Anuario da Facultade de Dereito da Universidade da Coruña Vol. 22 (2018), pp. 157-175
ISSNe: 2530-6324 || ISSN: 1138-039X
DOI: https://doi.org/10.17979/afdudc.2018.22.0.5180

LOS CIBERATAQUES: UNA NOCIÓN SIN TIPIFICACIÓN, PERO CON UN FUTURO

ELENA LAZĂR

DRAGOS NICOLAE COSTESCU

Resumen: Este documento intenta delinear y definir la noción de ciberataque en el contexto del Derecho internacional. En este sentido, queremos enfatizar la falta de un marco legal claro para regular esta noción. Finalmente, abordamos el tema de la ciberguerra en el Derecho internacional humanitario.

Palabras clave: Cibernético, Derecho internacional humanitario, Tipificación, Ciberguerra

Abstract: This paper attempts to delineate and define the notion of cyberattack in the context of international law. In this sense, we want to emphasize the lack of a clear legal framework to regulate this notion. Finally, we will address the issue of cyberwar in international humanitarian law.

Key words: Cybernetics, International humanitarian law, Typification, Cyberwar

SUMARIO: I. INTRODUCCIÓN. II. CATEGORÍAS DE CIBERATAQUES III. ¿FALTA DE REGLAMENTACIÓN ? IV. LA INSUFICIENCIA DE LA NORMATIVA EXISTENTE V. LA CIBERGUERRA Y EL DIH. VI. CONCLUSIONES

I. INTRODUCCIÓN

La posesión de conocimientos en el área de tecnologíaa para llevar a cabo ataques cibernéticos no entiende de fronteras, y hoy en día las fronteras son muy poco tangibles.

En este trabajo nos centraremos en aclarar tres cuestiones:en primer lugar, la definición de esta noción y las diferencias entre los ciberataques y otros ataques; en segundo lugar, la categorización de los tipos de ciberataques; en tercero lugar, la cuestión de la falta de reglamentación en esta área y, en cuarto lugar, la posibilidad de aplicar el Derecho internacional humanitario (en adelante, "DIH") a los ciberataques, especialmente cuando estamos frente a una ciberguerra. ¿Cuáles son las reglas que se aplican en este tipo de guerra? Por ejemplo, si el ataque cibernético es realizado por el uso de fuerzas convencionales, podemos identificar fehacientemente al atacante y defenderse conforme al *ius ad bellum*. Lo que es más, los daños físicos causados por armas o guerras tradicionales pueden verse de inmediato, en tanto que los ocasionados por armas cibernéticas son intangibles en su acción, pero tangibles en los eventuales daños.

Los medios y métodos de hacer la guerra evolucionan con el paso del tiempo, se han dejado de usar los medios tradicionales y, como los ciberataques son posteriores a las convenciones que hoy en día están vigentes en Derecho internacional, la guerra informática no está recogida dentro de ellas, y no existe norma alguna en el Derecho que incluya expresamente los ciberataques en el uso de la fuerza.

En cuanto a la primera cuestión que se aborda, realmente resulta muy complicado ofrecer una definición exacta de qué significa el concepto de ciberataque porque depende de

muchas variables, y tampoco existe una definición aceptada en la comunidad internacional, ya que entre los países hay conceptos diferentes en la mayoría de los sentidos.

La dificultad en el ámbito ciberataques consiste, por un lado, en la falta de una definición regulada y, por otro lado, en la complejidad de este concepto, que se diferencia de otros tipos de ataques. El ciberespacio mismo genera esta complejidad y está definido como "un dominio global dentro del entorno de información cuyo carácter distintivo y único está enmarcado por el uso de la electrónica y el espectro electromagnético para crear, almacenar y modificar información a través de redes interconectadas utilizando tecnología de la información[1]".

En primer lugar, el anonimato, que es la primera gran "ventaja" de los ataques cibernéticos para los que cometen este tipo de actos. Aunque los ataques puedan parecer originados en las computadoras y redes de un Estado, eso necesariamente no significa que este Estado esté involucrado en tales acciones. En segundo lugar, los actores atacantes, que pueden ser gubernamentales o no gubernamentales, civiles o militares, y esto hace muy dificil indentificarlos. En tercer lugar, porque las herramientas que se usan son intangibles y electrónicas en la mayoría de los casos. En cuarto lugar, por los efectos que causan: puede tratarse de destrucción física o de ataques conducidos a distancia sin necesidad de invasión física[2].

En cuanto al segundo problema que se trata, como hemos afirmado antes, la noción de ciberataques es muy compleja y, para ilustrar su complejidad, vamos a presentar las principales categorías de ciberataques. Representan ciberataques los cibercrímenenes, el ciberterrorismo y también la ciberguerra.

[1] D. T. KUEHL, "From cyberspace to cyber power: Defining the problem", en F. D. KRAMER, S. H. STARR, L. K. WENTZ, *Cyberpower and National Security*, National Defense University Press, 2009.
[2] W. BRENNER y J. J. SCHWERHA IV, "Cybercrime Havens: Challenges and Solutions", *Business Law Today*, vol. 17, noviembre/diciembre 2007.

