Amenaza y uso de la fuerza a través del ciberespacio: un cambio de paradigma

Margarita Robles Carrillo [1]†

El ciberespacio impone un cambio de paradigma en la aplicación del principio de prohibición de la amenaza y el uso de la fuerza. La aparición de distintas modalidades de uso de la fuerza a través del espacio cibernético plantea la necesidad de adaptar ese principio a esta diferente realidad. Los debates en el marco de Naciones Unidas muestran que este principio es el principal obstáculo para llegar a un consenso porque no existe acuerdo entre los Estados, en particular, en cuanto a la amplitud de sus excepciones y en relación con su utilización frente a actores no estatales. El alcance y el contenido del principio deben ajustarse a su formulación originaria. Sobre esa base, hay que resolver la doble problemática que plantea la determinación de su componente objetivo y de su dimensión subjetiva con objeto de clarificar su aplicación en el ciberespacio que constituye una conditio sine qua non para garantizar la paz y la seguridad internacional.

Palabras clave: ciberespacio, uso de la fuerza, amenaza y uso de la fuerza, legítima defensa, ciberataques

I. INTRODUCCIÓN

[1]† Margarita Robles es coordinadora y profesora del Máster Propio en Ciberseguridad de la Universidad de Granada. Es profesora y miembro de la Comisión Académica del Máster Universitario en Asesoría Laboral, Fiscal y Jurídica de la Empresa de la Universidad de Granada. También se desempeña como profesora del Máster de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Granada.

La prohibición del uso o de la amenaza de la fuerza ha sido descrita, siguiendo a Pratik Ranjan Das, como "la piedra angular de la paz, el corazón de la Carta de Naciones Unidas y la regla básica del derecho internacional contemporáneo."[2] La aplicación de este principio en el ciberespacio es, por una parte, absolutamente lógica por dos motivos principales: uno, porque es una norma básica para la coexistencia social en cualquier sistema jurídico, que se manifiesta, en los derechos internos, atribuyendo al Estado el monopolio de la violencia legítima y, en derecho internacional, mediante la regulación del uso legítimo de la fuerza como hace la Carta de Naciones Unidas; y dos, porque es una norma de naturaleza imperativa en vigor que obliga al conjunto de los Estados, con independencia del medio o ámbito de actuación sea el espacio virtual o el no virtual. Pero, por otra parte, la traslación de ese principio al ciberespacio no está exenta de problemas y, entre ellos, hay dos categorías principales: los técnicos-jurídicos, derivados de la dificultad de calificar una acción cibernética como uso o amenaza de uso de la fuerza armada y, no menos importantes, los político-jurídicos, resultantes de las diferentes interpretaciones de las cuales es objeto este principio, en ocasiones, con el propósito último de eludir su prohibición o de subvertir las condiciones legítimas que permiten excepciones a dicho principio.

En un artículo titulado Nuclear Lessons for Cyber Security, Joseph Nye explica que, aunque la identificación de "revoluciones en los asuntos militares" es arbitraria, hay que incluir entre ellas "la revolución de la información que ha producido, hoy en día, un crecimiento extremadamente rápido del ciberespacio."[3] En una línea de argumentación similar, Irving Wladawsky-Berger considera que, ahora, "una cuarta Revolución Industrial se está construyendo a partir de la tercera, la revolución digital que ha estado ocurriendo desde mediados del siglo pasado". En su opinión, esa revolución se caracteriza "por la fusión de tecnologías que está borrando los límites entre los ámbitos físicos, digitales y biológicos."[4] El cambio afecta inexorablemente a todos

[2] P.R. Das, "Linking Cyber Attacks And The Use Of Force In Public International Law: An Exercise In Interpretation", Nalsar International Law Journal, Vol. 1, Nº 1 (2015), p. 123.

[3] J.S. Nye Jr., "Nuclear Lessons for Cyber Security?", Strategic Studies Quarterly, (2011), p. 18 (http://www.au.af.mil/au/ssq/2011/winter/nye.pdf).

[4] Explica el autor que "casi todo el mundo está de acuerdo en que existe una diferencia cualitativa importante entre la primera y la segunda revolución industrial. Mientras algunos creen que la cuarta no es más que la evolución de la tercera, Schwab argumenta que son cualitativamente diferentes por tres razones principales: Velocidad: En comparación con las tres revoluciones

los ámbitos de la vida social y política y, en particular, a la seguridad internacional. En realidad, desde la Guerra del Golfo en 1991, el uso de la tecnología conduce a la afirmación de una "revolución en los asuntos militares (RMA, por sus siglas en inglés)."[5]

En una sesión del Comité de Asuntos Exteriores de la Cámara de Representantes del Congreso estadounidense realizada en septiembre de 2015 sobre el tema Cyber War: Definitions, Deterrence, and Foreign Policy, Matt Salmon afirma que "No es una exageración afirmar que estamos en el amanecer de una nueva era de guerra. (…) Si ocurre o no una guerra cibernética total está claro que estamos en un estado de conflicto cibernético continuo."[6]. En esa misma sesión, a propósito de los trabajos en Naciones Unidas, James A. Lewis afirma que "el punto esencial de desacuerdo es acerca del artículo 2.4 de la Carta de Naciones Unidas, que insta a los miembros de la organización a abstenerse de recurrir al uso de la fuerza para solucionar conflictos y el artículo 51 que reitera el derecho inmanente de los Estados miembros de legítima defensa en caso de ataque armado."[7]

El objeto de este trabajo es analizar el principio de prohibición del uso y de la amenaza de la fuerza a través del ciberespacio para tratar de constatar hasta qué punto y en qué medida implica y exige un cambio de paradigma en la organización de la seguridad colectiva. Con esa intención se aborda, en primer término, el contexto fáctico (I), político (II) y jurídico (III) en el que se enmarca dicho principio para, a continuación, analizar su alcance y contenido (IV) y sus componentes principales objetivo (V) y subjetivo (VI).

---

anteriores, la cuarta está evolucionando a un ritmo exponencial en lugar de un ritmo lineal. Alcance: Los efectos tienen lugar en casi todas las industrias en todos los países. Impacto en sistemas: La amplitud y profundidad de estos cambios anuncian la transformación de los sistemas enteros de producción, la gestión y la gobernabilidad." (Irving Wladawsky-Berger, The Fourth Industrial Revolution, online: http://blog.irvingwb.com/blog/2016/02/the-fourth-industrial-revolution.html).

[5] B.T. O'Donnell y J.C. Kraskam "International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement", International Legal Studies, Vol. 76 (2002), p. 396. En el mismo sentido J. Jun, S. LaFoy y E. Sohn, North Korea's Cyber Operations. Strategy and Responses (Londres: Center for Strategic & International Studies, 2015) pp. 19-20; S. Amit. "Cyber Wars: A Paradigm Shift from Means to Ends", Strategic Analysis, Vol. 34, Nº 1 (2010), pp. 62-73.

[6] Cyber War: Definitions, Deterrence, And Foreign Policy", Hearing Before The Committee On Foreign Affairs House of Representatives. First Session. 30 de septiembre de 2015, p. 1. Disponible en:
http://foreignaffairs.house.gov/hearing/hearing-cyber-war-definitions-deterrence-and-foreign-policy.

[7] Ibíd., p. 12.

II. UNA APROXIMACION A LA PRACTICA INTERNACIONAL.

La práctica internacional muestra que los Estados pueden realizar acciones en el ciberespacio susceptibles de ser calificadas como uso o amenaza de la fuerza y no sólo entendida en sentido virtual sino, también, con repercusiones físicas o materiales.

Hace tiempo que la ciberseguridad se encuentra en las agendas y estrategias de seguridad de los Estados no sólo en el plano de las declaraciones sino, también, a nivel operativo. Como explica Lewis, "cinco países tienen capacidades avanzadas de ciberataque: Estados Unidos, Reino Unido, Rusia, China e Israel. A su vez, varios otros países están desarrollando estas capacidades. Incluidos Irán y Corea del Norte, los cuales han llevado a cabo ciberataques contra compañías americanas"[8]. Corea del Norte muestra un activismo tan preocupante como el conjunto de su política en el ámbito militar.[9] En el proceso de modernización de su ejército, China ha creado la llamada Fuerza de Apoyo Estratégico centrada en el ámbito cibernético.[10] Es también un punto dentro de los nueve destacados de la Estrategia Nacional de Seguridad de Rusia.[11] La British Army ha establecido dos estructuras: la Brigada 77 para las operaciones psicológicas y la primera Brigada Intelligence, Surveillance and Reconnaissance, que combina guerra electrónica e inteligencia. En EE.UU., recientemente, el documento Beyond the Build: Delivering Outcomes Through Cyberspace del US Cyber Command Chief establece entre sus prioridades el desarrollo de capacidades operativas.[12]

En realidad, desde 2007, EE.UU. ha elaborado un marco político, doctrinal y operativo para el uso ofensivo de ciberoperaciones y reconoce su uso tanto en Afganistán como en Irak, bajo la cobertura de la autorización de las respectivas misiones. Según Lewis, el primer caso de un ciberataque con fines militares tiene lugar a mediados de los

---

[8] Lewis, supra nota 5, p. 4.

[9] Sobre las operaciones realizadas por este país, véase Jun et al., supra nota 4, p. 79.

[10] http://www.albanydailystar.com/world/china-creates-cyber-warfare-army-division-15046.html .

[11] http://usdefensewatch.com/2016/01/russias-national-security-strategy-for-2016-in-9-key-points-2/.

[12] http://www.defense.gov/News-Article-View/Article/616512/us-cyber-command-chief-details-plans-to-meet-cyberspace-threats.

noventa cuando EE.UU. usa un primitivo método cibernético contra Serbia.[13] A finales de esa década, China trabaja seriamente sobre la capacidad de los ciberataques para conseguir una ventaja asimétrica sobre EE.UU., mientras que, frente a esa perspectiva, en 1998, Rusia hace su primera propuesta de un tratado para limitar el uso de las armas cibernéticas[14]. Siguiendo un estudio realizado por la ONU, ya en 2013, más de treinta Estados incluyen la ciberguerra en su planificación militar operativa y más de ciento cuarenta han incorporado las armas cibernéticas a sus programas de desarrollo armamentístico. El conflicto en Siria es ahora el escenario de una guerra cibernética en la que participan, asimétricamente, Estados y actores no estatales, y los objetivos y métodos de los ciberataques están lejos de adecuarse a las normas del derecho internacional de los conflictos armados.

En ese contexto, como explican Rauscher y Korotkov, "cada vez hay más preocupación acerca de las posibles consecuencias de las armas cibernéticas que tienen la capacidad de iniciar nuevos tipos de agresión, un efecto cascada de múltiples grados, y la devastación social y económica. Las armas cibernéticas pueden generar, en un abrir y cerrar de ojos, comportamientos virales salvajes que son fácilmente reproducibles y transferibles, mientras que carecen de la capacidad de discriminar entre objetivos puntuales. Estas propiedades combinadas con una causa beligerante son un motivo de preocupación comprensible."[15] El avance científico y el desarrollo tecnológico incorporan, en efecto, medios y métodos de acción diferentes y alternativos al uso tradicional de la fuerza.

La experiencia cibernética muestra varias modalidades de actuación susceptibles de ser calificadas como uso de la fuerza que pueden ser clasificadas en las siguientes categorías: el uso subrepticio de la acción cibernética, el uso paralelo del ciberataque y del armamento convencional, el uso combinado de ambos y, por último, el uso del ciberataque como alternativa a la acción militar convencional.

---

[13] J.H. Smith y G.N. Lederman, "Weapons like to Lightning. US Information Operations and US Treaty Obligations", International Legal Studies, Vol. 76 (2002), p. 378. En prensa se publicaba la noticia de que, en realidad, Vietnam había sido el primer caso de ciberguerra de la historia (http://www.elconfidencial.com/tecnologia/2016-03-06/la-cara-menos-conocida-de-vietnam-la-primera-guerra-electronica-de-la-historia_1163446/.

[14] Lotrionte, supra nota 5, p. 17.

[15] K.F. Rauscher y A. Korotkov, Russia-U.S. Bilateral On Critical Infrastructure Protection. Working Towards Rules for Governing Cyber Conflict Rendering the Geneva and Hague Conventions in Cyberspace (Nueva York: EastWest Institute, 2011), p. 8.

A. El uso subrepticio de la acción cibernética

El análisis de la práctica internacional permite identificar situaciones en las que se hace uso de una acción cibernética con una finalidad específica, no necesariamente lícita, pero difícil de calificar desde el punto de vista jurídico, para alcanzar unos determinados objetivos que suelen tener unos resultados concretos, reales y generalmente efectivos. El anonimato y la opacidad son características del ciberespacio que facilitan la proliferación de este tipo de acciones que, en caso de ser auspiciadas por algún país, se benefician en términos de impunidad de la problemática que plantean la trazabilidad y la atribución de responsabilidad al Estado. No faltan los ejemplos, aunque sí, con demasiada frecuencia, las pruebas de este tipo de uso de la acción cibernética.

El término "subrepticio" o clandestino sirve para catalogar aquellas situaciones en las que el uso del ciberataque es la manifestación y la reacción encubierta frente a una situación de tensión, controversia o conflicto en el plano interestatal, que no aflora abiertamente como tal y se circunscribe a acciones en el ciberespacio. La acción cibernética permite infringir daños incluso similares a los de la acción cinética sin que haya constancia del autor, ni reconocimiento de la situación de conflicto, ni de la responsabilidad última del Estado, salvo que asuma como propia la acción. Los dos ejemplos más ilustrativos de esta modalidad de acción, por ser algo distintos, son Estonia y Ucrania. En el caso de Estonia, en 2007, no se ha podido demostrar la implicación rusa a pesar de la convicción generalizada de que este país apoyaba y promocionaba los ciberataques. Ucrania, por su parte, está siendo objeto de ciberataques a sus infraestructuras críticas que sólo parecen tener una finalidad política que se explica en el contexto de la situación de tensión con Rusia.

El caso de Estonia es paradigmático no sólo porque constituye el ejemplo por excelencia de las consecuencias de una acción cibernética para un Estado, sino también porque se convierte en el punto de inflexión a partir del cual muchos países y organizaciones internacionales asumen el problema de la ciberseguridad[16]. La primera

[16] El origen del asunto se encuentra en la imagen del Soldado de Bronce que encierra un simbolismo contradictorio porque mientras que para los rusos constituye un monumento a los libertadores de Tallin durante la Segunda Guerra Mundial, en cambio, para los estonios no deja de

conclusión a la que lleva ese asunto es, precisamente, la evidencia de que la amenaza cibernética es real y muy atractiva para causar un gran daño con un mínimo riesgo. En segundo lugar, sirve para demostrar la imposibilidad de reaccionar aisladamente y la necesidad de una cooperación internacional para frenar un ataque cibernético[17]. En tercer lugar, es una prueba de la impunidad del ciberataque porque concluye con una sanción menor a un individuo, sin llegar a la posibilidad de demostrar la implicación de Rusia a pesar de los muchos argumentos que avalaban su responsabilidad[18]. Por último, este caso demuestra que la amenaza cibernética no sólo puede afectar al normal desenvolvimiento de la vida de los ciudadanos de un país, sino que puede atacar su estructura y las infraestructuras críticas nacionales que, además de provocar daños materiales, pueden conllevar el riesgo de daños físicos para la población.

Ucrania ha sido también el escenario de una utilización clandestina de la acción cibernética que se enmarca, asimismo, en el contexto de las tensas relaciones con Rusia. En realidad, si las acciones fuesen

---

ser la representación de la dominación soviética. En 2007, la reacción al traslado de la estatua al Cementerio militar de las Fuerzas de Defensa estonias consiste en una sucesión de ciberataques en forma de Denegación de Servicio y Denegación Distribuida de Servicio que tienen como objetivos el conjunto de webs, redes y servicios estatales, afectando prácticamente al 100% de las mismas, así como a los servicios de e-banking con un porcentaje de incidencia en torno al 90% de las transacciones bancarias. Estonia es un país con una gran dependencia de las TICs por lo que resulta especialmente vulnerable a un ciberataque. Es, además, un país de dimensiones reducidas y perteneciente a la OTAN, con lo que un ciberataque masivo podía provocar una situación de crisis de seguridad nacional y podía, también, ser la vía para contrastar la capacidad cibernética de la Alianza Atlántica. Sobre este caso pueden verse M. Robles Carrillo, "Las Fuerzas Armadas ante el reto de la ciberseguridad", en S. Olarte Encabo (dir.), Estudios de Derecho Militar y Defensa (Madrid: Thomson Reuters Aranzadi, 2015) pp. 431-433; R. Heickerö, Emerging Cyber Threats and Russian Views on Information Warfare and Informations Operations (Estocolmo: Swedish Defense Research Agency, 2010); P.A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue y J. Spiegel, "The Law of Cyber-Attack", California Law Review, Vol. 100 (2012), pp. 817-885; J. Nazario, "Politically motivated denial of service attacks", The Virtual Battlefield: Perspectives on Cyber Warfare(2009), pp. 163-181.

