológico. La rapidez con la que cambian las tecnologías de la información provoca desafíos constantes que deben ser resueltos por la comunidad internacional a los fines de encontrar el mejor modo de regular este espacio.

[96] Las direcciones del Protocolo de Internet constituyen un número de identificación de los dispositivos que se encuentran interconectados en una red que utiliza el Protocolo de Internet para comunicarse. Sobre este punto se puede ver: RFC 791, Internet Protocol – DARPA Internet Program Protocol Specification (September 1981).

[97] Véase, entre otros, Yoo, C. S., *op. cit.,* nota 13, p. 10; Schmitt, M. N. (ed.), *op. cit.,* nota 2, p. 277; Waxman, M. C., "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions", *International Law Studies,* 89, 2013, pp. 109-122, p. 116; Roscini, M., *op. cit.,* nota 6, pp. 121 y 122.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

Las problemáticas que se planteen en el contexto cibernético están lejos de encontrarse resueltas; sin embargo el ordenamiento jurídico internacional provee un punto de referencia y establece un marco normativo que de alguna manera brinda una solución —muchas veces transitoria— a los problemas que deben ser resueltos sin dilación, y que en numerosas ocasiones refleja las necesidades y los intereses de los Estados que promueven una regulación particular.

Existen algunas cuestiones primordiales a las que el derecho internacional debe brindar una respuesta: la temática de la soberanía y la jurisdicción son esenciales a la hora de determinar las competencias del Estado en la regulación del ciberespacio y de las actividades vinculadas a éste. En este contexto, en primer lugar será necesario determinar el régimen jurídico del ciberespacio —*v. g.* si se trata de un espacio susceptible de apropiación o si se establece un régimen jurídico particular—[98] para poder determinar las competencias estatales tanto sobre el espacio en sí mismo considerado como respecto de las actividades que se llevan a cabo en él. De esto modo, será factible determinar la responsabilidad del Estado respecto del juzgamiento de las actividades delictivas que tienen lugar en el ciberespacio.

Asimismo, otro asunto de fundamental importancia está vinculado con el régimen de responsabilidad internacional del Estado. En este ámbito, determinar qué actos pueden ser atribuidos al Estado es indispensable ya que de esta atribución dependen cuestiones tales como las consecuencias de la responsabilidad internacional o el ejercicio del derecho de legítima defensa. Dadas las características de las operaciones cibernéticas es de particular importancia la determinación del valor que se les otorgará a aquellas ciberoperaciones llevadas a cabo por actores no estatales ya que la posibilidad de la ocurrencia de tales hechos es cada vez mayor.

En relación con el uso de la fuerza en el marco del *ius ad bellum* no caben dudas de que el régimen jurídico actual, compuesto por las normas convencionales —artículos 2 (4) y 51 de la Carta de las Naciones Unidas— y consuetudinarias, es capaz de proveer una respuesta satisfactoria, aunque transitoria, a los problemas que se plantean en torno a las ciberoperaciones. Sin embargo, también es indudable que será necesario adaptarlas a las nue-

[98] Shackelford, S. J., "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law,* 27, 1, 2009, pp. 192-251, pp. 211 y ss.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

vas realidades que se presenten y para ello será necesario un debate abierto entre todos los Estados.

V. Bibliografía

1. *Doctrina*

Benatar, M., "The Use of Cyber Force: Need for Legal Justification?", *Goettingen Journal of International Law,* 1, 3, 2009.

Boer, L. J. M.: "'Restating the Law "As It Is"': On the Tallin Manual and the Use of Force in Cyberspace", *Amsterdam Law Forum,* 5, 3, 2013.

Brownlie, I., *International Law and the Use of Force by States,* Oxford, Oxford University Press, 2002.

Diez de Velasco y Vallejo, M., *Instituciones de derecho internacional público,* 16a. ed., Madrid, Tecnos, 2007.

Dinstein, Y., *War, Agression and Self Defence,* Fifth, Cambridge University Press, 2011.

Eichensehr, K. I., "Cyberwar & International Law Step Zero", *Texas International Law Journal,* 50, Symposium Issue 2, 2015.

Gervais, M.: "Cyber Attacks and the Laws of War", *Berkeley Journal of International Law,* 30, 2, 2012.

Goldsmith, J. I., "How Cyber Changes the Laws of War", *European Journal of International Law,* 24, 1, 2013.

Hollis, D. B., "Why States Need an International Law for Information Operations", *Lewis & Clark Law Review,* 11, 4, 2007.

Jensen, E. T.: "Cyber Sovereignty: The Way Ahead" en *Texas International Law Journal*, 50, 2, 2015.

Jiménez De Aréchaga, E., "International Law in the Past Third of a Century", en *Recueil des cours,* 159, 1978.