II. CATEGORÍAS DE CIBERATAQUES

Cibercrimen

El cibercrimen comprende un amplio espectro de delitos cibernéticos, entre los que podemos citar la piratería de software, juegos, música o películas; estafas, transacciones fraudulentas, acoso y explotación sexual; pornografía infantil, fraudes de telecomunicaciones, amenazas, injurias, calumnias, etc. Como se puede deducir, el objetivo de cibercrimen es conseguir un beneficio económico.

Hoy en día, los cibercriminales han adquirido experiencia en el cifrado de sus datos al utilizar tecnologías de la información y la comunicación (uso de proxies, routers digitales IPs extranjeras,Cloud computación)[3]. A veces los delitos son cometidos a distancia en terceros países, con el uso de la infraestructura de comunicación de un tercer país, lo que reduce el riesgo de investigación por parte de la policía y de la fiscalía.

Dentro del cibercrimen, la mayoría de los ataques informáticos provienen del uso de phising, troyanos y malware. A través de los dos primeros, los delincuentes pueden hacerse con contraseñas, que utilizan para obtener información sensible a la que habitualmente no tendrían permiso para acceder. Su carta de presentación admite diferentes formas: virus, troyanos, programas espía (spyware) o gusanos (worms)[4]. Además, a causa de un malware pueden derivarse otros tipos de ataques, como puede ser la denegación de servicio DOS o la denegación de servicio distribuido DDOS. El ataque DOS es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, que se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue, mientras el ataque DDOS se lleva a

[3] A. M. COLARIK, *Cyber Terrorism. Political and Economic Implications*, Hershey / London / Melbourne / Singapore, Idea Group Publishing, 2006.

[4]Un gusano es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario..

cabo generando un gran flujo de información desde varios puntos de conexión (en febrero de 2000, los ataques DDOS que cerraron efectivamente Amazon y eBay, entre otros sitios[5]). Estonia, en 2007, fue también víctima de un ataque cibernético (la categoría de cybercrimenes) importante, que bloquea la mayor parte de las redes informáticas de empresas de servicios públicos, bancos y otros servicios relacionados durante varios días. Este fue el primer ataque virtual cometido contra una entidad estatal con suficientes recursos sustanciales para bloquear parte de la administración. Más tarde se demostró que estos ataques se produjeron a partir de sitios rusos[6].

Para ofrecer otro ejemplo de cibercrimen, podemos tratar el caso del virus I Love You Bug[7] que apareció el 4 de mayo de 2000 y se presentó en forma de mensaje de correo electrónico con el asunto "I love you" y contenía también un archivo adjunto con el nombre "Love Letter for you TXT", que al ser abierto infectaba el ordinador y se autoenviaba a las direcciones de correo que el usuario tuviera en su agenda de direcciones. Comenzó en Filipinas y le bastó un solo día para propagarse por todo el mundo. Este virus atacó el Pentágono y también el Parlamento británico.

También la aparición de redes sociales, como Twitter y Facebook, supuso millones de víctimas potenciales de cibercrímenes. Cuando los usuarios no restringen las opciones de comunicación para que permitan la interacción únicamente con su red privada de "amigos", dichas redes pueden dar acceso a un número enorme de víctimas potenciales a la vez.

Ciberterrorismo

El ciberterrorismo, aunque es muy parecido al cibercrimen, se diferencia de éste en que no persigue principalmente un fin económico, sino que se refiere más a aquellas acciones en las que se persigue intimidar, coaccionar y causar daños con fines fundamentalmente políticos y religiosos[8].

[5] http://dayintechhistory.com/dith/february-7-2000-mafiaboy-ddos-yahoo-6-web-sites/ sitio accedido el 6 de agosto de 2017.
[6] http://www.bbc.com/mundo/noticias/2014/03/140306_tecnologia_guerra_cibernetica_rusia_ucrania_aa sitio accedido el 14 de mayo de 2017.
[7] https://www.wsws.org/en/articles/2000/05/bug-m10.html sitio accedido el 2 de julio de 2017.
[8] M.C. BASSIOUNI, *Perspectives on international terrorism*, in International Criminal Law, 3rd edition, vol. I, Martinus Nijhoff, 2008, pp. 704-706.

El ciberespacio representa un espacio muy "beneficioso" para los terroristas debido a que está siendo utilizado cada vez más por éstos por el anonimato, la falta de regulación y el enmascaramiento. Las acciones que llevan a cabo en este espacio pueden ser la financiación de organizaciones terroristas, guerra psicológica, reclutamiento, comunicación, adoctrinamiento y propaganda, entre otras[9].

Para ilustrar mejor el beneficio del ciberespacio para los terroristas, en febrero de 2016, los esfuerzos del gobierno de Estados Unidos para obligar a Apple a proporcionar asistencia para desbloquear un iPhone propiedad de uno de los terroristas de San Bernardino desencadenaron debates nacionales e internacionales sobre la promesa y los peligros del cifrado en muchos contextos, incluidos los esfuerzos para contrarrestar el terrorismo cibernético[10]. En esta situación, nos enfrentamos a dos temas muy controvertidos: por una parte, el derecho a la protección de datos personales y, por otra, la lucha contra el terrorismo. Por lo tanto, no podemos dejar de criticar la decisión de Apple, que ha decidido dar prioridad a la protección de datos personales en el contexto actual en el que el terrorismo se está amplificando cada vez más.