[17] A pesar de la rapidez de la respuesta, la solución técnica fue claramente insuficiente por dos motivos principales: 1) la falta de capacidad técnica del Estado para ejecutar acciones sobre el tráfico de Internet por redes físicamente localizadas fuera de su territorio; 2) la ausencia de competencia para aplicar sus normas más allá de su territorio y su jurisdicción (D. Weissbrodt, "Cyber-conflict, Cyber-crime, and Cyber-Espionage", Minnesota Journal of International Law, Vol. 22 (2013), pp. 347-387).

[18] La implicación de Rusia y de ciudadanos rusos en los ataques no ofrece dudas tanto por las evidencias prácticas -el tráfico malicioso en lengua rusa o las instrucciones para realizar los ciberataques contenidas en foros, blogs y sitios web rusos-, como especialmente por la actitud de las autoridades rusas y, en particular, la renuncia por parte del gobierno ruso a prestar su ayuda, la falta de acción ante bloqueo de la Embajada de Estonia en Moscú y la presión económica ejercida por Rusia coincidiendo con los ciberataques, materializada en el corte de la frontera a transportes pesados y ferroviarios procedentes de Estonia o en las cancelaciones de contratos de importación de productos fabricados en Estonia, entre otros.

atribuibles a Rusia, se trataría de un supuesto de uso paralelo del arma cibernética[19], pero al carecer de pruebas acerca de su efectiva implicación más allá de las sospechas generalizadas, sólo admite rigurosamente su calificación como un uso clandestino.[20]

Los ciberataques contra la red eléctrica del oeste de Ucrania, en diciembre de 2015, tienen como objetivo los sistemas de control industrial de varias empresas energéticas provocando apagones que han afectado a un porcentaje importante de su población. Los sistemas de control industrial se infectan mediante una versión mejorada del malware BlackEnergy que se vincula a un grupo apoyado por Rusia, Sandworm Team, que ya han sido autores de acciones similares. En esa versión, BlackEnergy desactiva el reinicio de los ordenadores infectados incluyendo el malware KillDisk.[21] Según una información publicada por expertos en seguridad de la información, el ataque cuenta con tres componentes coordinados: en primer lugar, el malware, que tiene acceso al sistema; en segundo lugar, el ataque de denegación de servicio (DoS) contra las redes telefónicas de las empresas, que sirve para impedir cualquier respuesta de emergencia y prolongar el impacto del ataque; y, en tercer lugar, la interacción directa del malware habilitada por los piratas informáticos, lo que causa la falla física de las rejillas. En enero, una nueva oleada de ciberataques se dirige contra servicios públicos, incluido el aeropuerto internacional de Boryspil de Kiev. Aunque Rusia ha negado cualquier implicación, además del contexto de fondo de sus relaciones con Ucrania, el ataque sólo tiene sentido por el beneficio que pueda reportar a ese Estado porque carece de la rentabilidad económica que podría justificar la autoría del ciberdelincuente, máxime cuando se están atacando servicios públicos e infraestructuras críticas nacionales.

---

[19] Sería así en caso de haberse demostrado la autoría de Rusia. Siguiendo a Lotrionte, "dado que el conflicto entre Rusia y Ucrania es internacional en su naturaleza las ciberoperaciones subsiguientes están sujetas al derecho internacional humanitario" (Lotrionte, supra nota 5, p. 15).

[20] Lanoszka afirma que se trata directamente de un caso de guerra híbrida (A. Lanoszka, "Russian hybrid warfare and extended deterrence in eastern Europe", International Affairs, Vol. 92, Nº 1 (2016), pp. 175-195).

[21] L. Chakarova, EU and NATO design response to cyber-attacks, Jane's Intelligence Review (2016), pp. 1-4.

Los casos de Estonia y Ucrania podrían ser calificados como un uso de la fuerza[22] si el ciberataque hubiese podido imputarse a un Estado.[23] En ambos casos, las sospechas recaídas sobre Rusia no se han visto acompañadas de pruebas irrefutables de su implicación, pero es difícil encontrar otra motivación. Puede ser, efectivamente, que individuos o grupos de hackers actuando por su cuenta y riesgo hayan decidido actuar contra ambos países. Sin embargo, puede ser, también, que la opacidad y el anonimato en la red se hayan convertido en el caldo de cultivo para una nueva forma de expresión de la conflictividad interestatal mediante el uso de proxys o sustitutos con la intención de excluir la responsabilidad de cualquier Estado en esos sucesos.[24]

El uso clandestino del ciberataque cambia las reglas del juego en muchos sentidos y ninguno es positivo. Canalizar las posibles tensiones interestatales por esa vía, que sólo reporta beneficios al agresor, contribuirá más a una escalada de la tensión que a la búsqueda de una solución pactada entre las partes que sería lo deseable. No obstante, lo realmente grave es que se está generando una "práctica de impunidad" en el espacio cibernético porque empieza a ser habitual que se produzcan estas situaciones y que resulte imposible atribuir su autoría a un responsable internacional. Desde esa perspectiva, más allá de que los casos de Estonia y Ucrania se puedan calificar como uso de la fuerza, parece previsible que la evolución futura de esta modalidad de acción cibernética conduzca en su progresión natural a ese resultado que sólo puede alimentar la conflictividad internacional.

B. <u>El uso paralelo del ciberataque y del armamento convencional</u>

A diferencia del caso anterior, la modalidad de uso paralelo de la acción cibernética se sitúa en un contexto de conflicto armado, siendo ésta una circunstancia que facilita la calificación del ciberataque y las posibilidades de su atribución a un Estado.

---

[22] Sobre la dificultad de calificar los ciberataques en el caso de Estonia como cibercrimen, ciberterrorismo o ciberguerra, véase S.J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", Berkeley Journal of International Law, Vol. 27, Nº 1 (2009), pp. 232-233.

[23] Weissbrodt analiza el caso de Estonia aplicando los diferentes criterios doctrinales sobre la prohibición del uso de la fuerza y llegando a conclusiones distintas en cada uno de ellos (Weissbrodt, supra nota 16, p. 376).

[24] Crimea es un escenario que se ha caracterizado por la ausencia de identificación de algunas fuerzas militares procedentes, al parecer, precisamente de Rusia.

En esta categoría se engloban aquellas acciones cibernéticas desarrolladas de modo paralelo a la acción militar, pero sin una conexión estratégica, operativa o táctica en términos militares entre ambas. La acción cibernética no tiene una incidencia directa en el teatro de operaciones o en el dispositivo militar, sino que se concreta en la realización de ciberataques que favorecen a alguna de las partes por el impacto psicológico que imponen en el desarrollo del conflicto[25]. Como ejemplos se identifican los casos de Georgia y Siria.

El conflicto de Georgia con Rusia, por la situación de Osetia del Sur en 2008, muestra la utilidad a esos efectos de la acción cibernética[26]. Los ciberataques se realizan en paralelo a las operaciones militares y coincidiendo en intensidad y frecuencia con ellas, aprovechando la limitada capacidad de respuesta del país por su escaso desarrollo tecnológico.[27] Como en el caso de Estonia, Georgia demuestra la inviabilidad de una respuesta individual frente al ciberataque, la necesidad ineludible de una cooperación internacional y la imposibilidad de demostrar la implicación de Rusia, a pesar de que en este caso es evidente la motivación. Sin embargo, al tratarse ahora de acciones cibernéticas en el marco de un conflicto armado, hay otras conclusiones complementarias. La primera es que el ciberataque se convierte en un componente adicional a las operaciones militares incluido en el diseño global en la medida en que las ciberoperaciones están bien planificadas, organizadas y coordinadas en tiempo y espacio

---

[25] Gill y Duchaine califican esta modalidad como uso combinado porque no establecen otras categorías, ni distinguen este tipo del uso paralelo (T.D. Gill y A.L. Ducheine, "Anticipatory Self-Defense in the Cyber Context", International Law Studies, vol. 89 (2013), pp. 461-463).

[26] En 2008 tiene lugar la Guerra de Osetia del Sur entre Georgia, por un lado, y Osetia del Sur, Abjasia y Rusia por el otro, como consecuencia de un ataque realizado por las Fuerzas Armadas de Georgia contra las fuerzas separatistas osetias. Este hecho provoca la reacción de Rusia dirigida a proteger a los ciudadanos rusos fuera de sus fronteras. En agosto de 2008, el Presidente de Georgia declara el estado de guerra, al considerar que se ha producido una agresión militar por parte de la Federación Rusa contra Georgia. Véanse, sobre este caso, Robles Carrillo, supra nota 15, pp. 433-435; K. Giles, "Information Troops – A Russian Cyber Command", en C. Czosseck, R. Ottos y K. Ziolkowsky (eds.), Proceedings 2012 4th International Conference on Cyber Conflict, Tallin, 2011, pp. 45-60: Heickerö, supra nota 15; Nazario, supra nota 15, pp. 163-181.

[27] En este caso se trata de ataques prolongados y múltiples de tipo ICMP flood, TCP SYN flood, HTTP flood contra sitios web oficiales; ataques DDoS a través de botnets, con centros de mando y control dispersos en diferentes países, mejor organizados y coordinados, con mayor capacidad destructiva; y ataques de tipo inyección SQL, bien planeados y organizados que resultan difíciles de detectar. Como respuesta técnica, el Proyecto Gery Goose 2 es una iniciativa de Inteligencia de Fuentes Abiertas (Open Source Intelligence -OSINT) lanzada el 22 de agosto 2008 con la función de examinar los ciberataques rusos contra Georgia y comprobar la implicación del gobierno ruso y de los movimientos de voluntarios rusos. Este proyecto identificó dos sitios web rusos desde donde se organizan ciberataques coincidiendo con el conflicto armado: «www.stopgeorgia.ru» y «www.xakep.ru».

con las acciones cinéticas. Una segunda conclusión es que el objetivo del ciberataque consiste esencialmente en debilitar la capacidad de respuesta militar y política de Georgia mediante operaciones psicológicas para desmoralizar al adversario y en operaciones propagandísticas para reclutar adeptos a la propia causa. La tercera conclusión es que la autoría de los ciberataques corresponde, en gran medida, a voluntarios que pueden residir en el propio país o a un tercero lo que supone un cambio significativo en las reglas del juego. Son varios los interrogantes y, entre ellos, principalmente dos: uno, la posibilidad de atribuir esas acciones a Rusia en la medida en que la forma de realizar dichas acciones dificulta la trazabilidad de las mismas; y, dos, la definición del estatuto de los cibernautas autores de las acciones ya que, al tratarse de ciberataques realizados en el marco de un conflicto armado, podrían o deberían estar sometidos al régimen jurídico específico que regula esa situación en derecho internacional.[28]

Siria es un escenario en el que la acción cibernética está prácticamente asumida por todos los operadores implicados en el conflicto hasta tal punto que resulta difícil establecer pautas de acción porque se cruzan ciberataques entre distintos tipos de destinatarios y con diversos objetivos. Hay, paradójicamente, un mayor equilibrio en cuanto al uso de estas medidas por todas las partes, y no sólo una, pero hay también una mayor asimetría entre los actores que recurren a esta modalidad de acción. El llamado Ejército Electrónico de Siria (SEA, por sus siglas en inglés) es un grupo de hackers informáticos leales al Presidente Bashar al-Assad que lanza sus ataques frente a cualquiera de los Estados, en particular, EE.UU. y no sólo contra sus recursos cibernéticos públicos, sino también se dirigen contra sus empresas privadas. En sentido opuesto, la agencia de noticias oficial siria, Sana, ha sido víctima de modo recurrente de ciberataques impidiendo el acceso a sus páginas web. La prensa ha informado sobre un plan secreto de ciberataque contra el Gobierno de Bashar al-Assad promovido por EE.UU. que, ya desde 2011, se concibe como una batalla cibernética cuyo objetivo principal son determinadas infraestructuras críticas. Esta opción es una alternativa de bajo coste material y humano, pero que, al parecer, no se pone en marcha por el temor a posibles represalias sobre

[28] Europa Press apuntaba, como autores, al grupo "Sandworm". (http://www.europapress.es/internacional/noticia-informe-senala-piratas-informaticos-responsables-apagon-ucrania-20160110072937).

sus propias infraestructuras, algo que es perfectamente posible en el mundo cibernético porque es un espacio reductor de las asimetrías entre actores estatales y entre ellos y los no estatales. La opción cibernética es especialmente atractiva desde que se contempla, además, como una fórmula intermedia entre la no intervención y la participación sobre el terreno que, naturalmente, plantea mayores problemas.

Los ciberataques en Georgia y Siria constituyen, pues, modalidades del uso paralelo de la acción cibernética en el contexto de un conflicto armado. Son, por una parte, una práctica perfectamente lógica, como ha ocurrido a lo largo de toda la historia de la humanidad, porque la guerra absorbe de modo directo y natural para sus fines los avances y desarrollos tecnológicos. No obstante, son, por otra parte, un motivo de preocupación en la medida en que, convirtiéndose en una alternativa más atractiva que la acción cinética y con mayores posibilidades de proyección, puede tener un efecto multiplicador del conflicto no sólo en términos materiales y funcionales, sino también subjetivos por su capacidad para integrar a cualquier actor como consecuencia de la interconexión, la opacidad y el anonimato de la red.

C. El uso combinado del ciberataque y de la acción militar convencional

El uso combinado de la acción cibernética es una modalidad claramente diferenciada del uso paralelo en la medida que, a diferencia de este último, implica que la acción cibernética está integrada en el dispositivo militar en términos estratégicos, tácticos y/o operativos. En este caso, la acción ciberespacial afecta, condiciona, permite o facilita la operación militar convencional que no sería posible con los mismos parámetros y con idéntica secuencia sin la fase previa cibernética. Como ejemplos de esta categoría se encuentran la "Operación Huerto" y la "Operación Gerónimo".

La "Operación Huerto" supone un uso prematuro del ciberataque como parte integrante de una operación militar que, de no haber existido la acción cibernética, podría haber tenido un resultado completamente distinto y con mayores riesgos, menores garantías y menor efectividad[29]. La acción cinética es claramente atribuible a Israel,

[29] La Operación Huerto consiste en un ataque aéreo israelí sobre un objetivo conocido por los sirios con el nombre clave de Al-Kibar, situado en la región de Dayr az-Zawr, en la República Árabe de Siria, llevado a cabo el 6 de septiembre de 2007. La particularidad de este caso radica en que,

mientras las pruebas de la existencia del ataque cibernético o, incluso, de los mismos hechos son más difusas como demuestran las reacciones políticas en Siria, Corea del Norte y el propio Israel. En cualquier caso, al tratarse de parte de un operativo más amplio del cual sólo es un componente es razonable atribuirle la misma calificación que a la acción global en su conjunto porque facilita o posibilita el uso de la fuerza como ocurre en este caso mediante el ataque aéreo israelí al enclave de Al-Kibar. Una secuencia similar se reproduce mucho tiempo después en la "Operación Gerónimo" llamada, también, "Operación Lanza de Neptuno".

"Operación Gerónimo" es la denominación atribuida a la captura de Bin Laden en 2011 por unidades de élite de las fuerzas militares estadounidenses en el transcurso de un tiroteo en Abbottabad.[30] La operación es posible porque, desde Fort Meade, Maryland, efectivos del Mando de Ciberdefensa de EEUU facilitan la incursión mediante una acción cibernética realizada para infiltrarse y apagar el sistema de defensa aérea de Pakistán impidiéndole identificar el asalto físico de las unidades enviadas por EE.UU. En este caso, la atribución de la acción cibernética no plantea dudas porque forma parte del dispositivo global de la operación.