Kanuck, S., "Sovereign Discourse on Cyber Conflict Under International Law", en *Texas Law Review,* 88, 7, 2010.

Kessler, O. y Werner, W., "Expertise, uncertainty, and international law: a study of the Tallinn Manual on Cyberwarfare", *Leiden Journal of International Law,* 26, 4, 2013.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

MCCORMACK, T., "A *non Liquet* on Nuclear Weapons. The ICJ Avoids the Application of General Principles of International Humanitarian Law", *International Review of the Red Cross,* 316, 1997.

OTTIS, R. y LORENTS, P., "Cyberspace: Definition and Implications" en *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April, Reading: Academic Publishing Limited.

PAGLIARI, A. S., *Curso de derecho internacional público,* 2a. ed., Córdoba (Argentina), Advocatus, 2013.

RABOIN, B., "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Journal of the National Association of Administrative Law Judiciary,* 31, 2, 2011.

ROSCINI, M., Cyber Operations and the Use of Force in International Law. Oxford University Press, Oxford, 2014.

ROSCINI, M., "World Wide Warfare-*Jus ad bellum* and the Use of Cyber Force", en *Max Planck Yearbook of United Nations Law,* 14, 2010.

SCASSA, T y Currie, R. J., "New First Principles? Assesing the Internet's Challenges to Jurisdiction" en *Georgetown Journal of International Law,* 42, 4, 2011.

SCHMITT, M. N., "In Defense of Due Diligence in Cyberspace", *The Yale Law Journal Forum,* 125, 2015.

————, "Rewired Warfare: Rethinking the Law of Cyber Attack", *International Review of the Red Cross,* 96, 893, 2014.

————, "The Law of Cyber Warfare: *Quo vadis?*", *Standford Law & Policy Review,* 25, 2, 2014.

————, "Cyber Operations and the *Jus ad bellum* revisited", *Villanova Law Review,* 56, 2011.

————, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law,* 37, 2, 1999.

———— (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge Universtity Press, 2013.

———— y VIHUL, L., "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", *Fletcher Security Review,* 1, 1, 2014.

SHACKELFORD, S. J., "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law,* 27, 1, 2009.

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

SHACKELFORD, S. J. *et al.*, *Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector – Research Kelley School of Business Research Paper*, Nª 15-41 [en línea], Kelley School of Business, 2015, disponible en: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594323* (fecha de consulta: 10 de marzo de 2016).

SIMMA, B., *et al.*, *The Charter of the United Nations. A commentary,* I, Third, Oxford University Press, 2012.

VÄRK, R., "The Legal Framework of the Use of Armed Force Revisited", *Baltic Security & Defence Review,* 15, 1, 2013.

VON HEINEGG, W. H., "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies*, 89, 2013.

WALDOCK, C. H. M., "The Regulation of the Use of Force by Individual States in International Law", *Recueil des cours,* 81, 1952.

WALKER, P. A., "Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace", en Maybaum, M. *et al.*, *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallin, NATO CCD CDE Publications, 2015.

WAXMAN, M. C., "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions", *International Law Studies,* 89, 2013.

YOO, C. S., "Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures", *Penn Law: Legal Scholarship Repository*, 2015.

ZEKOS, G. I., "State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction", *International Journal of Law and Information Technologies*, 15, 1, 2007.

2. *Documentos*

Comisión de Derecho Internacional, *Anuario de la Comisión de Derecho Internacional 2001. Vol. II. Segunda Parte.* Naciones Unidas. A/CN.4/SER.A/2001/Add.1 (Part 2).

International Law Commision, *Yearbook of the International Law Commision. 1966.Vol. II.* United Nations. A/CN.4/191

Pew Research Center, *Cyber Attacks Likely to Increase*, 2014, disponible en: *http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/* (fecha de consulta: 19 de septiembre de 2016).

DOI: http://dx.doi.org/10.22201/iij.24487872e.2017.17.11052

RFC 791, Internet Protocol – DARPA Internet Program Protocol Specification (September 1981)

3. *Jurisprudencia*

A. *Corte Internacional de Justicia*

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168.

Corfu Channel case, Judgment of April 9th, 1949: I.C. J . Reports 1949, p. 4.

Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports 1986, p. 14.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226.

Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I. C. J. Reports 2003, p. 161.

B. Tribunal Internacional para la ex Yugoslavia

ICTY, *Prosecutor vs. Dusko Tadic,* Case number: IT-94-1-A-AR77, 27 February 2001.

4. *Notas periodísticas*

WHITEHEAD, T., "Cyber attacks threatening national security double in past year, GCHQ reveals", The Telegraph, 9/11/15, *http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11984217/Cyber-attacks-threatening-national-security-double-in-past-year-GCHQ-reveals.html* (fecha de consulta: 19 de septiembre de 2016).