También el ciberterrorismo plantea amenazas reales a la vida humana. En 2010, el virus gusano Stuxnet, que tuvo como objetivo la central nuclear iraní, podría haber tenido consecuencias potencialmente peligrosas para la población, los Estados y otros países vecinos en todo el mundo. El virus Stuxnet impactó redes de ordenadores que controlan los servicios públicos también en países lejanos, incluyendo Estados Unidos, Indonesia, India, Azerbaiyán y Pakistán (Symantec, 2010). Según IEEE Spectrum en 2013[11], "[e]l reconocimiento de este tipo de amenazas estalló en junio de 2010 con el descubrimiento de Stuxnet, un gusano informático de 500 KB que infectó el software de al menos 14 plantas industriales en Irán, incluyendo una planta de enriquecimiento de uranio. A pesar de que un virus informático se basa en una víctima involuntaria para instalarlo, el gusano se propaga por sí mismo, a través de una red informática".

[9] B. SAUL, *Research handbook on International Law and Terrorism*, Elgar Publishing, 2014, p. 4.
[10] E. LICHTBAU **y** K. BENNER, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone", *New York Times*, 18 February 2016, A1.
[11] https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet sitio accedido el 2 de octubre de 2017.

Por lo tanto, las instalaciones militares y nucleares pueden ser objeto de un ataque terrorista cibernético. Aquí es muy importante hacer una distinción: si en nuestro ejemplo con el central nuclear iraní el objetivo del ataque hubiera sido el inicio de una guerra, entonces estamos frente a un posible acto de ciberguerra[12]. Por otra parte, si el objetivo fuera generar miedo o intimidar, podemos hablar de un acto de ciberterrorismo.

Ciberguerra

Un ataque cibernético se puede realizar en tiempo de paz o en tiempo de conflicto armado y es ahí donde al conflicto realizado en el ciberespacio se le denomina "ciberguerra". Más precisamente, los ataques cibernéticos que alcanzan el umbral de un conflicto armado o que se realizan en el marco de un conflicto armado, en el sentido del DIH. Para ofrecer un ejemplo de acto de ciberguerra, lo constituiría un ataque dirigido contra las centrales nucleares y los sistemas de control aéreo, que también son vulnerables en caso de ataque cibernético, a causa de su dependencia de los ordenadores[13].

Como este tipo de ciberataque plantea preocupaciones con respecto a las normas de realización de la guerra, vamos a tratar por separado esta categoría.

En cuanto a la tercera cuestión que se aborda, tenemos que precisar que hoy en día no hay una cooperación internacional suficientemente buena con respecto a esta área y, aunque existen organizaciones creadas con este fin, como la OTAN, realmente no hay una legislación internacional obligatoria que pueda aplicarse y con la que todos los Estados estén de acuerdo.

III. ¿FALTA DE REGLAMENTACIÓN ?

[12] N. TSAGOURIAS, R. BUCHAN, *International law and cyberspace*, Elgar Publishing, 2017, p. 153.
[13] N. TSAGOURIAS, R. BUCHAN, *International law and cyberspace*, Elgar Publishing, 2017, p.. 154.

Empecemos con la Carta de la ONU[14], que fue redactada hace más de 60 años y notaba en Capítulo VII "Acción en casos de amenaza a la paz, quebrantamiento de la paz o actos de agresión", en su Art. 41 que "[e]l Consejo de Seguridad podrá decidir qué medidas que no impliquen el uso de la fuerza armada han de emplearse para hacer efectivas sus decisiones, y podrá instar a los Miembros de las Naciones Unidas a que apliquen dichas medidas, que podrán comprender la interrupción total o parcial de las relaciones económicas y de las comunicaciones ferroviarias, marítimas, aéreas, postales, telegráficas, radioeléctricas, y otros medios de comunicación, así como la ruptura de relaciones diplomáticas".

Podemos deducir de este artículo que hay también otros tipos fuerza, no sólo la fuerza armada. Sin embargo, en la Carta de la ONU, se agrega en muchos lugares el adjetivo "armada" a la palabra fuerza, pero en el Artículo 2, se habla de liberar a las generaciones futuras del flagelo de la guerra, sin incluir otras formas de coerción. Así, el término fuerza armada también da lugar a interpretaciones: "armada" significa el uso de un arma, y podría no restringirse a un tipo específico. En estas condiciones, nos preguntamos: ¿Por qué no pueden ser las armas cibernéticas consideradas armas también para los propósitos de la Carta de las Naciones Unidas, si se usan con intención hostil? Hay opiniones diversas sobre si un ataque cibernético, en especial, si no tiene fuerza letal o incluso destructiva de bienes, constituye lo que en la Carta de la ONU se entiende por "uso de la fuerza" o "ataque armado"[15].