Más allá del asunto de la calificación, hay que cuestionar la licitud de esas operaciones desde una perspectiva general. La acción unilateral de un Estado violando el principio de soberanía territorial y la jurisdicción de otro Estado, interfiriendo en sus estructuras de control para neutralizarlas o inutilizarlas y, además, no menos importante,

---

para llevar a cabo la operación, se utiliza un sistema tecnológico similar al Suter, desarrollado por EE.UU., mediante el cual los aviones de combate de la Fuerza Aérea Israelí penetran en el espacio aéreo sirio sin ser detectados por radar. Aunque hay varias teorías, la explicación más convincente apunta que, con ese sistema, se manipula la señal recibida por los radares enemigos, mostrando en sus sensores objetivos falsos, de manera que permite invadir las redes de comunicaciones, ver los sensores del enemigo y controlarlos para alterar la información detectada por los radares. De acuerdo con la información que se da a conocer en los diversos medios de comunicación, el ataque es realizado por el 69º Escuadrón de F-15I Strike Eagle de la Fuerza Aérea Israelí, además de aviones F-16 Fighting Falcon y una aeronave militar de Inteligencia Electrónica. Un informe indica que un comando de Shaldag que forma parte de la Fuerza Aérea Israelí accede el día previo para señalizar los objetivos vía Láser. Los miembros del Sayeret Matkal, unidad de las Fuerzas de Defensa Israelíes, se introducen en la central nuclear siria antes del ataque del 6 de septiembre y llevan pruebas a territorio israelí sobre la procedencia de dicho material de Corea del Norte (Robles Carrillo, supra nota 15, pp. 435-437).

[30] Según la información oficial, en poco más de tres horas, el equipo entra en el espacio aéreo paquistaní, asalta el complejo en Abbottabad y vuelve de regreso a Afganistán, sin que las autoridades paquistaníes tengan conocimiento de la incursión (S. Moore, "Cyber Attacks and the Beginnings of an International Cyber Treaty", North Carolina Journal of International Law, Vol. XXXIX (2013), pp. 223-257).

infringiendo daños materiales y personales es posible, en ambos casos, gracias a una acción cibernética que garantiza la consecución del objetivo militar.

En ambas operaciones, el ciberataque es un factor decisivo en la organización y en el éxito de la misión, fácilmente atribuible al Estado autor de la acción cinética y es una manifestación de uso de la fuerza porque es un componente necesario para su empleo en los términos en los que se producen los hechos. No hay, sin embargo, un planteamiento sobre su licitud o ilegalidad como actos autónomos. Esa calificación habría sido necesaria si no se materializa finalmente la acción cinética y los hechos se circunscriben a la parte cibernética, porque ésta sería la única sobre la que habría que preguntarse a propósito de su calificación como uso o amenaza de la fuerza. Esa es la situación cuando se usa el ciberataque como alternativa frente a la acción militar tradicional.

D. <u>El uso del ciberataque como alternativa a la acción militar convencional</u>

La acción cibernética puede ser una alternativa a la acción militar tradicional en cuyo caso, a diferencia de los precedentes, no recibe la cobertura de las acciones cinéticas a las que acompaña o en las que se integra a efectos de su calificación. En ese caso se trata de una acción sólo cibernética para cumplir una función o alcanzar un objetivo sin utilizar medios cinéticos de empleo de la fuerza. Después de Flame,[31] Stuxnet ejemplifica este caso.

Stuxnet es identificado por una compañía de seguridad informática de Bielorrusia al descubrirlo en unos ordenadores pertenecientes a un cliente iraní.[32] Hace tiempo que se sospecha que Irán estaba desarrollando un programa nuclear cuando, en 2010, sufre un ataque informático contra sus instalaciones nucleares que se considera entonces el ataque cibernético más grande de la historia.[33] Según los

---

[31] Weissbrodt, supra nota 16, pp. 352-354. Flame y Stuxnet son reconocidos generalmente como armas cibernéticas.

[32] J.R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", Security Studies, Vol. 22, Nº3 (2013), pp. 365-404 (DOI:10.1080/09636412.2013.816122); M.J. TEPLINSKY, "Fiddling on the Roof: Recent Developments in Cybersecurity", American University Business Law Review, Vol. 2, Nº 2 (2013), pp. 270 y ss.

[33] Los sistemas de control de la central nuclear de Bushehr, así como de otras industrias, se ven afectados por este virus con una potencia sin precedentes que se convierte en un agente durmiente y se puede accionar a distancia en el momento que su creador lo desee sin conocimiento del usuario del dispositivo. Es un programa de software dañino del tipo troyano muy avanzado, que aprovecha la vulnerabilidad MS10-0466 de los sistemas operativos Windows CC,

expertos en seguridad informática, por la complejidad del programa, no puede ser el trabajo de un pirata informático o de un grupo de hackers porque sólo los Estados y, dentro de ellos, sólo algunos pueden disponer de los recursos y la capacidad para diseñar y poner en marcha ese programa. Stuxnet ha sido calificado como el primer ejemplo de guerra cibernética o como un misil cibernético de precisión de carácter militar.

En este caso, el ciberataque se utiliza como alternativa al uso de la fuerza armada cinética frente a una posible amenaza nuclear demostrando su enorme eficacia al cumplir su función sin ser detectado. Las sospechas recaídas sobre Israel y EE.UU. se desvanecen frente a la imposibilidad material de demostrar su autoría, mientras que la situación del Estado víctima se complica porque cualquier reacción puede ser interpretada como un reconocimiento implícito del incumplimiento por su parte de las disposiciones del Tratado de No Proliferación Nuclear.

La diferencia de este caso respecto de los anteriores es que permite y ha propiciado el debate sobre su calificación como acción autónoma. Una idea no necesariamente compartible es la definición de ese ciberataque como un ejercicio de legítima defensa anticipada[34], lo que implica reconocer que es imputable a uno o más Estados y que es un uso de la fuerza según el derecho internacional. Weissbrodt explica que puede ser un uso de la fuerza y ser susceptible, también, de ser calificado como un ataque armado.[35]

En realidad, las cuatro modalidades de uso de la acción cibernética son diferentes entre sí y en sus consecuencias. El uso alternativo y el uso encubierto son los que plantean mayores problemas en cuanto a su calificación como uso de la fuerza, a pesar de que sus efectos pueden ser

---

empleados en los sistemas SCADA (Supervisory Control and Data Acquisition). Se trata de un virus muy sofisticado que utiliza técnicas de rootkit para instalarse en el sistema operativo. Una vez dentro de una planta, puede reprogramar las centrifugadoras para hacerlas fallar sin ser detectadas. Según los expertos, es el primer virus capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas. Por otra parte, este tipo de virus no pretende la infección masiva de ordenadores domésticos, sino que está pensado para atacar a infraestructuras críticas o para sabotajes industriales. Como va dirigido contra infraestructuras críticas que no utilizan Internet, se supone que el troyano se introduce en los ordenadores a través de lápices de memoria tipo USB y luego se multiplica a sí mismo, pasando de un ordenador a otro, recogiendo información y dañando tanto sitios web como sistemas operativos (Robles Carrillo, supra nota 15, pp. 437-439).

[34] Gill y Ducheine, supra nota 24, p. 471.

[35] El autor aplica las distintas teorías elaboradas doctrinalmente a esos efectos (Weissbrodt, supra nota 16, pp. 377-378).

perfectamente equiparables a los propios del empleo de la fuerza cinética. En cambio, cuando se trata del uso combinado, esa calificación es automática por tratarse de un componente del dispositivo de la operación. En el caso del uso paralelo, la opción es reconducir esa acción al ámbito del Derecho internacional de los conflictos armados y proceder a su calificación en ese contexto. Como advierte Das, "existe una necesidad clara de analizar la naturaleza de estos ataques a la luz del debate sobre uso de la fuerza[36]". Esa necesidad no parece estar obteniendo la respuesta deseada en el contexto político.

III. EL CONTEXTO POLITICO

Con carácter general, la cooperación internacional sobre el ciberespacio se caracteriza por tres datos principales: (a) el avance inexorable de la tecnología que obliga a adoptar decisiones de esta naturaleza que pueden condicionar a priori el debate de fondo; (b) la dificultad de alcanzar un acuerdo político dadas las diferencias de criterio de los Estados que están motivadas no sólo por factores socio-políticos o económicos, sino también lógicamente tecnológicos; y (c) la necesidad cada vez más acuciante de proceder a una cierta organización jurídica del ciberespacio.

La gobernanza tecnológica sigue una evolución y unas coordenadas que la distancian claramente de las otras dimensiones. Sin estar exenta de polémica, como demuestran las posiciones mantenidas por Rusia y China con el apoyo de un buen número de países en el marco de la UIT frente a EE.UU., mantiene por ahora una dinámica propia impuesta por el propio progreso tecnológico y por sus implicaciones económicas.[37] El contraste entre ese avance en lo tecnológico y la relativa parálisis en lo político no es positivo.

---

[36] En su opinión, "Ataques como los de Estonia y Georgia, o el uso del virus Stuxnet en el programa nuclear iraní, son buenos ejemplos de este enfoque. En Estonia y Georgia, los sistemas informáticos en el Parlamento, hospitales, sistemas de llamada de emergencia, bancos y otros objetivos se vieron obligados a ser apagados. El virus Stuxnet, que se utiliza en el programa nuclear iraní, infectó cientos de ordenadores en los principales sistemas operativos de las instalaciones nucleares de Natanz y Bushehr obligándolos a cerrar temporalmente. Ambos ataques cibernéticos muestran que las operaciones que no causan daño físico, sino simplemente impiden el uso de los sistemas afectados, pueden ser tan perjudiciales como las que causan la destrucción" (Das, supra, nota 1, p. 135).

[37] Pueden verse, al respecto, L. Pigoni, "Internet Governance: Time for an Update", CSS Analyses in Security Policy, Nº 163 (2014), pp. 1-4; P.A. Yannakogeorgos, "Internet Governance and National Security", Strategic Studies Quarterly (2012), pp. 102-125; L.G. Krueger, "Internet Governance and the Domain Name System: Issues for Congress", CRS Report for Congress (2013), pp. 1-23.

Las disensiones entre los Estados son el resultado, básicamente, de dos variables. Por una parte, las propias diferencias de desarrollo que, sin ser una novedad, se extreman como consecuencia del cambio que imponen las TICs en el camino hacia la sociedad y la economía del conocimiento. Por esa impronta globalizadora, la llamada brecha digital es mucho más que un problema coyuntural con la agravante de que ahora no es sólo un debate interestatal en la medida en que la industria y las empresas, por razones económicas o de otra índole, participan en ese debate con una capacidad de influencia hasta ahora desconocida. Junto a ello, en el plano socio-político, se identifican tres cosmovisiones básicas y distintas de la ciberseguridad: la ciberliberal defensiva representada por la UE y los países europeos, la ciberliberal ofensiva abanderada por EE.UU. y la cibernacionalista-aislacionista de Rusia y China.[38] Una conciliación entre esas concepciones, en particular, entre Rusia y EE.UU., se adivina difícil por la filosofía de base que preside su acercamiento al ciberespacio.[39] Tampoco resulta fácil en el caso de China.[40]

En el plano jurídico, la cooperación internacional está evolucionado hacia un punto de consenso desde dos posiciones iniciales, enfrentadas a favor y en contra de la creación de un régimen jurídico específico para el ciberespacio y lideradas, respectivamente, de un lado, por Rusia y

---

[38] E. Sánchez de Rojas Díaz, "Cooperación internacional en temas de ciberseguridad", en Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario (Madrid: Ministerio de Defensa, 2013), p. 262.

[39] Entre otros motivos, ello se debe a que "Según los expertos rusos, los términos estadounidenses de seguridad cibernética y el ciberespacio son principalmente tecnológicos, mientras que los términos rusos para "seguridad de la información" y "espacio de información" son considerados como con significados filosóficos y políticos más amplios. La tecnología se percibe como uno de los muchos componentes en la comprensión de Rusia de seguridad de la información y no se considera que sea la más importante. La Doctrina de Seguridad de la Información de la Federación Rusa, por ejemplo, no menciona ni una sola vez la palabra Internet. Los objetivos declarados por Rusia para su concepto de información son la protección de los conocimientos y la cultura de la nación, y que garantice la libre circulación de la información. Por supuesto, esta última afirmación ha sido controvertida por los críticos del Kremlin en el país y en el extranjero que creen que su concepto de información está diseñado realmente para silenciar a ciertos críticos del gobierno. Este aspecto político complica la toma de decisiones para los funcionarios estadounidenses que temen la censura interna por trabajar con Rusia para mejorar la colaboración en torno a la ciberseguridad. Las principales prioridades de la política de seguridad cibernética de EE.UU. son salvaguardar tecnologías domésticas de las interrupciones, el acceso no autorizado, o cualquier otro tipo de interferencia, destacando así los aspectos tecnológicos de la seguridad cibernética. En general, EE.UU. Unidos se centra mucho más en un enfoque de aplicación de la legislación nacional, mientras que Rusia prefiere añadir un objetivo adicional de establecer regímenes internacionales" (F.-S. Gady y G. Austin, Russia, The United States, And Cyber Diplomacy. Opening the Doors (Nueva York: The EastWest Institute, 2010), p. 5.
http://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf.

[40] Jun y et ali, supra nota 4, p. 20.

China y, de otro, por EE.UU. y el Reino Unido. En la práctica se ha llegado a un cierto acuerdo sobre dos principios básicos: la aplicación del derecho internacional en vigor, en particular, los principios contenidos en la Carta de Naciones Unidas, y la adopción progresiva de las normas específicas necesarias atendiendo a la singularidad del ciberespacio.

En ese contexto, curiosamente, la rotundidad con la que se afirma la vigencia de la soberanía o de los principios de igualdad, no intervención en los asuntos internos o arreglo pacífico de controversias, no se reproduce cuando se trata de la prohibición del uso o de la amenaza de la fuerza, a pesar de ser, por pura lógica, un principio esencial en la garantía de la seguridad y, por ende, de la ciberseguridad. La prueba de ello se encuentra en los trabajos de la Asamblea General de Naciones Unidas en tres contextos complementarios, aunque diferentes: las observaciones remitidas por los Estados, las propuestas conjuntas y los informes de los Grupos de Expertos Gubernamentales.

A. Las observaciones de los Estados

En la resolución 53/70 sobre "Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional", del 4 de enero de 1999, la AGNU invita a todos los Estados miembros a que hagan llegar al Secretario General sus opiniones y observaciones sobre esa cuestión.[41] El análisis de la práctica muestra que, a diferencia de lo que ocurre con otros principios o conceptos, las referencias concretas al principio de prohibición del uso o de la amenaza de la fuerza o a las TICs, como arma susceptible de contrariar esa prescripción, son realmente escasas y están motivadas más por la interpretación global que de ese principio hace el Estado en cuestión, que por la voluntad de concretar su aplicación en el ciberespacio.

La prohibición del uso y de la amenaza de la fuerza no aparece en todos los comentarios, ni siquiera merece una mención expresa en la mayoría de ellos. Hay un primer grupo de países que simplemente

[41] La AGNU solicita los comentarios de los Estados sobre: "a) Evaluación general de los problemas de la seguridad de la información; b) Determinación de criterios básicos relacionados con la seguridad de la información, en particular la injerencia no autorizada o la utilización ilícita de los sistemas de información y de telecomunicaciones y de los recursos de información; c) Conveniencia de elaborar principios internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información"(A/RES/53/70, 4 de enero de 1999, p. 2).

mencionan este principio y la obligación de respetarlo. Así, China se limita a considerar que las TICs deben regirse por el derecho internacional y por las normas de la Carta de Naciones Unidas[42]. Para la República Islámica de Irán, el derecho internacional es aplicable a las TICs y, en consecuencia, los Estados deben respetar los propósitos y principios de las Naciones Unidas y sus obligaciones con arreglo a su Carta y, en particular, el artículo 2.3, la prohibición contemplada en el artículo 2.4 de recurrir a la amenaza o al uso de la fuerza en cualquier forma incompatible con los propósitos de las Naciones Unidas; y la prohibición establecida en el artículo 2.7 de la intervención e interferencia en los asuntos internos de los Estados.[43] Australia entiende, asimismo, que son aplicables algunos de los actuales principios jurídicos internacionales y, entre ellos, los principios de igualdad soberana de los Estados y la prohibición del uso de la fuerza y los actos de agresión, así como el derecho internacional humanitario. No obstante, considera necesario proseguir el debate para determinar con mayor precisión el alcance y la aplicabilidad de estos principios a las amenazas que emanan del ámbito del ciberespacio.[44]

Un segundo grupo de países identifica el problema del arma o de la guerra cibernética. Qatar propone que la ONU debe continuar "dirigiendo el debate y aclarar las cuestiones en relación con el uso de la información y la tecnología de la comunicación alámbrica e inalámbrica en la guerra electrónica y determinar si los principios de derecho internacional existentes son suficientes para asegurar un marco adecuado para definir el comportamiento apropiado en línea ante actos de agresión."[45] En sus comentarios, Alemania se suele ocupar de los aspectos militares de la seguridad cibernética aludiendo a los cambios en sus fuerzas armadas, así como a la defensa del espacio cibernético de la OTAN y al papel de la OSCE.[46] Sin embargo, en 2015, reconoce que,

---

[42] A/62/98, 2 de julio de 2007, p. 8.