Además, otro problema con respecto a la actividad legislativa está representada por la soberanía. La soberanía la ejerce un Estado sobre su territorio y población y, aunque ningún Estado puede reclamar soberanía sobre el ciberespacio[16], lo que sí se puede decir es que todos los Estados tienen soberanía sobre sus infraestructuras cibernéticas y son responsables de todas las actividades que realizan dichas infraestructuras. Y en conexión con la soberanía tenemos también es el principio de no intervención, que se encuentra regulado en el artículo

[14] Se firmó el 26 de junio de 1945 en San Francisco, al terminar la Conferencia de las Naciones Unidas sobre Organización Internacional, y entró en vigor el 24 de octubre del mismo año. El Estatuto de la Corte Internacional de Justicia es parte integrante de la Carta.

[15] M.J. MATHESON, D.MOMTAZ, *Les règles et institutions du droit international humanitaire à l'épreuve des conflits armés récents,* Academia de Derecho Internacional de La Haya, Martinus Nijhoff Publishers, 2010, p. 180.

[16] N. TSAGOURIAS, R. BUCHAN, *International law and cyberspace*, Elgar Publishing, 2017, p. 121.

2.7 de la Carta de la ONU y tiene como fin respetar la soberanía que tiene cada Estado. Los Estados respetan los derechos soberanos, exclusivos y supremos de los otros Estados en sus territorios respectivos y no interfieren en los asuntos internos. En este caso, nos preguntamos si el ciberespacio es un asunto interno o no.
En un panorama utópico, la creación de una normativa especializada en la materia de los ciberataques sería la herramienta ideal para regular estas actividades, pero la posibilidad de que esto suceda en la realidad es limitada debido al dinamismo del ciberespacio y a la falta de voluntad de los Estados de regular, como hemos visto, aunque actualmente el Derecho internacional tiene las bases necesarias para dar respuesta a los Estados por la comisión de ciberataques, que representan obviamente hechos internacionalmente ilícitos en tiempos de paz o incluso de guerra.

Así, podemos afirmar que hay un vacío legal para los ciberataques y las posibles formas de regularlos.

IV. LA INSUFICIENCIA DE LA NORMATIVA EXISTENTE

Comenzamos a presentar la principal normativa, pero con carácter de recomendación, que existe en el plano internacional para comprender y tipificar los ciberataques.

La OTAN, durante la conferencia de Praga de 2002, decidió poner en marcha un programa global de coordinación de la ciberdefensa, con el objetivo de reforzar las capacidades de la Alianza y luchar contra los ataques informáticos. No fue hasta después de los acontecimientos de Estonia (2007), cuando se decidió a trabajar con el objetivo de definir un nuevo concepto estratégico de política de ciberdefensa, el cual fue el resultado de la Cumbre de Lisboa (2010)[17]. Así, y como resultado de esta Cumbre, los ministros de defensa de la OTAN aprobaron el 8 de junio la nueva política de ciberdefensa. En él se contemplan los ciberataques como acciones que pueden poner en riesgo la prosperidad, la seguridad y la estabilidad de los Estados miembros y se marcan directrices y recomendaciones en el área

[17] http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf, sitio accedido el 21 de julio de 2017.

de la ciberdensa. Pero es importante precisar que este documento no tiene fuerza vinculante. Además, el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN publicó en 2013 el Manual de Tallín sobre el Derecho internacional aplicable a la Ciberguerra, un documento que analiza las posibilidades de aplicar las normas que ya existen en el Derecho internacional al ámbito de la ciberguerra, pero hay que precisar de nuevo que este no es un documento oficial, sino solamente un manual que recoge las opiniones de un grupo de expertos.

En cuanto a las Naciones Unidas, las iniciativas para la regulación del ciberespacio han sido escasas y no se ha logrado, hasta el momento, un consenso internacional; no existen aún normas consuetudinarias con respecto a los ciberataques. Además, el ataque cibernético, en principio una agresión, no fue incluida por la ONU en su definición de la UN Res AG 3314/74. Por eso, pensamos que la definición de Agresión de la UN Res 3314/74, debería ser actualizada.

Sin embargo, por parte de las Naciones Unidas, tenemos algunos resoluciones de la Asamblea General en esta área:

- Resoluciones de la Asamblea General 55/63 (2000) y 56/121 (2001). A través de estas resoluciones se invita a los Estados Miembros a que tengan en cuenta las medidas propuestas, al elaborar leyes y políticas nacionales, para combatir la utilización de la tecnología de la información con fines delictivos.
- Resoluciones de la Asamblea General 57/239 (2002) para la creación de una cultura global de ciberseguridad. A través de esta resolución se intenta crear una cultura teniendo en cuenta los principios de conciencia, responsabilidad, respuesta ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y reevaluación.
- Resolución de la Asamblea General 58/199 (2004) para proteger las infraestructuras de información y estimular el desarrollo de normas de conducta en el ciberespacio.