[43] Sobre la posible vulneración del principio de no intervención mediante un ciberataque, véase Hathaway, supra nota 14, p. 843.

[44] A/66/152, 15 de julio de 2011, p. 11.

[45] A/65/154, 20 de julio de 2010, p. 11.

[46] A/66/152, 15 de julio de 2011, pp. 4-6. Posteriormente, Alemania comenta que "Los días 27 y 28 de junio de 2013, la tercera Conferencia Cibernética de Berlín, centrada en el tema de Asegurar la libertad y la estabilidad del ciberespacio: el papel y la importancia del derecho internacional y organizada por la Oficina Federal de Relaciones Exteriores en estrecha cooperación con la Universidad de Potsdam, trató de ofrecer evaluaciones jurídicas internacionales de operaciones cibernéticas que no traspasan el umbral de ataque armado y que por tanto no vulneran el derecho sobre conflictos armados. De acuerdo con las normas y los principios internacionales vigentes, los

aunque por el momento no parece probable que se desate una guerra cibernética en toda regla, "el uso limitado de las capacidades cibernéticas como parte de una empresa bélica más amplia, incluso en el contexto de conflictos híbridos, ya es una realidad" y, además, "los incidentes que ocurren en el ciberespacio pueden acabar en conflictos en el mundo real"[47]. España incluye el uso de Internet como un arma asumiendo, en concreto, "la utilización de Internet como un medio para lanzar ataques contra sistemas informáticos de infraestructuras críticas o contra la propia infraestructura de Internet". Es cierto que se identifican como amenazas que derivan del uso de Internet por parte de organizaciones terroristas y, además, curiosamente se refiere al caso de Estonia en este contexto y en el marco de la delincuencia común.[48] En 2015, España insiste en que los Estados deben seguir reflexionando sobre cómo interpretar y aplicar los principios y normas del derecho internacional en el ciberespacio y, entre ellos, los relativos a la amenaza o uso de la fuerza.[49]. Por su parte, Cuba se refiere reiteradamente al uso hostil de las telecomunicaciones, pero, en general, situándolas en el contexto de sus relaciones con EE.UU.[50]

Para cerrar este punto, Rusia y EE.UU. merecen un capítulo aparte porque, en ambos casos, el uso de la fuerza es objeto de una especial atención. Desde sus primeros comentarios, Rusia alerta sobre el hecho de que "resulta particularmente peligrosa la utilización del arma de la información contra objetivos militares y civiles y los sistemas e instituciones de un Estado, el trastorno de cuyo funcionamiento normal

---

Estados son responsables de las acciones de quienes dentro de su esfera de control perjudiquen a la seguridad y estabilidad de las tecnologías de la información y las comunicaciones" (A/68/156/Add.1, 9 de septiembre de 2013, p. 10).

[47] A/70/172, 22 de julio de 2015, p. 2.

[48] A/68/156, 16 de julio de 2013, p. 4.

[49] A/70/172, 22 de julio de 2015, p. 8.

[50] Cuba sostiene que "el uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una violación de las normas internacionalmente reconocidas en esta materia y una manifestación negativa e irresponsable del empleo de esos medios, cuyos efectos pueden generar tensiones y situaciones desfavorables para la paz y la seguridad internacionales, y socavar así los principios y propósitos consagrados en la Carta de las Naciones Unidas". En su opinión, los sistemas de información y telecomunicaciones pueden convertirse en armas "cuando se diseñan y/o emplean para causar daños a la infraestructura de un Estado y, como consecuencia, pueden poner en riesgo la seguridad y la paz internacionales" (A/65/154, 20 de julio de 2010, p. 2).

pone en peligro directamente la seguridad nacional."[51] Hay tres aspectos destacables en su argumentación.

En primer lugar, Rusia constata que entre las principales orientaciones de las estrategias de defensa de los Estados se encuentra la adquisición de un poderío en materia de información. Esas nuevas estrategias se benefician de una doble circunstancia: por una parte, el desarrollo de esas nuevas tecnologías no suscita en la opinión pública la misma reacción negativa que provocan las armas corrientes; y, por otra parte, suelen ser más compatibles con el concepto de tecnologías de doble uso para fines tanto militares, como civiles y comerciales. Lógicamente, también, entiende que esos presupuestos obligan a revisar los conceptos tradicionales de la amenaza a la soberanía nacional y la observancia del derecho internacional.

En segundo término, Rusia identifica la guerra estratégica de información como una nueva categoría de conflicto que, por las propias características del arma de la información, puede resultar más operativa, pero ser percibida de un modo menos negativo o, incluso, positivo, como si tuviese un carácter meramente humanitario.

Para terminar, desde el punto de vista de la seguridad internacional, Rusia entiende que esa situación puede encerrar dos peligros principales: por una parte, la posibilidad de una carrera de armamentos en el plano tecnológico que "podría revertir a las condiciones características del período de la guerra fría" en materia de control de armamentos; y, por otra, el hecho de que "la conjugación del poderío económico y el poderío en materia de información permite ejercer una influencia efectiva en la evolución de la política internacional sin tener que recurrir a los medios tradicionales y 'burdos' de coerción basados en la utilización de la fuerza armada."[52] El reconocimiento del valor de la fuerza cibernética es paralelo a la asunción de los límites y carencias, comparativamente, de la fuerza cinética.

EE.UU. también parte de la asunción de las singularidades del arma tecnológica[53], que invalidan las estrategias tradicionales para el control

[51] Rusia dedica un apartado especial a la "Formulación y adopción por los Estados de planes o doctrinas que incluyan la posibilidad de hacer la guerra en el campo de la información y puedan provocar una carrera de armamentos y generar tensiones en las relaciones entre los Estados y conducir a guerras de información per se" (A/56/164/Add.1, 3 de octubre de 2001, p. 5).

[52] A/56/164/Add.1, 3 de octubre de 2001, p. 5.

[53] En su opinión, las armas cibernéticas son furtivas e invisibles, con un alcance amplio e indeterminable, anónimas en cuanto al origen, la identidad y el patrocinio del autor, no son monopolio principal de los gobiernos, están al alcance de todos y su utilización sólo depende de la

de armas y obligan a adoptar enfoques más creativos para prevenir y mitigar los riesgos. No obstante, después de haber constatado ese cambio de parámetros, este país defiende la aplicación de los principios vigentes de derecho internacional y, en concreto, el jus ad bellum y el jus in bello[54].

Sobre el jus ad bellum, EE.UU. cita las tres disposiciones relevantes de la Carta: el artículo 2.4, el artículo 39 y el artículo 51. El caso es que reconoce la dificultad de calificar una actividad perjudicial en el ciberespacio como ataque armado[55], pero no considera necesario establecer un nuevo marco jurídico específico para el ciberespacio porque, en su opinión, es un problema más de interpretación de los que resultan normalmente de la aplicación de la Carta. A pesar de ello, como en determinadas circunstancias, una actividad ciberespacial puede constituir un ataque armado, defiende la aplicación de los siguientes principios: a) El derecho a la legítima defensa contra un ataque armado inminente o en curso se aplica si el atacante es un agente estatal o un agente no estatal; b) El uso de la fuerza en legítima defensa debe limitarse a lo necesario para hacer frente a un ataque armado inminente o en curso y debe ser proporcional a la amenaza que se plantea; c) Los Estados están obligados a adoptar todas las medidas necesarias para garantizar que sus territorios no sean utilizados por otros Estados o actores no estatales a los efectos de actividades armadas, lo que incluye planificación, amenaza, comisión o prestación de apoyo material para ataques armados contra otros Estados y sus intereses.[56]

En definitiva, EE.UU. extiende su propia doctrina sobre el uso de la fuerza con la cobertura jurídica de que se trata de la aplicación de los

---

motivación del usuario, además de que pueden ser de índole civil, militar o ambas (A/66/152, 15 de julio de 2011, p. 15).

[54] En el caso del jus in bello, EE.UU. considera que los principios fundamentales del derecho aplicable a los conflictos armados "contribuirían considerablemente a la hora de juzgar la legalidad de los ataques cibernéticos durante un conflicto armado". Entre ellos cita el principio de distinción, la prohibición de ataques indiscriminados y el principio de proporcionalidad. En su opinión, en el caso de ataques con utilización de las TICs se debería operar del mismo modo que se ha hecho con los ataques con armas cinéticas convencionales y estratégicas (A/66/152, 15 de julio de 2011, p. 17).

[55] Así, por ejemplo, cuando se desconoce al autor de la amenaza y el motivo, y los efectos no causan directamente la muerte o una destrucción física importante, es posible que se llegue a conclusiones divergentes a la hora de determinar si se ha producido un ataque armado (Ibíd., p. 16).

[56] Como indica Lotrionte, "Mientras que EE.UU. ha afirmado en un informe a las Naciones Unidas que 'en determinadas circunstancias una actividad perjudicial en el ciberespacio podría constituir un ataque armado,' no ha indicado qué tipo de actividades disruptivas se calificarían como tal" (Lotrionte, supra nota 5, p. 14).

principios de la Carta y no, como es en realidad, de la aplicación de su propia interpretación de los principios de la Carta[57]. No es, desde luego, una propuesta para adaptar la prohibición del uso y de la amenaza de la fuerza a las particularidades del ciberespacio.

B. Las propuestas conjuntas

Rusia y China han liderado dos propuestas conjuntas ante la AGNU con escasas referencias al principio del artículo 2.4 de la Carta. La primera se encuentra en una carta, fechada el 12 de septiembre de 2011, en la que China, Rusia, Tayikistán y Uzbekistán presentan una propuesta de resolución conteniendo un código internacional de conducta para la seguridad de la información[58]. La primera medida es cumplir con la Carta de las Naciones Unidas y las normas reconocidas universalmente que rigen las relaciones internacionales concretando algunas de ellas entre las que no se menciona expresamente el uso o amenaza de la fuerza. En segundo término, se recoge el compromiso de no utilizar las TICs para realizar actividades hostiles o actos de agresión, plantear amenazas a la paz y la seguridad internacionales, ni contribuir a la proliferación de armas informáticas o tecnologías conexas. Finalmente, en la última previsión se incluye "resolver por medios pacíficos toda controversia resultante de la aplicación del código y abstenerse de la amenaza o el uso de la fuerza".

Cuatro años después, incorporando a Kazajstán y Kirguistán, se presenta la versión revisada del código de conducta[59]. La segunda medida consiste ahora de forma más genérica en "no utilizar las tecnologías de la información y las comunicaciones ni las redes de la información y las comunicaciones para realizar actividades que se opongan a la tarea de mantener la paz y la seguridad internacionales". La tercera se dedica al principio de no intervención en los asuntos internos. Para terminar, se reproduce la misma y escueta fórmula de la propuesta anterior en relación con el uso o la amenaza de la fuerza.

---

[57] A/66/152, 15 de julio de 2011, pp. 16-17.

[58] Abierto a todos los Estados y voluntario, el propósito del código es determinar los derechos y responsabilidades de los países en el espacio de la información, promover su desempeño constructivo y responsable y fomentar su cooperación para hacer frente a las amenazas y los problemas comunes en el espacio informático, a fin de garantizar que las TICs se utilicen exclusivamente en favor del desarrollo social y económico y el bienestar de la población con el objetivo de mantener la estabilidad y la seguridad internacionales (A/66/359, 14 de septiembre de 2011, pp. 3-5).

[59] A/69/723, 13 de enero de 2015, pp. 3-6.

El motivo de esta escasa atención al principio del artículo 2.4 puede ser tanto la falta de acuerdo entre ambos países sobre una propuesta en ese sentido, como la intención de no entorpecer la posible adhesión de otros Estados a su proyecto de código con un principio controvertido en su alcance y excepciones. El hecho de que se trata de una norma que encierra mayores problemas que los demás se pone de manifiesto, asimismo, en los informes de los grupos de trabajo creados a petición de la AGNU.

C. Los informes de los grupos de expertos gubernamentales

Los informes de los Grupos de Expertos Gubernamentales (GEG) permiten apreciar la progresiva formación de un consenso sobre el régimen jurídico del ciberespacio.[60] Al fracaso del primer grupo incapaz de concluir un informe en 2004, sigue el acuerdo de mínimos del informe del siguiente grupo en 2010 centrado en las amenazas y las medidas de cooperación y es, finalmente, el informe de 2013 el que establece tres premisas básicas: primera, la aplicación de normas derivadas del derecho internacional vigente que son pertinentes para el uso de las TICs; segunda, la necesidad de seguir avanzando para establecer un entendimiento común sobre cómo se aplicarán esas normas al ciberespacio; y tercera, la posibilidad de elaborar normas adicionales con el transcurso del tiempo si son necesarias atendiendo a las singulares características de las TICs. En ese contexto se asumen dos ideas principales: por una parte, que el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías; y, junto a ello, que la soberanía de los Estados y las normas y principios internacionales que de ella emanan son aplicables a la realización de actividades relacionadas con las TICs.[61]

El informe del GEG emitido en 2015 reconoce, entre las amenazas reales y potenciales, el hecho de que varios Estados están desarrollando capacidades en materia de TICs con fines militares aumentando, en consecuencia, las probabilidades de futuros conflictos mediante el uso de esas tecnologías.[62] Tras una extensa relación de medidas de

[60] Sobre esos trabajos, puede verse Lewis, supra nota 5, pp. 11-13.
[61] A/68/98, 24 de junio de 2013, pp. 8-9.
[62] A/70/174, 22 de julio de 2015, p. 8.

desarrollo en la línea de los acuerdos alcanzados en 2013, en la parte del informe relativa a la aplicación del derecho internacional vigente al uso de las TICs, el GEG "señala la importancia fundamental de los compromisos" de los Estados recogidos en la Carta y, entre ellos, la prohibición del uso y de la amenaza de la fuerza. No obstante, al ofrecer sus opiniones, recordando que no son exhaustivas, sobre la forma de aplicar el derecho internacional a las TICs, sólo menciona expresamente en un apartado la soberanía, la igualdad soberana, la solución pacífica de controversias y la no intervención en los asuntos internos de los Estados, junto con el respeto de los derechos y libertades fundamentales. Y es, a continuación, en un párrafo distinto y con un tenor también diferente, donde el GEG, "subrayando las aspiraciones de la comunidad internacional de lograr el uso de las TICs con fines pacíficos para el bien común de la humanidad y recordando que la Carta se aplica en su totalidad, manifiesta que los Estados tienen el derecho inmanente de adoptar medidas compatibles con el derecho internacional como se reconoce en la Carta."[63] Conectado con lo anterior, parece estar referido al ejercicio de la legítima defensa que es una cuestión objeto de amplia controversia como excepción al uso de la fuerza.

Las observaciones individuales de los Estados, las propuestas conjuntas y los informes consensuados por los GEG permiten llegar a la conclusión de que, más allá de la referencia genérica a la aplicación del derecho en vigor, no hay realmente un consenso definido sobre la gestión del principio de prohibición del uso y de la amenaza de la fuerza en el ciberespacio[64]. Es una tarea compleja por varios motivos que alientan el discurso político y jurídico.

IV. EL DISCURSO JURIDICO

Desde la aprobación de la Carta de Naciones Unidas, la prohibición del uso y de la amenaza de la fuerza es un componente básico del sistema de seguridad colectiva de la ONU y se convierte, asimismo, en un principio estructural del modelo de organización internacional. Durante mucho tiempo, sin embargo, "el hecho de que la guerra continúe a pesar de las normas de la Carta es usado frecuentemente para ilustrar la debilidad o incluso la ingenuidad de la ambición por regular la guerra a

[63] Ibíd., p. 16.
[64] Lewis, supra nota 5, pp. 11-12.

través de un instrumento legal interestatal."[65] Ha sido, incluso, un argumento utilizado recurrentemente para cuestionar la eficacia y la validez mismas del derecho internacional. La trayectoria de este principio muestra la falta de coincidencia entre las interpretaciones político-institucionales, jurídicas y académicas, incluso éstas a veces sólo buscan respaldar aquéllas.[66] Un brevísimo repaso de las mismas es un paso previo necesario para la comprensión de este principio en el ciberespacio.

A. La interpretación político-institucional

La interpretación de la prohibición del uso y de la amenaza de la fuerza en sede política tiene protagonistas conocidos y momentos fijados en la memoria colectiva. No han sido pocas las situaciones que han puesto a prueba el respeto de dicho principio. Por diversas razones, destacan Kosovo en 1999 donde se alega la necesidad de remediar una crisis humanitaria;[67] Afganistán en 2001 defendido como un ejercicio de legítima defensa frente a un ataque inminente procedente de actores no estatales; Irak en 2003 cuando se discute más sobre el alcance de las resoluciones del Consejo de Seguridad que sobre el hecho mismo de haber usado la fuerza sin cobertura jurídica; o, finalmente, el complejo entramado de Siria en 2015. En este caso, además de las acciones de la Coalición de Estados, está la intervención de Rusia a petición del gobierno sirio o las medidas adoptadas por Francia tras el viernes 13-N

---

[65] I. Hurd, "Permissive Law on the International Use of Force", en The Use of Armed Force: Are We Approaching Normative Collapse? ASIL Proceedings 2015, p. 10.

[66] Ruys explica que "desde un punto de vista normativo, puede haber una actitud más crítica por parte de la doctrina jurídica europea hacia las pretensiones expansionistas sobre el recurso admisible a la fuerza y una mayor conciencia de la posibilidad de abuso –una conciencia, cabría decir, de que los precedentes que creamos hoy pueden ser usados contra nosotros mañana (tal como ilustra ampliamente la crisis ucraniana). Por el contrario, una serie de académicos estadounidenses parecen estar concentrados principalmente en la justificación de las acciones de Estados Unidos frente a la comunidad internacional en general y por proporcionar los argumentos teóricos para sustentar legalmente estas acciones" (T. Ruys, "Divergent Views on The Chapter Norms on the Use of Force – A Transatlantic Divide?, en The Use of Armed Force: Are We Approaching Normative Collapse?,ASIL Proceedings 2015, p. 14).

[67] Siguiendo a Wood, "El Gobierno británico dijo entonces que "no hay ninguna doctrina general de intervención humanitaria en el derecho internacional", pero que habían surgido casos en los que "un uso limitado de la fuerza estaba justificado… cuando este era el único medio para evitar una catástrofe humanitaria inmediata y abrumadora. En 2013, sin embargo, en el contexto de un posible uso de la fuerza contra el régimen sirio después de su uso de armas químicas, el Reino Unido se refirió a "la doctrina de la intervención humanitaria'" (M. Wood, The Use of Force in 2015 With Particular Reference to Syria,Hebrew University of Jerusalem Legal Studies Research Paper, Serie Nº 16-05 (2015), p. 4).

y seguidas por otros Estados en su lucha contra el autodenominado Estado Islámico. La intervención por invitación, el derecho de legítima defensa, individual o colectiva, la legítima defensa preventiva o la doctrina unable and unwilling han sido argumentos utilizados por separado o combinados para justificar el uso de la fuerza.[68] El balance es una larga secuencia de diversas acciones individuales o, incluso grupales, pero ni globalmente colectivas ni consensuadas en el marco institucional, que ponen a prueba la efectividad del principio de prohibición del uso de la fuerza y del sistema de seguridad colectiva de Naciones Unidas.

La necesidad de una interpretación institucional y colectiva para abordar el uso de la fuerza y, en general, el nuevo contexto de seguridad del siglo XXI, justifica diversas iniciativas y, entre ellas, la constitución del Grupo de Alto Nivel sobre las amenazas, los desafíos y el cambio, creado por el Secretario General de Naciones Unidas (SGNU) a raíz de su discurso en 2003 en la AGNU. En su informe "Un mundo más seguro: la responsabilidad que compartimos"[69], se afirma que "La fuerza militar, utilizada legítima y debidamente, es un componente esencial de cualquier sistema viable de seguridad colectiva". Aunque reconoce que hay pocas cuestiones que susciten más dificultades, el mantenimiento de la paz y la seguridad internacionales "depende en gran medida de que haya aceptación y un concepto común en el mundo de cuándo es legal y legítimo utilizar la fuerza"[70]. Con esa intención, el Informe identifica los cinco criterios básicos de legitimidad que debe tener en cuenta el Consejo de Seguridad al autorizar el uso de la fuerza –gravedad de la amenaza, propósito correcto, último recurso, proporcionalidad de los medios y balance de las consecuencias– [71] y

[68] T. Ruys y L. Ferro, "Divergent Views on the Content and Relevance of the Jus ad Bellum in Europe and the United States? The case of the U.S-led military coalition against 'Islamic state'", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2731597.

[69] En ese Informe asumen que el desafío central del siglo XXI es plasmar un concepto nuevo y más amplio de seguridad colectiva, confirmando el protagonismo de los Estados y basado en tres pilares: el primero es que las amenazas actuales no respetan las fronteras nacionales, están interrelacionadas y deben abordarse desde los planos mundial, regional y nacional; el segundo es que ningún Estado es invulnerable frente a las amenazas actuales; y el tercero es que no se puede suponer que todos los Estados podrán o querrán siempre cumplir con su deber de proteger a su propia población y no causar daño a sus vecinos (A/59/565, 2 de diciembre de 2004, p. 11).

[70] Ibíd.

[71] El Consejo de Seguridad, al debatir si ha de autorizar o aprobar el uso de la fuerza militar, debe tener siempre en cuenta, además de cualesquiera otras consideraciones, por lo menos los cinco criterios básicos de legitimidad que se indican a continuación: a) Gravedad de la amenaza. La amenaza de daño a la seguridad del Estado o del ser humano, ¿es de índole tal y es suficientemente clara y grave como para justificar a primera vista el uso de la fuerza militar? En el

trata, asimismo, de dar respuestas a tres cuestiones particularmente más complejas: 1) El derecho a recurrir a la fuerza a título preventivo, en legítima defensa, ante una amenaza que no es inminente, respecto del cual no se manifiestan partidarios de modificar el texto ni la interpretación del artículo 51;[72] 2) La amenaza externa, real o posible, de un Estado a otros Estados o pueblos más allá de sus fronteras, que es una situación que, a juicio del Grupo, tampoco ha de justificar un uso de la fuerza individual;[73] 3) La amenaza de índole primordialmente interna para la propia población de un Estado respecto de la que hay que esperar una autorización del Consejo de Seguridad.[74]

El Informe del SGNU también advierte que el núcleo del consenso ha de ser cuándo y cómo se puede hacer uso de la fuerza para defender la paz y la seguridad internacionales. Las tres modalidades controvertidas son el uso anticipatorio, el uso preventivo y el uso proactivo para la protección frente a graves violaciones de derechos humanos.[75] Siendo polémicas en el mundo físico, suscitan un debate incluso más intenso en el ciberespacio. Como advierte Melzer, "la velocidad, impredecibilidad y

---

caso de las amenazas internas, reales o que se consideren inminentes, ¿entrañan genocidio u otras matanzas en gran escala, actos de depuración étnica o infracciones graves del derecho internacional humanitario? b) Propósito correcto. ¿Queda de manifiesto que el objetivo primordial de la acción militar que se propone consiste en poner fin a la amenaza o evitarla, cualesquiera que sean los demás motivos o propósitos que estén en juego? c) Último recurso. ¿Se han considerado todas las demás opciones no militares para hacer frente a la amenaza y hay fundamentos razonables para creer que no arrojarán resultados? d) Proporcionalidad de los medios. La escala, la duración y la intensidad de la acción militar que se propone ¿constituyen el mínimo necesario para hacer frente a la amenaza? e) Balance de las consecuencias. ¿Hay posibilidades razonables de que la acción militar logre hacer desaparecer la amenaza sin que sus consecuencias sean peores que las de no hacer nada? (Ibíd., p. 64).

[72] Según el Informe, si existen buenos argumentos para una acción militar preventiva y buenas pruebas que los corroboren, hay que presentarlos al Consejo de Seguridad que puede autorizar esa acción si decide hacerlo. Si el Consejo de Seguridad decide no hacerlo, habrá tiempo para estudiar otras estrategias previas a la opción militar como la persuasión, la negociación, la disuasión y la contención. En su opinión, el riesgo para el orden mundial es demasiado grande como para aceptar la legitimidad de la acción preventiva unilateral, en contraposición a la aprobada colectivamente. Dejar que uno lo haga es dejar que lo hagan todos" (Ibíd., p 61).

[73] Como reza el Informe, a pesar de la desconfianza que pueda generar su propia práctica o su proceso de adopción de decisiones, el Consejo de Seguridad es el único legitimado sobre la base del Capítulo VII para actuar si hay pruebas verosímiles del carácter real de la amenaza y si la respuesta militar es la única razonable. En su opinión, "la tarea no consiste en encontrar alternativas al Consejo de Seguridad como fuente de autoridad sino en hacer que funcione mejor que hasta ahora" (Ibíd., p. 64).

[74] A pesar de la previsión del artículo 2.7 de la Carta y de que hasta ahora su práctica no ha sido sistemática ni eficaz, sobre la base de los poderes reconocidos en el Capítulo VII y en cumplimiento de la obligación colectiva de proteger, el Consejo de Seguridad puede autorizar una intervención militar como último recurso en caso de genocidio y otras matanzas en gran escala, de depuración étnica o de graves infracciones del derecho internacional humanitario que un gobierno soberano no haya podido o no haya querido prevenir (Ibíd., p. 63).

[75] A/59/2005, 21 de marzo de 2005, p. 36.

naturaleza clandestina de la mayoría de las operaciones cibernéticas dificultan la capacidad de defensa de un Estado para reaccionar a tiempo para detectar y prevenir o repeler un ataque inminente o en marcha, el cual bien puede ser diseñado y programado para producir sus efectos dañinos meses después de la intrusión del agresor. En la práctica, la ciberdefensa debe confiar en sistemas automatizados, que hacen que un examen y verificación humana, caso por caso, tanto de la identidad del agresor, como de la necesidad y proporcionalidad de una acción de legítima defensa sean extremadamente difíciles de ser llevados a cabo."[76]

La Cumbre Mundial de 2005 no supone un avance en la solución de la problemática del uso de la fuerza, sino la evidencia de que no se ha llegado a un acuerdo sobre las modalidades de uso objeto de controversia. Además de reiterar la obligación contenida en el artículo 2.4, hay dos afirmaciones ilustrativas en ese sentido: la primera es que las disposiciones pertinentes de la Carta son suficientes para hacer frente a toda la gama de amenazas a la paz y la seguridad internacionales; y la segunda es la autoridad y la competencia del Consejo de Seguridad para imponer medidas coercitivas con el fin de mantener y restablecer la paz y la seguridad internacionales.[77]

En realidad, la ausencia de un pronunciamiento sobre la legalidad o ilicitud de esas modalidades de uso –anticipatorio, preventivo y proactivo– es la prueba de la falta de consenso sobre esta cuestión. Sin embargo, esa ausencia no supone en este caso un obstáculo para aquellos usos, sino que puede y, de hecho, está siendo interpretada como una aceptación o, al menos, una no desautorización de tales prácticas que, en realidad, difícilmente pueden conciliarse con el contenido jurídico de la prohibición del uso y de la amenaza de la fuerza.[78] Los avatares de este principio en sede política se multiplican con la interpretación jurisprudencial y su revalorización en el marco doctrinal.

B. La interpretación jurídica y académica

[76] N. Melzer, Cyberwarfare and International Law, UNIDIR Resources, 2011, p. 187.
[77] A/RES/60/1, 24 de octubre de 2005, pp. 23-24.
[78] Matt Salmon sostiene que "De hecho, se ha dicho que es precisamente la falta de normas internacionales para responder es lo que ha hecho que las armas cibernéticas se tornen tan atractivas para Rusia, China, Irán y Corea del Norte" (Salmon, supra nota 4, p. 1).

La Corte Internacional de Justicia (CIJ) no ha tenido ocasión de pronunciarse sobre el uso o la amenaza de la fuerza en el plano cibernético, pero sus decisiones en el mundo no virtual[79] pueden trasladarse analógicamente al ciberespacio. Por motivos distintos destacan, a esos efectos, sus decisiones en los asuntos de las actividades militares y paramilitares en Nicaragua y contra Nicaragua (1986), la legalidad de la amenaza o el empleo de armas nucleares (1996), las plataformas petrolíferas (2003) y las consecuencias jurídicas de la construcción de un muro en territorio palestino ocupado (2004).

El asunto Nicaragua aporta tres conclusiones importantes a los efectos de su extrapolación al ciberespacio. La primera es que la CIJ constata la existencia de diferentes modalidades de uso de la fuerza de manera que hay que distinguir entre las formas más graves y otras modalidades menos brutales, porque no todas alcanzan el grado de ataque armado capaz de justificar una respuesta en legítima defensa.[80] La segunda es la equiparación entre las acciones emprendidas por fuerzas armadas regulares a través de una frontera internacional y el envío por parte de un Estado de bandas armadas al territorio de otro Estado cuando realizan operaciones que, por su escala y efectos, habrían sido clasificadas como un ataque armado de haber sido realizada por fuerzas armadas regulares. La tercera es que la CIJ no considera que el concepto de ataque armado incluya la asistencia a rebeldes en forma de suministro de armas o apoyo logístico o de otra índole.[81] La diferenciación entre la mayor o menor gravedad de una acción cibernética plantea mayores dificultades que en el caso de las acciones cinéticas, pero es un criterio lógico de aplicación. Las otras dos aportaciones de la CIJ son, por su parte, especialmente valiosas a efectos de determinar si se ha producido o no una vulneración de la prohibición del uso o de la amenaza de la fuerza en el ámbito ciberespacial que se caracteriza, precisamente, por la abundancia de agentes no estatales que pueden actuar en lugar de los Estados, pero haciendo suyas sus

[79] Entre los estudios doctrinales sobre este principio, los casos y la jurisprudencia, pueden verse T. Franck, Recourse to Force. State Action Against Threats And Armed Attacks (Oxford: Cambridge University Press, 2002); Ch. Gray, International Law and the Use of Force (Oxford: Oxford University Press, 2008, 3ª ed).

[80] Sentencia de 27 de junio de 1986, Rec. 1986, párr. 227-238.

[81] Como ejemplos destacan, entre otros, el apoyo a fuerzas rebeldes de un Estado por medio del suministro de armas o apoyo logístico; un ataque puntual con el lanzamiento de un misil contra un buque mercante o los disparos repetidos hacia un helicóptero militar desde una patrullera; o el sembrado de una mina con la que choca un navío de guerra (Ibíd.).

pretensiones como ocurre con los sustitutos, proxys o mercenarios. En caso de que sus acciones fuesen equiparables a las de las fuerzas cibernéticas regulares de un Estado podrían tener la misma calificación. No sería, en cambio, un ataque armado cuando se trata de asistencia o apoyo logístico, aunque sí podría ser un uso de la fuerza.

La opinión consultiva de la CIJ sobre la legalidad de la amenaza o el empleo de armas nucleares tiene dos elementos relevantes desde la perspectiva de su traslación al ciberespacio: por una parte, la afirmación de la irrelevancia del medio a los fines de determinación de la existencia de una amenaza o uso de la fuerza que sirve para incluir el arma cibernética como un medio posible de uso o amenaza de la fuerza; y, por otra parte, después de recordar las condiciones de ejercicio de la legítima defensa, el reconocimiento de que "en el estado actual del derecho internacional, y teniendo en cuenta los elementos de hecho a su disposición, el Tribunal no puede afirmar de manera definitiva si la amenaza o el uso de armas nucleares sería ilegal o no en una extremada circunstancia de legítima defensa, en la que estuviera en juego la supervivencia misma del Estado."[82] Esa afirmación es perfectamente extrapolable al contexto cibernético donde la respuesta en legítima defensa plantea una problemática propia.[83]

El asunto de las plataformas petrolíferas insiste en la idea de que la legítima defensa es una reacción a una agresión previa de manera que cabe deducir que no admite una dimensión anticipatoria como la pretendida por EE.UU.[84] y que además es igualmente aplicable en el contexto del ciberespacio.