De nuevo, hay que subrayar que estas resoluciones son recomendaciones. ¿Por qué hemos comenzado con la normativa con carácter de recomendación? Porque la normativa obligatoria en esta área, por un lado, no trata la categoría de cibertaques precisamente y, por

otro lado, los documentos obligatorios dependen de la voluntad de los Estados de convertirse en partes.

Los tratados internacionales contienen las obligaciones más importantes en el Derecho internacional. Ejemplos de este tipo de tratados incluyen las cuatro Convenciones de Ginebra y sus Protocolos (el DIH, que abordaremos más tarde), o la Convención para la Prevención y la Sanción del Delito de Genocidio[18]. Como ya hemos indicado, los tratados son de cumplimiento obligatorio para las partes, dependen de la aceptación expresa de las reglas por parte de los Estados y producen un efecto generador de obligaciones[19]. Sin embargo, ninguno de estos tratados trata los ciberataques de una manera precisa.

Para ofrecer un ejemplo concreto, utilizamos el Convenio Internacional para la Represión de la Financiación del Terrorismo[20], la cual establece la prohibición de proveer o recolectar fondos que se utilizarán en su Art. 2.1[21]. El problema es aplicar este convenio a los ciberataques, porque el artículo 2.1.b) de la Convención lo limita a actos que causen la muerte o lesiones físicas graves en las personas, con el objetivo de intimidar a una población u obligar a un gobierno o una organización internacional a realizar un acto o

[18] La Convención sobre el Genocidio fue adoptada en 1948 en respuesta a las atrocidades cometidas durante la Segunda Guerra Mundial. Desde entonces, la Convención ha sido ampliamente aceptada en la comunidad internacional y ratificada por la mayoría de los Estados. https://ihl-databases.icrc.org/ihl/INTRO/3577OpenDocument.

[19] J. CRAWFORD, *Brownlie's Principles of Public International Law***.,** 8th edition, Oxford University Press**,** p. 31.

[20] Convenio Internacional para la Represión de la Financiación del Terrorismo. Aprobado por la Asamblea General de Naciones Unidas en su resolución A/RES/54/109 de 9 de diciembre de 1999 y abierto a la firma el 10 de enero de 2000. Entrada en vigor: 10 de abril de 2002, de conformidad con el artículo 26 (1).

[21] Artículo 2
1. Comete delito en el sentido del presente Convenio quien por el medio que fuere, directa o indirectamente, ilícita y deliberadamente, provea o recolecte fondos con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte, para cometer:
a) Un acto que constituya un delito comprendido en el ámbito de uno de los tratados enumerados en el anexo y tal como esté definido en ese tratado;
b) Cualquier otro acto destinado a causar la muerte o lesiones corporales graves a un civil o a cualquier otra persona que no participe directamente en las hostilidades en una situación de conflicto armado, cuando, el propósito de dicho acto, por su naturaleza o contexto, sea intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo.

abstenerse de hacerlo. Resulta que la aplicación de la convención está limitada a los ciberataques dirigidos a un medio que implique la muerte de las personas por causa del mismo; si no, aplicar la Convención no sería posible.

También, la Convención Interamericana contra el Terrorismo establece en su Art. 4 que: "[c]ada Estado Parte, en la medida en que no lo haya hecho, deberá establecer un régimen jurídico y administrativo para prevenir, combatir y erradicar la financiación del terrorismo y para lograr una cooperación internacional efectiva al respecto". Resulta que, para aplicar esta obligación, necesitamos de nuevo la voluntad del Estado que haya ratificado el tratado, y muchas veces, esta voluntad falta.

También podemos considerar la costumbre internacional, que consiste en uniformidad, consistencia y generalidad de la práctica. En este sentido, debemos considerar los dos elementos para determinar la existencia de costumbre: generalidad en la práctica de los Estados y *opinio iuris*, pero el problema es que no hay o hay poca práctica en el ámbito de los ciberataques.

De todo lo presentado anteriormente, podemos afirmar de nuevo que hay un vacío legal en la normativa que regula los ciberataques.

V. LA CIBERGUERRA Y EL DIH

En cuanto a la cuarta cuestión tratada, hasta la aparición de Internet las guerras se habían llevado a cabo solamente en los espacios terrestre, marítimo y aéreo[22]. Es a partir de los años 2000 cuando la consolidación del crecimiento de la infraestructura tecnológica y el uso de las redes transforman el ciberespacio en un nuevo campo de batalla, donde se lleva a cabo la ciberguerra, planteando nuevos desafíos legales con respecto a la normativa aplicable.

[22] L. R. BLANK, G. P. NOONE, *International law and armed conflict*, Wolters Kluwer, 2013, p. 4.

Como premisa, primero hay que hacer una distinción entre el uso de la fuerza en el *ius ad bellum* y el recurso a la fuerza armada en el *ius in bello*. En el caso de Nicaragua[23], la CIJ consideró que "el uso de la fuerza puede en algunas circunstancias plantear cuestiones de [DIH]". Si sólo en algunas o ciertas circunstancias el uso de la fuerza plantea cuestiones de DIH, entonces se puede concluir que en otras circunstancias no lo hace. Un ejemplo sería el del suministro de armas a rebeldes que usan la fuerza contra un Estado. Tal conducta de un Estado sería inevitablemente calificada como un uso de la fuerza en virtud del Art. 2.4 de la Carta de la ONU, pero no se consideraría un "recurso a la fuerza armada" a los efectos del DIH.