Por último, el asunto de las consecuencias jurídicas de la construcción del muro en territorio palestino ocupado da ocasión a la Corte para rechazar la posibilidad de invocar el derecho a la legítima defensa de los Estados fuera del marco interestatal.[85] Aunque en este caso se trata de excluir su aplicación en los casos de violencia interna, contra atentados terroristas, la práctica de los Estados y la propia doctrina internacionalista se ha apartado claramente de esta

[82] Dictamen de 8 de julio de 1996, Rec. 1996, párr. 37-50 y 49-73.
[83] Melzer, supra nota 74, p. 187; Gill y Duchaine, supra nota 24, pp. 471.
[84] Sentencia de 6 de noviembre de 2003, Rec. 2003, párr. 78.
[85] Según la CIJ, en el artículo 51 se reconoce "la existencia de un derecho inmanente de legítima defensa en caso de ataque armado de un Estado contra otro. Ahora bien, el Estado de Israel no alega que los ataques dirigidos contra él sean imputables a un Estado extranjero". (Dictamen de 9 de julio de 2004, Rec. 2004, párrafos 138-139).

sentencia[86]. A pesar de que, ya entonces, algunos jueces no se muestran conformes con esa interpretación del artículo 51 de la Carta, posteriormente, en el asunto de la República Democrática del Congo contra Uganda, teniendo la posibilidad de hacerlo, la CIJ no ha cambiado de posición y ha eludido alterar su jurisprudencia al respecto.[87]

La jurisprudencia de la CIJ ha sido clara y constante en la definición de los aspectos conceptuales del uso de la fuerza y de la legítima defensa incluido el reconocimiento de su incapacidad para apreciarla en el caso del arma nuclear. Ni el Consejo de Seguridad, ni muchos Estados comulgan con todos sus aspectos, pero los más controvertidos son el alcance de la legítima defensa y su utilización respecto de agentes no estatales. No es extraño, dada la diversidad de pareceres, que la doctrina se muestre dividida, básicamente, en la interpretación de las excepciones a la prohibición del uso o de la amenaza de uso de la fuerza que constituyen un elemento clave para distinguir cuando hay o no uso o amenaza de uso de la fuerza. Doctrinalmente, hay dos posturas completamente opuestas a favor y en contra de la legalidad de las modalidades de legítima defensa que pueden constituir una excepción a la prohibición del uso de la fuerza, esto es, anticipatorio, preventivo y proactivo[88]. Es tan difícil que pueda producirse un acercamiento entre ellas como lo es resolver definitivamente el asunto en sede política.

Michael Glennon reconoce que "las divisiones culturales respecto del uso de la fuerza no separan simplemente el occidente del resto, sino que además separan cada vez más a los Estados Unidos del resto del occidente."[89] Desde ese punto de partida, Ruys y Ferro defienden que "la idea de que todos los abogados internacionalistas europeos son 'restriccionistas' y que todos los académicos estadounidenses son

---

[86] N. Lubell, Extraterritorial Use of Force against Non-State Actors (Nueva York: Oxford University Press, 2010) p. 35.

[87] Ibíd., p. 32.

[88] Aunque con frecuencia se plantea como un discurso que divide a EE.UU. y a los países europeos, Ruys y Ferro consideran que"la brecha también se da en el nivel de los abogados internacionalistas. En particular, en el plano metodológico, parece que hay una mayor adhesión al enfoque positivista tradicional del derecho internacional en el lado europeo, mientras que los académicos estadounidenses parecen más abiertos a otros enfoques metodológicos alternativos y orientados a políticas. Traducido a la esfera del jus ad bellum, los académicos estadounidenses generalmente se adhieren a un enfoque más 'expansionista' (que se centra principalmente en la costumbre y en la práctica de los Estados poderosos), mientras que Europa (así como varios otros académicos no estadounidenses) se adhieren a un enfoque más "restrictivo" (prestar más atención a la opinio juris como elemento constitutivo de la costumbre)" (Ruys y Ferro, supra nota 66, p. 2).

[89] M.J. Glennon, "The UN Security Council in a Unipolar World", Virginia Journal of International Law, Vol. 44 (2003-2004), p. 97.

'expansionistas' es, sin lugar a dudas, una burda tergiversación". Ello es así, a su juicio, por tres motivos: "Primero, cabe recordar que Estados Unidos no ha dado la espalda al marco regulatorio del uso de la fuerza en la Carta de Naciones Unidas, pero ha tratado de articular constantemente justificaciones legales para sus operaciones militares en el exterior a raíz de este marco (…). En segundo lugar, la búsqueda de nuevas excepciones a la prohibición del uso de la fuerza, o de una lectura más flexible de las excepciones existentes no siempre se han originado desde el lado occidental del Atlántico. Por ejemplo, en los últimos años, el Reino Unido ha mostrado ser uno de los más firmes defensores de la legalidad de la autorización unilateral de intervenciones humanitarias sin autorización del Consejo de Seguridad (…). En tercer lugar, en relación con determinados temas controvertidos, tales como, por ejemplo, la legalidad de la legítima defensa anticipatoria, un examen más detallado revela que las posiciones de Estados Unidos y de varios Estados europeos en realidad han llegado a converger en una medida considerable, al igual que las de los académicos del derecho americanos y europeos."[90]

En realidad, sobre esta argumentación, caben algunas observaciones. La primera es que el hecho de que EE.UU. pretenda justificar sus acciones mediante una interpretación de la Carta puede servir tanto para defender que la respeta, como para demostrar que la incumple porque cuando una actuación es claramente conforme a la legalidad no necesita mayores justificaciones teóricas como ha ocurrido cuando se ha contado con la autorización del Consejo de Seguridad[91]. La segunda es que el Reino Unido no se ha caracterizado precisamente por distanciarse de las políticas de EE.UU., ni es representativo de las políticas europeas, razón por la cual identificar su política como un acercamiento con los países europeos resulta poco justificado.[92] En tercer lugar, la idea de que se está produciendo una convergencia general euroatlántica en temas como la legítima defensa anticipada no tiene en cuenta que las acciones individuales de los Estados deben explicarse en el contexto actual, caracterizado por un cambio en el

[90] Ruys y Ferro, supra nota 66, pp. 3-4.
[91] Kolb demuestra que incluso la invocación del famoso asunto Carolina es una conducta propia de los países tradicionalmente más inclinados al uso de la fuerza (R. Kolb, Ius contra bellum. Le droit international relatif au maintien de la paix (Bruselas: Bruylant. 2003), p. 196.
[92] Gray advierte precisamente que muchos países no aceptan esa interpretación amplia de las excepciones al uso de la fuerza (Gray, supra nota 77, pp. 252-253).

origen y la naturaleza de las amenazas, por la ausencia o limitación de los mecanismos existentes para conjurarlas y por una situación de incertidumbre global sobre las mismas. En esta situación, ningún Estado estaría razonablemente dispuesto a pronunciarse en contra o a renunciar al margen de discrecionalidad que resulta de la posibilidad de operar con esas distintas doctrinas que tienen en común servir como excepciones a la prohibición del uso de la fuerza que, para los Estados, es la solución definitiva frente a cualquier amenaza.

El problema de fondo estriba en que el aumento de las excepciones o la interpretación extensiva de las excepciones al principio de prohibición del uso de la fuerza se acaban convirtiendo en la garantía misma del respeto de dicho principio. Es una especie de construcción diabólica porque se entiende que ese principio está siendo respetado en la misma medida en que se articulan doctrinas para crear o ampliar sus excepciones, esto es, para justificar el motivo de su no respeto. Y es fácil cumplir con ese principio si se pueden crear doctrinas ad hoc cuando se pretende incumplirlo. Buscar justificaciones jurídicas o metajurídicas para no cumplir la norma no es, ni puede ser, una garantía de su cumplimiento. Sorprende, por ello, que el principio de prohibición del uso y de la amenaza de uso de la fuerza sea objeto de una revalorización en sede doctrinal. Hace prácticamente una década, el autor del célebre artículo Who Killed Article 2(4)? publicado en 1970[93], Thomas Franck, afirmaba que "el marco normativo establecido por la Carta de Naciones Unidas no se está erosionando. Por el contrario, su legitimidad es defendida bastante consistentemente en la retórica de todos los Estados y la conducta de la mayoría."[94] No es el único.

En un coloquio reciente de la American Society of International Law titulado The Use of Armed Force: Are We Approaching Normative Collapse?, la doctrina se muestra coincidente en apreciar no sólo la vigencia del principio de prohibición del uso y de la amenaza de la fuerza, sino también su contribución al fortalecimiento mismo del Derecho. Según Hurd, "el éxito de la Carta de Naciones Unidas en torno a

[93] Para el autor, "El fracaso del sistema normativo de la Carta de Naciones Unidas es equivalente a la incapacidad de cualquier regla, como la establecida en el artículo 2.4, en sí misma para controlar el comportamiento de los Estados". En su opinión, "lo que mató el artículo 2.4 fue la gran disparidad entre las normas que pretendía establecer y los objetivos prácticos que los países están llevando a cabo en defensa de sus intereses nacionales" (T.M. Franck, "Who Killed Article 2 (4) or: Changing Norms Governing The Use of Force By States", The American Journal of International Law, Vol. 64 (1970), pp. 809-837, en concreto pp. 836-837).

[94] Citado por Ruys, supra nota 64, p. 14.

la constitución y regulación de la legalidad del uso de la fuerza por parte de los Estados es una evidencia convincente del poder del derecho internacional"[95]. En una línea de argumentación similar, Ruys sostiene que "es difícil aceptar el colapso normativo de las normas de la Carta sobre el uso de la fuerza. Por un lado, ningún Estado ha buscado repudiar abiertamente las normas (…). Por otro lado, a pesar de lo que pudiera pensarse al leer las noticias, las violaciones de jus ad bellum no son tan generalizadas. Los verdaderos choques fronterizos a pequeña escala entre los Estados se producen semanalmente, sino diariamente, en todo el mundo, no obstante en general, la incidencia de los conflictos armados interestatales probablemente ha disminuido."[96]. Sin llegar a estar totalmente de acuerdo con este diagnóstico de la situación[97], no hay duda de que se ha producido un cambio de paradigma, pero no tanto por una relativización de la conflictividad internacional y un aumento de la interna, sino por un cambio en las modalidades mismas de conflictividad y de las amenazas a la seguridad[98], que está superando los parámetros tradicionales de comprensión de las mismas en el marco de las relaciones meramente interestatales y en la dialéctica de su diferenciación con las internas.[99]

A lo largo de la historia y, en particular, desde la formación del Estado moderno, la idea de la guerra y la imagen del uso de la fuerza es el conflicto interestatal como la amenaza por excelencia a la paz y la seguridad internacionales. Es, en efecto, el tipo de conflicto que se ha de conjurar cuando la Carta de Naciones Unidas establece literalmente que los miembros de esta organización, en sus relaciones internacionales,

---

[95] Hurd, supra nota 63, p. 13.
[96] Ruys, supra nota 64, p. 15.
[97] Como explica Wood, además de Siria, "Por supuesto, hubo muchos otros usos de la fuerza en 2015: la intervención de terceros Estados en la guerra civil en Yemen planteó la cuestión de la intervención por invitación; los interminables conflictos, o conflictos en Afganistán; intervenciones francesas en África, y así sucesivamente. Incluso en lo que respecta a Siria, tendré que limitarme. No voy a referirme, por ejemplo, a las operaciones turcas o rusas, incluyendo el derribo por parte de Turquía de un avión militar ruso. Cada uno de ellos merecería una conferencia en sí misma" (Wood, supra nota 65, p. 4).
[98] Sobre esta cuestión, véase el Informe "Un mundo más seguro: la responsabilidad que compartimos", A/59/565, 2 de diciembre de 2004, pp. 34-38.
[99] En el marco de la ONU, la reglamentación del uso de la fuerza se remite al conflicto interestatal y al interno sólo en la medida en que requiere la intervención del Consejo de Seguridad, esto es, cuando su continuación es susceptible de poner en peligro la paz y la seguridad internacional. Esta dialéctica internacional versus interno se sigue formalizando, en 1977, cuando los Protocolos Adicionales a los Convenios de Ginebra de 1949 contemplan por separado la protección de las víctimas de los conflictos armados internacionales y de los conflictos armados sin carácter internacional.

"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". Es, asimismo, la modalidad de conflicto que autoriza la acción de la ONU como se desprende del artículo 2.7 en virtud del cual "Ninguna disposición de esta Carta autorizará a las Naciones Unidas a intervenir en los asuntos que son esencialmente de la jurisdicción interna de los Estados, ni obligará a los Miembros a someter dichos asuntos a procedimientos de arreglo conforme a la presente Carta; pero este principio no se opone a la aplicación de las medidas coercitivas prescritas en el Capítulo VII".

Con el tiempo, sin embargo, por razones de distinta índole en las que importan lógicamente también los efectos de la globalización económica, financiera y comercial, además de política y social, cambia el contenido de la conflictividad internacional. Sin soslayar la existencia de controversias interestatales, incluso persistentes y graves, ni pecar de idealismo, las amenazas para la paz y la seguridad internacionales son más amplias y diversas y no provienen sólo o principalmente de un actor estatal. Tampoco el concepto de guerra es exactamente el mismo. Hay, lamentablemente, una sensación de amenaza más próxima y real y una conciencia creciente de que la seguridad no se garantiza en la frontera.

A pesar de ese cambio de contexto, la prohibición del uso y de la amenaza de la fuerza es el principio en torno al que se construye la reacción internacional frente a las nuevas amenazas y a las nuevas modalidades de conflictividad internacional, sirviéndose para ello, y esto es lo importante, de una interpretación del mismo en la que tienen mayor presencia sus excepciones que su propio contenido imperativo.

V. EL ALCANCE Y CONTENIDO DEL PRINCIPIO

El creciente protagonismo de los actores no estatales y la proliferación y diversificación de las amenazas ya eran características de la sociedad internacional en el período de la llamada globalización, pero se extreman con la llegada del ciberespacio y conducen a la necesidad de plantearse, en este punto, dos cuestiones conexas: si el principio de prohibición de la amenaza de uso y el uso de la fuerza sigue siendo la clave de bóveda del sistema de seguridad colectiva y si es suficiente para garantizar una coexistencia internacional en la que los Estados se han

visto negativamente afectados por dos dinámicas concurrentes: una creciente internacionalización y una creciente privatización.

El modelo de Naciones Unidas se apoya en unos principios básicos que son la igualdad soberana de los Estados, la obligación de solución pacífica de controversias y la prohibición del uso y de la amenaza de la fuerza. Son interactivos porque no pueden entenderse aislados o descontextualizados, principalmente, porque forman parte de un sistema global de seguridad asumido por los Estados cuando tenían el monopolio y el control del poder coactivo junto con la capacidad, además de la autoridad, para asumir esos principios como obligaciones para el conjunto de la sociedad internacional.

La aplicación de ese modelo de seguridad en el ciberespacio plantea un primer dilema de orden general porque es un pacto interestatal creado en, por y para una sociedad internacional definida en términos interestatales, que ha de funcionar en un escenario diferente marcado, en el plano subjetivo, por el protagonismo asumido por los actores no estatales y, en términos funcionales, por la asimetría como parámetro característico de las relaciones ciberespaciales[100]. La efectividad de ese pacto para la ordenación del ciberespacio depende de una doble variable: por una parte, la propia capacidad de los Estados para preservar su legitimidad y su autoridad realizando sus funciones en este diferente contexto; y, por otra parte, la aceptación de esa situación por parte del resto de los actores del ciberespacio, circunstancia ésta nada fácil.

La respuesta mayoritaria de los Estados a los desafíos de estos tiempos se ha canalizado en una doble dirección: por una parte, hacia una interpretación pragmática y flexible del principio de prohibición del uso y de la amenaza de uso de la fuerza pretendiendo abarcar dentro del mismo cualquier modalidad de conflictividad más allá de la estrictamente interestatal; y, por otra parte, hacia una interpretación amplia de sus excepciones, particularmente, la legítima defensa[101].

---

[100] El ciberespacio es "un elemento igualador de capacidades y reductor de asimetrías". En efecto, "partiendo de la concepción westfaliana que rige en la política de los Estados-Nación, Internet y el ciberespacio son intrusos que propician un reequilibrio de fuerzas en que la asimetría se convierte en una estrategia por sí misma" (A. Gómez de Ágreda, "El ciberespacio como escenario del conflictos Identificación de las amenazas", en El ciberespacio. Nuevo escenario de confrontación (Madrid, Ministerio de Defensa, 2012, pp. 176 y 179). Así, entre otras cosas, "los ataques cibernéticos pueden llegar a ser una poderosa arma de los débiles" (Hathaway, supra nota 14, p. 842).

[101] Hay, como explica Kolb, una legítima defensa jurídica y una legítima defensa política

Además de que supone apartarse del tenor literal de las normativas, posiblemente no sea la mejor opción frente a esas nuevas modalidades de conflictividad.