Por supuesto, no hay necesidad de una declaración de guerra, ya que el uso de la fuerza armada es una condición alternativa a la declaración de guerra. Estos criterios objetivos fueron confirmados por el Tribunal Penal Internacional para Rwanda en el caso de Jean Paul Akayesu[24]. La Cámara subrayó que "la determinación de la intensidad de un conflicto no internacional no depende del juicio subjetivo de las partes en conflicto". Del mismo modo, en los casos Boškoski y Tarčulovski, la Sala de Primera Instancia del TPIY declaró que "la cuestión de si había un conflicto armado en el momento pertinente es una determinación fáctica que debe adoptar la Sala de Primera Instancia al oír y revisar las pruebas admitidas en el juicio", pero, cuando nos acercamos a la noción de fuerza armada en una ciberguerra, hay ciertas peculiaridades específicas.

La guerra cibernética o ciberguerra en DIH implica ataques informáticos que se desarrollan dentro de un conflicto armado nacional o internacional. Los ataques que no se desarrollan dentro de un conflicto armado no son parte de una ciberguerra, sino que son simples ataques informáticos que se regulan por la normativa interna de cada Estado[25]. ¿Por qué hablamos de DIH en este caso? Porque esta nueva forma de hacer la guerra no se limita solo a efectos sobre las redes, sino que sus consecuencias pueden también trasladarse al mundo físico. ¿Cómo? Consideremos, por ejemplo, el principio de distinción[26]. Es obvio que, mientras que en un conflicto armado un ataque con misiles contra un vecindario civil violaría el

[23] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits*, Judgment, *I.C.J. Reports*, 1986, p. 14, para. 216.

[24] *The Prosecutor v. Jean-Paul AKAYESU*, Sentencia en Camara I, *ICTR-96-4-T* , 1998, para. 603.

[25] *Prosecutor v. Ljube Boškoski, Johan Tarčulovski*, Sentencia de la Sala II, IT-04-82-T, 2008, para. 174.

[26] Según el principio de distinción, las partes en conflicto deben distinguir en todo momento entre civiles y combatientes. Los ataques sólo pueden dirigirse contra los combatientes y no deben dirigirse contra civiles

principio de distinción, y lo mismo ocurriría con una operación cibernética en la central eléctrica local que hiciera que la población se quedase sin electricidad durante el invierno. También en caso de paralización de los sistemas GPS durante un vuelo de aviones de rescate que prestan servicios vitales es posible que haya víctimas civiles, por ejemplo. Así, estamos sobre un terreno muy ambiguo: no está claro si los daños que se pueden causar a un Estado en un ataque cibernético serían de tal magnitud que entrasen dentro de lo que el sistema internacional denomina como DIH, que protege a los no combatientes. Sin embargo, según Jean Pictet, no es necesaria una cierta intensidad del uso de la fuerza, "no supone ninguna diferencia cuánto dura el conflicto, o cuánto sacrificio tiene lugar"[27].

No cabe duda de que el DIH es aplicable a las operaciones cibernéticas. La práctica de los Estados y la doctrina ya han acordado que, en el contexto de un conflicto armado, las normas que regulan la ejecución de las hostilidades se aplican a las herramientas y operaciones utilizadas en el ciberespacio[28].

El DIH es aplicable desde el momento en que la situación es clasificable como conflicto armado, mientras no se tenga ninguna regulación de estos nuevos conflictos llamados ciberguerras. Se divide en dos categorías principales: la primera es comúnmente llamada el "Derecho de La Haya" y cubre las normas que rigen la conducción de las hostilidades. La segunda trata las normas relativas al tratamiento de las personas en poder del enemigo (prisioneros, heridos, enfermos, etc.) y se conoce comúnmente como "Derecho de Ginebra". Se podría argumentar que los cuatro Convenios de Ginebra tienen por objeto proteger a los enfermos, los heridos, los náufragos, los prisioneros de guerra o los civiles, en los que falta el componente virtual. Por otra parte, el principio de distinción entre objetivos militares y objetos civiles, consagrado en el Protocolo Adicional I, no establece ninguna diferencia en cuanto a cómo se dañan tales objetivos u objetos. De esta interpretación resulta que los daños podrían ser causados también por un ciberataque.

---

[27] J. S. PICTET., *Commentary on the Geneva Conventions of 12 August 1949*, Geneva, 1952, vol. I, p. 29, *Commentary of 1952 to common Article 2 of the four Geneva Convetions*, pp. 31-32, disponible en https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=02A56E8C272389A9C12563CD0041FAB4, sitio accedido el 2 de octubre de 2017, *Commentary of 2016 to common Article 2 of the four Geneva Conventions*, paras. 210-219.

[28] M.N. SCHMITT., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013, p. 75

El DIH convencional no proporciona una definición explícita de lo que constituye el recurso a la fuerza armada. Sin embargo, la interpretación de los tratados pertinentes a través de la práctica de los Estados y la jurisprudencia puede ofrecer una imagen clara para la comprensión del significado de la frase. La primera oración del Art. 2, común a los cuatro Convenios de Ginebra, así como el párrafo 4 del Art. 1 del Protocolo Adicional I, relacionan el contenido del conflicto armado con el estado de guerra o de lucha y con el recurso a la fuerza armada. La frase fue posteriormente cristalizada en la doctrina y la jurisprudencia. En el caso Tadić, el Tribunal Penal Internacional para la antigua Yugoslavia, sostuvo que "existe un conflicto armado cuando existe un recurso a la fuerza armada entre los Estados"[29].

El problema es que los ataques cibernéticos son difíciles de relacionar con los conceptos de paz y guerra. De hecho, la mayoría de las operaciones cibernéticas entre Estados, incluso con fines hostiles, se llevan en tiempo de la paz y no suponen una guerra cibernética; por lo tanto, no les resulta de aplicación el Derecho de la guerra, ni una respuesta militar. El Estado víctima de tales operaciones cibernéticas puede reaccionar a través de medidas coercitivas no militares, como las contramedidas, en el ciberespacio o en el mundo real. Por lo tanto, es difícil aplicar los conceptos de combatiente y no combatiente. ¿Cómo identificar el combatiente detrás el ordenador ?

Este derecho podría ser tal vez aplicable a las operaciones cibernéticas que ocurren durante una guerra convencional o cuando estas operaciones cibernéticas son clasificables como "conflicto armado cibernético", pero no hay aún una normativa para este tipo de operaciones o para la cyberguerra. Entonces, ¿cómo clasificar una operación como conflicto armado cibernético para poder aplicar las reglas del DIH?

Un ejemplo simple sería un hack informático por parte de una unidad de inteligencia del Estado A en una instalación nuclear del Estado B. Sin duda, una explosión causada por este hack informático provocaría un conflicto armado internacional, pero ¿y la destrucción electrónica de datos en un nuevo misil balístico desarrollado por el Estado? ¿Se podria considerar también un caso de conflicto armado internacional si no existen efectos fisicos? No se ha llegado a una conclusión definitiva en la investigación doctrinal y no existe

[29] *Prosecutor v. Duško Tadić*, Decisión sobre la Demanda de defensa de la Apelación Interlocutoria sobre Jurisdicción, IT-94-1-A, 2 de octubre de 1995, para. 70.

ninguna práctica o jurisprudencia estatal relevante, ya que los argumentos apoyan a ambas corrientes.

Aunque no existe una conclusión clara, la aplicación práctica de las normas del DIH dará lugar a preguntas cuyas respuestas podrían no ser tan claras. De hecho, el DIH se aplicó a las operaciones cibernéticas de 2008 llevadas a cabo entre Rusia y Georgia porque ya había un conflicto armado entre los dos estados[30]. Sin embargo, no parece tan obvio cuándo el DIH comenzó a aplicarse a estas operaciones cibernéticas o si esas operaciones por sí solas habrían sido capaces de dar origen al conflicto armado en sí. Por lo tanto, ¿es la preexistencia de un conflicto armado por medios convencionales una condición para que el DIH se aplique a las operaciones cibernéticas o las operaciones cibernéticas pueden dar lugar a un conflicto armado?

Otro problema está relacionado con la atribución de responsabilidad de un acto de ciberguerra. En el mundo físico es más fácil identificar a las personas culpables, pero en el mundo virtual, en el medio electrónico, si utilizamos el criterio de adjudicación, como la participación de un "órgano del Estado" en la comisión de actos de guerra cibernética, en que se permite la atribución de la responsabilidad internacional de un Estado a causa de las acciones de sus funcionarios cuando causan daños, los individuos detrás de los ataques cibernéticos, lejos de ser agentes oficiales del Estado, son en su mayoría nacionales del Estado que operan desde otro territorio estatal.

Dentro de la ciberguerra, el Estado podrá ser responsable cuando el ataque cibernético esté relacionado con el Estado y no es necesario que el Estado planifique todas las operaciones de las unidades dependientes, elija sus objetivos, o dé instrucciones específicas sobre la ejecución de las operaciones militares y las presuntas violaciones de DIH si el estado lleva a cabo un papel o acto de organización, coordinación o planificación de las acciones militares del grupo militar además de financiamiento, capacitación y equipamiento para realizar la operación, pero en la mayoría de los casos es difícil probar la existencia de este papel/documento. Por lo tanto, estos criterios demuestran, por sí mismos, insuficientes para ofrecer una respuesta a la cuestión de la ciberguerra en el medio informático.

[30] M.N. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013, p. 76

VI. CONCLUSIONES

Con las nuevas tecnologías y la evolución informática, el Derecho internacional ha tenido que adaptarse a dichos cambios para encontrar una solución a estos desafíos del ciberespacio a nivel interno, pero desafortunadamente no hay un una respuesta clara y uniforme en esta área de ciberataques y tampoco una legislación especializada sobre este tema.