A. Una interpretación extensiva

En un ensayo titulado La carrera hacia ninguna parte. Diez lecciones sobre nuestra sociedad en peligro, publicado recientemente[102], Giovanni Sartori advierte que estamos viviendo una guerra inédita. Es terrorista, global, religiosa y tecnológica. Occidente y sus valores están en peligro y no han sido capaces de preverla, ni están preparados para afrontarla. Es una guerra "de una ferocidad que nuestra memoria histórica no recordaba" y en ella "es secundario el componente militar". Es cierto que el uso del término guerra para calificar el terrorismo islámico puede ser discutible y, en cualquier caso, sigue fluctuando entre su rechazo desde la ortodoxia aún imperante y su uso común y generalizado. No obstante, asumiendo la guerra como manifestación extrema del conflicto, sin entrar en otros formalismos, las reflexiones de Sartori alertan sobre una situación tan real como extraordinariamente grave. En otro contexto, pero en la misma línea, el experto en ciberseguridad y candidato a la Presidencia de EE.UU., John McAfee, alertaba sobre una ciberguerra contra el autodenominado Estado Islámico (ISIS, por sus siglas en inglés) que sería "más devastadora que una guerra nuclear."[103] La cuestión estriba en determinar si esa guerra inédita se puede conjurar mediante la prohibición del uso y de la amenaza de uso de la fuerza.

Hasta hace poco, el camino natural hacia la guerra había sido básicamente el uso de la fuerza armada por parte de los Estados. Cuando los miembros de las Naciones Unidas asumen la obligación de abstenerse de usar o de amenazar con el uso de la fuerza en sus relaciones internacionales, hace más de siete décadas, eran los Estados quienes fundamentalmente usaban y podían usar la fuerza en el ámbito internacional y quienes detentaban el monopolio de la violencia legítima en el ámbito interno. Hacia el exterior con el compromiso jurídico de no usarla y hacia el interior con el derecho legítimo de

(Kolb, supra nota 89, pp. 217-218).

[102] G. Sartori, La carrera hacia ninguna parte. Diez lecciones sobre nuestra sociedad en peligro (Madrid: Taurus, 2016).

[103] https://actualidad.rt.com/actualidad/194439-estado-islamico-devastadora-guerra-nuclear.

ejercerla y controlarla, el Estado era el depositario y garante de la regulación del uso de la fuerza armada[104]. Sin embargo, la guerra inédita que conceptualiza Sartori no es una guerra entre Estados, ni se emplea del mismo modo la fuerza. Es una amenaza a la totalidad que no conoce fronteras ni se limita por ellas, que no permite identificar a priori agresores y víctimas, que no permite discriminar medios y objetivos entre lo civil y lo militar, que no está territorialmente localizada en la esfera interna o internacional y que, resumidamente por esas y otras razones, no admite con facilidad una regulación similar a la arbitrada para impedir el conflicto interestatal.[105] No puede ser, en línea de principio, por tratarse de una realidad muy diferente, una regulación válida y eficaz. Sin embargo, es la que han aplicado hasta ahora los Estados en el ámbito internacional.

En esas circunstancias, con ese cambio de paradigma y ante esas nuevas amenazas, hay cierta lógica en la interpretación flexible del principio mismo del artículo 2.4 y en la interpretación extensiva de los componentes de "excepcionalidad" de la prohibición del uso de la fuerza. El caso paradigmático es el terrorismo internacional que, especialmente desde el 11-S, ha justificado una lectura de dicho principio que excede con mucho su versión original, en particular, en la definición de la legítima defensa anticipada y en la identificación de los actores no estatales como objetivo de esa legítima defensa. Por una

---

[104] Sobre el modelo de organización de la fuerza consolidado en la concepción post-Westfalia, véase G.P. Corn, "Should the best Offense Ever Be a Good Defense? The Public Authority to Use Force in Military Operations: Recalibrating the Use of Force Rules in the Standing Rules of Engagement", Vanderbilt Journal of Transnational Law, Vol. 49, Nº 1 (2016), pp. 27-28.

[105] Raboin expresa la magnitud de ese cambio cuando afirma que "la aparición de la guerra cibernética es más que otro paso evolutivo en el desarrollo de la estrategia de guerra y la metodología; (…) Representa un cambio fundamental en la naturaleza misma del concepto de la guerra misma. La idea de que la guerra cibernética alterará la naturaleza inherente de la guerra está enraizada en la idea conceptual de que la guerra cibernética no se limita a cambiar el armamento de las guerras modernas, sino que representa un cambio radical en la naturaleza del campo de batalla en tiempos de guerra. Considerando que toda la evolución histórica de la guerra se ha producido dentro de la esfera común del mundo físico, tangible, la guerra cibernética redefine el campo de batalla central en tiempos de guerra. Sin embargo, las consecuencias de las acciones dentro de este nuevo campo de batalla cibernético son únicas porque a pesar de que se producen en el dominio inmaterial de las redes de ordenadores y flujos de información, los efectos de las medidas adoptadas dentro de ese dominio tienen efectos "reales" en el mundo físico de nuestra la realidad cotidiana" (B. Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", Journal of the National association of Administrative Law Judiciary, Vol. 31, Nº 2 (2011), p. 604). Como explica López de Turiso, "el ciberespacio extiende la zona de combate hasta el mismo corazón de la nación al ser capaz de entrar en cada una de las casas de los ciudadanos y de cortarle los suministros básicos que necesita para su supervivencia" (J. López de Turiso y Sánchez, "La evolución del conflicto hacia un nuevo escenario bélico", El ciberespacio. Nuevo escenario de confrontación, Monografías del CESEDEN, nº 126, febrero 2012, p. 139).

parte, hay que partir de la base de que la legítima defensa es, por definición, por ser defensa[106], una reacción frente a una acción previa y no una anticipación, ni un mecanismo de prevención.[107] Por otra parte, aunque el artículo 51 de la Carta no identifica al autor del ataque armado merecedor de la respuesta en legítima defensa, no es difícil argumentar que está originariamente pensado para Estados basándose en dos datos: uno, la Carta es un pacto entre Estados y el artículo 51 una excepción a un principio que prohíbe el uso de la fuerza entre Estados; y, dos, los actores no estatales no están capacitados entonces para cometer y atribuirse ilícitos internacionales porque carecen de la necesaria subjetividad y porque sus acciones ilícitas se resuelven en el ámbito interno dentro de la categoría de la delincuencia o la criminalidad. Es un tema en el que, como se ha visto, no hay coincidencia entre la posición de los Estados avalada por el Consejo de Seguridad, la jurisprudencia[108] y la doctrina.[109]

En la doctrina, Boeglin explica las consecuencias de este fenómeno a propósito de la declaración del Presidente Hollande de 16 de noviembre de 2015 tras los atentados del 13 de noviembre en Francia. Según sus palabras, "Francia está en guerra. Los actos cometidos el viernes por la noche en París, cerca del estadio de Francia, son actos de guerra. Ellos causaron al menos 129 muertos y muchos heridos. Ello constituye una agresión contra nuestro país, contra sus valores, contra su juventud, contra su estilo de vida". Desde la perspectiva jurídica, Boeglin advierte dos problemas: en primer lugar, una peculiar interpretación del concepto tradicional de "guerra" porque "declararle la 'guerra' a una

[106] Kolb explica certeramente la legítima defensa como un derecho residual, provisional y subordinado (Kolb, supra nota 89, pp. 189-194).

[107] Como explica Fuentes, "La mayoría de la doctrina considera que la legítima defensa preventiva no está permitida en el derecho internacional. Es interesante destacar al respecto lo que señala Christine Gray, en el sentido que los estados, antes de justificar sus acciones en un concepto de legítima defensa preventiva, prefieren recurrir al concepto tradicional de legítima defensa recurriendo a un concepto ampliado de ataque armado. Para quienes insistan en la legalidad de la legítima defensa preventiva viene a ser útil la discusión relativa a la existencia de una regla consuetudinaria de legítima defensa que no se ha subsumido enteramente en el artículo 51 de la Carta de Naciones Unidas. Sin embargo, en general los estados partidarios de la legítima defensa preventiva han preferido buscar estrategias para que se tenga su acción como cubierta por el propio artículo 51. (…) Obviamente, este tipo de interpretaciones se presta para abrir la puerta al uso de la fuerza en situaciones no contempladas originalmente y, por lo mismo, las palabras del Secretario General no son probablemente representativas de una visión mayoritaria entre los estados" (X. Fuentes Torrijo, "La prohibición de la amenaza y del uso de la fuerza por el derecho internacional", Araucaria: Revista Iberoamericana de filosofía, política y humanidades, Vol., 16, Nº 32 (2014), pp. 263-264 (doi: 10.12795/araucaria.2014.i32.13).

[108] Supra nota 81.

[109] Lubell, supra nota 84, p. 35.

entidad no estatal es reconocer de manera implícita a un grupo privado algunas prerrogativas que ostenta un Estado", siendo ésta una línea de acción que puede contribuir a consolidar el liderazgo de ISIS sobre las demás organizaciones; y, en segundo lugar, el uso de la expresión "agresión" porque "ese término adquiere un significado particular cuando un Estado califica como 'agresión' un acto cometido por una entidad no estatal."[110] Aunque realmente hay que distinguir entre acto y crimen de agresión, EE.UU. asume el discurso galo aceptando ese término para legitimar las acciones militares francesas contra ISIS que, sin embargo, son objeto de condena por Rusia, al tiempo que Francia alega su derecho a la legítima defensa de conformidad con la Carta.

La "Declaración sobre el mejoramiento de la eficacia del principio de la abstención de la amenaza o de la utilización de la fuerza en las relaciones internacionales" adoptada por la resolución 42/22 de la Asamblea General de las Naciones Unidas del 16 de noviembre de 1998 traslada, sin embargo, una concepción puramente interestatal de este principio[111]. La mención al terrorismo se realiza sólo con la intención de impulsar la cooperación entre los Estados tanto para prevenirlo y combatirlo, como para contribuir a la eliminación de sus causas subyacentes.[112]

---

110 http://www.dipublico.org/103176/francia-en-guerra-breves-apuntes-desde-la-perspectiva-del-derecho-internacional/.

111 En el apartado 2 se establece que "El principio de abstenerse de recurrir a la amenaza o al uso de la fuerza en las relaciones internacionales es universal en su carácter y es obligatorio para todos los Estados, cualesquiera que sean su sistema político, económico, social o cultural o sus relaciones de alianza". Por otra parte, el apartado 6 dispone que "Los Estados cumplirán las obligaciones que les impone el derecho internacional de abstenerse de organizar, instigar, y apoyar en otros Estados actos paramilitares, terroristas o subversivos, incluidos los actos de mercenarios, así como de participar en ellos o de dar su consentimiento para la realización de actividades organizadas dentro de su territorio que apunten a la comisión de dichos actos" (A/RES/42/22, 18 de noviembre de 1987).

112 Idem.

La resolución 2249 (2015) del Consejo de Seguridad, en cambio, adopta una orientación distinta.[113] La referencia al Capítulo VII ha podido ser interpretada de diversas maneras, incluida la perspectiva de una acción futura, pero, como explica Wood, "Es importante legalmente porque, nuevamente, el Consejo se ha expresado, y lo ha hecho unánimemente, indicando que el derecho inmanente a la legítima defensa individual o colectiva es aplicable a los ataques armados por terroristas y que aplica también frente a los ataques terroristas actuales llevados a cabo por Da'esh". Eso significa, como entiende el representante francés, que "la resolución enmarca nuestra acción dentro del marco del derecho internacional y el respeto por la Carta" y que "los sucesos del 13 de noviembre fueron una agresión armada contra Francia."[114]

El discurso jurídico-político se construye, pues, en torno al principio de prohibición del uso y de la amenaza de uso de la fuerza y sus excepciones y, progresivamente, se normaliza y se trata de legitimar la reacción del Estado mediante el uso de la fuerza armada frente a sujetos no estatales que pueden ser grupos o individuos nacionales de otro Estado o, como se ha demostrado, incluso del propio Estado[115]. En ese caso, el terrorismo internacional del 11-S o del 11-M está dando paso a un terrorismo internacional internalizado o interiorizado que se

---

[113] El apartado 5 de la Resolución "Exhorta a los Estados Miembros que tengan capacidad para hacerlo a que adopten todas las medidas necesarias, de conformidad con el derecho internacional, en particular la Carta de las Naciones Unidas y el derecho internacional de los derechos humanos, el derecho internacional de los refugiados y el derecho internacional humanitario, sobre el territorio que se encuentra bajo el control del EIIL, también conocido como Daesh, en Siria y el Iraq, redoblen y coordinen sus esfuerzos para prevenir y reprimir los actos terroristas cometidos específicamente por el EIIL, también conocido como Daesh, así como el Frente Al-Nusra, y todas las demás personas, grupos, empresas y entidades asociados con Al-Qaida y otros grupos terroristas designados por el Consejo de Seguridad de las Naciones Unidas, y los que acuerde el Grupo Internacional de Apoyo a Siria y corrobore el Consejo de Seguridad, de conformidad con la declaración del Grupo Internacional de Apoyo a Siria de 14 de noviembre, y erradiquen el cobijo que han establecido en partes importantes del Iraq y Siria" (S/RES/2249(2015) de 20 de noviembre de 2015).

[114] Wood, supra nota 65, p. 8.

[115] No comparto la opinión de que "No hay necesidad de nuevas normas de derecho internacional general para hacer frente a la utilización de la fuerza en relación con el terrorismo internacional. El marco establecido en la Carta de Naciones Unidas es la piedra angular del régimen jurídico internacional sobre el uso de la fuerza y los Estados están profundamente comprometidos con él. Sin embargo, la Carta no es un instrumento estático y debe ser interpretado a la luz de la práctica contemporánea y teniendo en cuenta las expectativas de los Estados. Se insta a los Estados a que expresen sus puntos de vista pronto y abiertamente en todos los foros disponibles, sobre la legalidad (o falta de ella) de cualquier instancia en la que la fuerza se utilice." (N. Schrijver y L. van den Herik, Leiden Policy Recommendations on Counter-terrorism and International Law (Leiden: Universidad de Leyden, 2010), p. 11.

produce cuando los autores son los propios nacionales de un Estado asumiendo los objetivos de un colectivo no exactamente exterior, sino transnacional. Si los presuntos autores, o al menos, algunos de ellos, son nacionales del Estado víctima, como parece demostrar el hecho de que entre las medidas previstas se encuentre la retirada de la nacionalidad, hay un problema diferente que ha dejado de ser el uso de la fuerza para combatir una amenaza externa no estatal y se ha convertido en el uso de la fuerza armada para combatir una amenaza de orden interno o mixta si también hay un componente internacional.

La cuestión es determinar si mediante la interpretación o la formulación de excepciones al principio de prohibición del uso de la fuerza puede legítimamente justificarse el uso de la fuerza armada frente a actores no estatales[116], incluso, cuando en el origen del ilícito se puede identificar la autoría de agentes nacionales. La situación encierra, incluso, una paradoja: mientras, por una parte, se eleva al actor no estatal al estrado protagónico de los Estados, por otra, se le excluye del régimen de derechos y garantías constitucionalmente habilitado y, también, de la protección ofrecida por los convenios internacionales en materia de protección de los derechos y libertades fundamentales, sin que tampoco se le pueda encajar con facilidad en el marco de protección del derecho internacional humanitario[117]. Es cierto que, teóricamente, se argumenta el recurso a ambos sistemas, pero en la práctica difícilmente es viable cuando no tienen reconocido ni un estatuto como combatientes.

En este contexto, no está de más preguntarse si en lugar de forzar la aplicación del principio de prohibición del uso de la fuerza y de sus excepciones extrapolando el régimen interestatal a los actores no estatales no sería más adecuado, considerando que son problemas de carácter transnacional, utilizar vías de solución de esa naturaleza mediante modalidades específicas de cooperación interestatal.

---

[116] Sobre las distintas dimensiones de este problema puede verse el completo análisis realizado por Noam Lubell (Lubell, supra nota 84).

[117] Según Schrijver y Herik, "Los actos de terrorismo en sí mismos no constituyen automáticamente un "conflicto armado". La mayoría de los actos terroristas que tienen lugar en el mundo no se califican como conflictos armados y deberían ser tratados en virtud de un paradigma de aplicación de la ley. Esto significa que los regímenes legales aplicables son el derecho interno, las normas de derechos humanos y el derecho penal internacional. El umbral para la aplicación del derecho internacional humanitario (DIH) es la existencia de un conflicto armado u ocupación" (Schrijver y Herik, supra nota 113, pp. 18-19).