Un primer paso sería encontrar una definición uniformemente aceptada entre Estados o expertos que cubra todo los tipos de ciberataques, y, para conceptualizar y analizar los ciberataques, junto con esa definición resulta necesario considerar una tipificación obligatoria. Por lo tanto, pensamos que no es suficiente con referirse a los Principios Generales del Derecho a la regulación existente sobre responsabilidad internacional de los Estados y a los tratados generales que pueden también ser aplicables a los ciberataques.

Es cierto que un ciberataque puede ser activado y tener lugar únicamente en el mundo cibernético. Las dificultades residen en el hecho de que algunas operaciones cibernéticas no tienen un efecto cinético o físico, pero con una normativa obligatoria en esta área podemos encontrar soluciones.

Para concluir, es importante remarcar la inexistencia de una legislación internacional que incluya los delitos informáticos, o la posible ampliación de la legislación ya existente en la actualidad para poder incluir estos conceptos. Esto sería posible con una mejor y diferente cooperación internacional al respecto. Sin embargo, es complicado que se llegue a un acuerdo al respecto, ya que cada Estado o actor de las relaciones internacionales tiene conceptos diferentes sobre qué es un ciberataque y cómo combatirlo. A pesar de la existencia del Manual de Tallín, la comunidad internacional no pone suficiente de su parte para la creación de esta legislación o de este nuevo sistema de gobernanza en el cual exista una normativa para los ciberataques o incluso unas normas para los conflictos cibernéticos o la ciberguerra. Por eso, el DIH, al igual que el derecho internacional en general, deben interpretarse de manera evolutiva.

Bibliografía

Libros y artículos

M.C. BASSIOUNI, *Perspectives on international terrorism*, in International Criminal Law, 3rd edition, vol. I, Martinus Nijhoff, 2008

L. R. BLANK, G. P. NOONE, *International law and armed conflict*, Wolters Kluwer, 2013

W. BRENNER, JOSEPH J. SCHWERHA IV, "*Cybercrime Havens*: *Challenges and* Solutions", *Business Law Today*, vol. 17, noviembre/diciembre, 2007

E. LICHTBAU, K. BENNER, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone", *New York Times*, 18 February 2016 A1.

A. M. COLARIK, *Cyber Terrorism. Political and Economic Implications*, Hershey / London / Melbourne / Singapore, Idea Group Publishing, 2006

J. CRAWFORD, *Brownlie's Principles of Public International Law***.,** 8th edition, Oxford University Press

D. T. KUEHL, "From cyberspace to cyber power: Defining the problem", en F. D. Kramer, S. H. Starr, L. K. Wentz, *Cyberpower and National Security*, National Defense University Press 2009

M.J. MATHESON, D.MOMTAZ, *Les règles et institutions du droit international humanitaire à l'éprouve des conflits armés récents,* Academia de Derecho Internacional de La Haya, Martinus Nijhoff Publishers, 2010

J. S. PICTET, *Commentary on the Geneva Conventions of 12 August 1949*, vol. I, Geneva, 1952

B. SAUL, *Research handbook on International Law and Terrorism*, Elgar Publishing, 2014

M.N. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013

N. TSAGOURIAS, R. BUCHAN, *International law and cyberspace*, Elgar Publishing, 2017

Sitios de Internet

http://dayintechhistory.com/dith/february-7-2000-mafiaboy-ddos-yahoo-6-web-sites/
http://www.bbc.com/mundo/noticias/2014/03/140306_tecnologia_guerra_cibernetica_rusia_ucrania_aa https://www.wsws.org/en/articles/2000/05/bug-m10.html
https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf,
https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=02A56E8C272389A9C12563CD0041FAB4,

Convenios y documentos internacionales

Carta de la ONU, firmada el 26 de junio de 1945 en San Francisco, y en vigor desde el 24 de octubre del mismo año

Resoluciones de la Asamblea General 55/63 (2000) y 56/121 (2001).

Resolución de la Asamblea General 57/239 (2002) para la creación de una cultura global de ciberseguridad

Resolución de la Asamblea General 58/199 (2004) para la protección de las infraestructuras de información y estimular el desarrollo de normas de conducta en el ciberespacio

Convenio de Ginebra (I) sobre heridos y enfermos de las fuerzas armadas en campaña, 1949

Convenio Internacional para la Represión de la Financiación del Terrorismo. Aprobado por la Asamblea General de Naciones Unidas en su resolución A/RES/54/109 de 9 de diciembre de 1999

Jurisprudencia

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Juicio. I.C.J. Informes, 1986

The Prosecutor v. Jean-Paul AKAYESU, Sentencia en Camara I, *ICTR-96-4-T* , 1998

Prosecutor v. Ljube Boškoski, Johan Tarčulovski, Sentencia en Camara II, IT-04-82-T, 2008

Prosecutor v. Duško Tadić, Decisión sobre la Demanda de defensa de la Apelación Interlocutoria sobre Jurisdicción, IT-94-1-A, 2 Octubre 1995