Por el momento, sin embargo, la existencia de esa guerra inédita terrorista, global, religiosa y tecnológica es un motivo para introducir diferentes excepciones al principio de prohibición del uso de la fuerza. El problema es que no son homogéneas, porque los Estados no siempre utilizan la misma doctrina, ni siempre en el mismo sentido, ni tampoco parecen mostrarse eficaces para conjurar esas amenazas. Pero es que, además, pueden tener un efecto negativo introduciendo distorsiones en la aplicación primigenia y natural de dicho principio en el marco de las relaciones estrictamente interestatales que es la que se corresponde con su interpretación literal.

B. Una interpretación literal

La aplicación de la prohibición del uso y de la amenaza de la fuerza en el ciberespacio tiene que partir de la identificación de su ámbito de aplicación natural. Aparte de su formulación consuetudinaria, este principio se establece en el artículo 2.4 de la Carta de Naciones Unidas en los siguientes términos: "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".

Consecuentemente con ello, el ámbito de aplicación está claramente delimitado desde varias perspectivas: subjetivamente, a los miembros de la organización; funcionalmente, a sus relaciones internacionales; materialmente, tanto a la amenaza, como al uso de la fuerza armada; y, en el plano teleológico, a una amenaza o un uso de la fuerza concreto que es el especificado en esa disposición y no cualquiera.

La aplicación de este principio al ciberespacio debe ajustarse a esos parámetros jurídicos. En primer lugar, subjetivamente, la prohibición del uso o de la amenaza de uso de la fuerza obliga a los Estados y no a otros actores de las relaciones internacionales para quienes los actos de esa naturaleza están prohibidos en los derechos internos pues encajan en la categoría de actos delictivos o criminales.[118] En segundo término, funcionalmente, es una obligación que se impone en el marco de las "relaciones internacionales"[119], siendo ésta una condición fácilmente identificable en el mundo físico –marcado, como está, por la existencia

[118] Melzer, supra nota 74, p. 10.
[119] Kolb, supra nota 89, p. 183-185.

de la frontera que separa, al menos, formalmente, lo nacional de lo internacional–, pero que plantea indudablemente mayores dificultades, por su propia naturaleza, en el espacio cibernético. En tercer lugar, materialmente, para ser una conducta prohibida, una "amenaza" de actuar[120] o una "acción" en el ciberespacio, diferentes por naturaleza de la actividad cinética, debe merecer la doble calificación de ser "fuerza" y de ser "armada"[121]. Para terminar, la amenaza o la acción se encuentra prohibida si está dirigida "contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas".

Junto a ello, la necesidad de una interpretación basada en un enfoque integral y sistemático de este principio se justifica porque es preciso superar ese método de análisis imperante, centrado en la relación del principio con sus excepciones, que es claramente sesgado y parcial.

La amenaza de uso o el uso de la fuerza tienen una serie de consecuencias que van más allá de la posibilidad de justificar excepciones a dicho principio. Si el ciberataque en cuestión puede ser calificado como un "ataque armado" permite la activación de los mecanismos de legítima defensa en las condiciones estipuladas en el artículo 51 de la Carta. Si el ciberataque es considerado una amenaza a la paz un quebrantamiento de la paz o un acto de agresión admite la adopción de las medidas previstas en el Capítulo VII de la Carta, incluidas las coercitivas, por parte del Consejo de Seguridad. Tanto si alcanza esos umbrales, como si no, la amenaza de uso o el uso de la fuerza constituye, por sí misma y sin estar vinculada a la operatividad de sus excepciones, una vulneración de una norma imperativa de derecho internacional de la que derivan dos consecuencias directas y una posible: la responsabilidad internacional del autor que puede ser reclamada por cualquier Estado al tratarse de la violación de una obligación erga omnes, la posibilidad de adoptar sanciones contra dicho Estado y, como opción, la posibilidad de adopción de contramedidas por parte de los afectados que a su vez pueden revestir la forma de retorsión

[120] Sobre la amenaza, N. Stürchler, The threat of Force in International Law (Cambridge: Cambridge University Press, Cambridge, 2007).

[121] En efecto, "puede por lo tanto concluirse que las ciberoperaciones destinadas a obligar económicamente a otro Estado a participar en, o a desistir, en una determinada línea de no equivaldrían a un uso de la fuerza; tampoco sería la financiación de operaciones cibernéticas de un grupo rebelde" (M.N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?", Standford Law & Policy Review, Vol. 25 (2014), pp. 269-299, en concreto, p. 280). Sobre los motivos que justifican su limitación sólo a la fuerza armada, véase Kolb, supra nota 89, pp. 182-183.

o de represalias. Esto significa que, más allá de la interpretación vinculada a sus excepciones, la categorización de los conceptos de amenaza o uso de la fuerza en el espacio cibernético es necesaria como parte de un enfoque integral y sistémico que reconoce las consecuencias de la vulneración de la prohibición del artículo 2.4 y no sólo la activación de sus excepciones. La importancia de las excepciones no puede obviar el valor de la prohibición misma y las consecuencias de su violación.

En resumen, la acción cibernética prohibida por el artículo 2.4 de la Carta es aquella calificable como amenaza o uso de la fuerza armada, atribuible a un Estado, realizada en el marco de sus relaciones internacionales y dirigida contra la integridad territorial o la independencia política de otro Estado o realizada de modo incompatible con los propósitos de las Naciones Unidas. Ninguno de esos elementos constitutivos de la prohibición contenida en el artículo 2.4 resulta fácilmente extrapolable al ciberespacio, pero probablemente el que ha desencadenado mayor polémica es el componente objetivo de dicho principio: la determinación del concepto de amenaza o uso de la fuerza en el ciberespacio.

VI. EL ELEMENTO OBJETIVO

La determinación del concepto de amenaza o uso de la fuerza en el ciberespacio es objeto de controversia no sólo por la propia dificultad que encierra la calificación de un ciberacto como uso o amenaza de la fuerza en el sentido del artículo 2.4 de la Carta, sino también por el hecho de que esa norma se interpreta atendiendo a sus dos excepciones: una, el derecho de legítima defensa individual o colectiva de los Estados previsto en el artículo 51 de la Carta en caso de ataque armado; y dos, la adopción de las medidas coercitivas del artículo 42 por parte del Consejo de Seguridad cuando se produzca una amenaza a la paz, un quebrantamiento de la paz o un acto de agresión, siendo ésta una situación cuya existencia determinará el propio Consejo de Seguridad de conformidad con el artículo 39.

Como consecuencia de ello, al concepto de “uso” o “amenaza de uso” de la fuerza se suman los de “ataque armado”, “amenaza a la paz”, “quebrantamiento de la paz” y “acto de agresión”, dificultando su

delimitación conceptual[122]. La búsqueda de una interpretación contextual mediante la combinación de esas categorías es una tendencia común en la doctrina que, sin embargo, no está exenta de problemas. El primero es que no existe una identidad material claramente establecida y delimitada entre el contenido de la norma del artículo 2.4 y sus excepciones, como demuestran las dificultades que han rodeado la definición de agresión hasta la Conferencia de Kampala de 2010 y la ausencia de un concepto definitivamente aceptado de ataque armado. En segundo término, tampoco cabe una identidad en términos subjetivos porque mientras la prohibición del artículo 2.4 se dirige a los Estados y también sólo a ellos se les reconoce el derecho de legítima defensa individual o colectiva, el uso o la amenaza de uso de la fuerza, el ataque armado, la amenaza a la paz, el quebrantamiento de la paz o el acto de agresión pueden tener como autores a otros actores diferentes de los Estados, siendo ello otra manifestación de asimetría. Y, en tercer lugar, no existe tampoco una identidad funcional porque, mientras que el uso de la fuerza o el ataque armado son relativamente objetivables, la determinación de que un ciberacto constituye una amenaza a la paz, un quebrantamiento de la paz o, incluso, un acto de agresión corresponde a una decisión del Consejo de Seguridad[123]. El crimen de agresión sí tiene un contenido objetivo tipificado en el artículo 8 bis del Estatuto de la CPI.

En cualquier caso, el concepto de uso de la fuerza es más amplio y potencialmente más difícil de precisar que los conceptos de agresión y de ataque armado. En el ciberespacio, el problema previo es la posibilidad de otorgar la calificación de "armada" a una acción cibernética.

---

[122] Citando a Randelzhofer, Robertson subraya que "Los diversos términos utilizados en la Carta, incluido el –guerra (preámbulo), fuerza armada (preámbulo), actos de agresión (artículo 1), amenaza o uso de la fuerza (artículo 2.4), acto de agresión (artículo 39), y ataque armado (artículo 51)– difieren en alcance y contenido. Aunque están relacionados en el contenido, difieren considerablemente en su significado. Ninguno de ellos se explica con más detalle en la Carta" (H.B. Robertson, "Self-Defence against Computer Network Attacks under International Law", International Law Studies, Vol. 76 (2002), p. 133).

[123] Weissbrodt señala que "El Consejo de Seguridad tiene la autoridad total para clasificar cualquier CNO como una amenaza para la paz, pero es poco probable que lo haga. La decisión de utilizar la fuerza en virtud de los artículos 39 y 42 se determina después de amplios debates y deliberaciones, y durante la votación cualquier decisión de utilizar la fuerza podrá ser bloqueada a través de un veto por cualquiera de los miembros permanentes del Consejo de Seguridad. (…) A la luz de la presencia de China y Rusia en el Consejo (las ciberoperaciones regularmente provienen de su territorio), esta limitación puede así representar el mayor obstáculo para una acción eficaz de las Naciones Unidas frente a una operación cibernética que de alguna manera ponga en peligro la estabilidad internacional." (Weissbrodt, supra nota 16, p. 361).

A. La calificación de ciberacción "armada"

La doctrina se muestra dividida sobre la posibilidad de otorgar la consideración de "armada" a una acción cibernética partiendo de la base de que, en la actualidad, "no hay una definición internacionalmente convenida para el término 'arma cibernética'"[124]. Hay cuatro aproximaciones doctrinales principales a esta cuestión desde planteamientos metodológicos diferentes o, incluso, opuestos. Hay una concepción autónoma de arma cibernética (a), una propuesta alternativa finalista que prima los efectos de su uso sobre su naturaleza (b), una tercera opción basada en su analogía con el arma cinética (c) y, por último, el rechazo a esa opción sugiriendo, incluso, la posibilidad de que no admitan la calificación misma como acciones armadas (d).

El Informe del EastWest Institute Critical Terminology Foundations, donde especialistas rusos y estadounidenses trabajan para un entendimiento sobre los conceptos de ciberseguridad, define arma cibernética como el "software, firmware o hardware diseñado o utilizado para causar daño a través del dominio cibernético"[125]. El ciberataque es "el uso ofensivo de un arma cibernética dirigida a dañar un objetivo puntual". Según el Informe, el término "daño" incluye "degradar, inhibir –temporal o permanentemente". Se advierte, asimismo, que un ciberataque "es definido por el tipo de arma y no por la naturaleza del objetivo."[126]

Mele se sitúa en esta línea, aunque asume en parte el componente de los efectos, al considerar al arma cibernética como "una parte del equipamiento, un dispositivo, o un conjunto de instrucciones informáticas utilizadas en un conflicto entre actores tanto nacionales, como no nacionales, con el fin de causar, incluso indirectamente, un daño físico al equipamiento o las personas, o sabotear o dañar de forma

---

[124] J. Stinissen, T. Minárik, N. Pissanidis, M. Veenendaal y L. Glorioso, A Study of Existing and Possible Rules of Engagement for Cyberspace, (Tallin: CCDCOE, 2015), p. 12.

[125] J.B Godwin III, A. Kulpin, K.F. Rauscher y V. Yaschenko, Critical Terminology Foundations 2 (Nueva York, EastWest Institute, 2011) p. 56.

[126] Ibíd., p. 44. Un contraataque cibernético es "el uso de un arma cibernética con intención de ocasionar un daño al objetivo designado en respuesta a un ataque. Un contraataque cibernético puede ser asimétrico. Por lo tanto, un contraataque cibernético puede ser un arma cibernética contra un activo no cibernético o en contra de un activo cibernético. Pero no es un arma no cibernética contra un activo no cibernético. Al igual que un ciberataque, un contraataque cibernético se define por el tipo de arma y no por la naturaleza del objetivo" (Ibíd., p. 45).

directa los sistemas de información de un objetivo sensible del sujeto atacado."[127]

Una segunda opción es vincular el concepto de arma cibernética a los efectos del ciberataque de manera tal que, en realidad, "no es la naturaleza de la herramienta en sí misma lo que importa, sino los efectos que puede causar por su diseño o uso"[128]. Boothby entiende que esa noción "comprendería cualquier equipamiento informático o dispositivo informático que sea diseñado, destinado o usado para generar consecuencias violentas, es decir, causar la muerte o lesiones a personas; o dañar, o destruir objetos"[129]. El Manual de Tallin procede a su definición como "medios cibernéticos de guerra que por su diseño, uso o intención de uso sean capaces de causar lesiones o muerte de personas; o daño a, o la destrucción de los objetos, es decir, con las consecuencias requeridas para la clasificación de una operación cibernética como un 'ataque'."[130] En esta línea, Richard A. Clarke propone la doctrina de la "equivalencia cibernética" según la cual el ciberataque es calificado por sus consecuencias y no por el arma utilizada a esos efectos.[131]

La concepción basada en su analogía con las armas cinéticas es defendida por Brown para quien "tres armas de la información pueden

---

[127] S. Mele, "Cyber-weapons: Legal and strategic aspects", Defense IQ (2013), p. 10. Para el autor, "es necesario centrarse en tres elementos esenciales: [1]. El contexto, que debe ser el contexto típico de un acto de guerra cibernética. Este concepto se puede definir como un conflicto entre actores, tanto nacionales y no nacionales, que se caracteriza por el uso de sistemas de información tecnológica, con el fin de lograr, mantener o defender una condición de ventaja estratégica, operativa y/o táctico. [2]. El propósito, provocando, incluso indirectamente, daño físico a los equipos o las personas, o más bien sabotear o dañar de manera directa los sistemas de información de un objetivo sensible del sujeto atacado. [3]. El medio u herramienta, un ataque llevado a cabo mediante el uso de sistemas de información tecnológica, incluyendo Internet" (Ibíd.).

[128] Stinissen et al., supra nota 122, p. 13. Para un análisis pormenorizado de ese concepto, puede verse Hathaway, supra nota 14, pp. 817-885. En su opinión, "Un ciberataque consiste en cualquier acción destinada a debilitar las funciones de una red de ordenadores para un propósito de seguridad política o nacional" (Ibíd., p. 826).

[129] W.H. Boothby, "Methods and Means of Cyber Warfare", International Law Studies, Vol. 89 (2013) p. 389.

[130] Regla Nº 11, pp. 45-48.

[131] Citado por Das, supra nota 1, p. 133.

ser identificadas: el código, el sistema informático, y el operador."[132] Entiende el autor que el uso de cada una de ellas "se ve limitado a los principios de distinción, necesidad militar, proporcionalidad, humanidad y caballerosidad, y las armas en sí mismas se convierten en objetivos legítimos."[133] En esa línea, pero asumiendo también la tesis de los efectos, se pronuncia Katharina Ziolkowski que aduce sus similitudes con las armas biológicas y químicas. En su opinión, "el uso de armas biológicas y químicas no causa destrucción en un sentido tradicional, en tanto estas armas no liberan energía cinética. El uso de armas biológicas y químicas es considerado como una forma de uso [armado] de la fuerza ya que pueden causar muerte o lesiones a seres vivos. Por lo tanto, en el caso de las armas biológicas y químicas, el término 'arma' se define en referencia a sus efectos y no a su método, lo cual se corresponde perfectamente con el enfoque del derecho internacional público basado en los efectos"[134]. En una línea de argumentación que lleva a un resultado similar, Kolb considera que el concepto de arma es relativo porque "se pueden utilizar muchos objetos como armas, siempre que resulte en una restricción física similar a la armada". El autor identifica las armas explosivas y no explosivas, junto con "técnicas tales como la propagación de un incendio, la apertura de embalses de agua, la propagación de la radiactividad, el terrorismo cibernético (ataques de los sistemas informáticos de control de las centrales nucleares, embalses, etc.)."[135]

No toda la doctrina está de acuerdo en la asimilación de efectos o en la definición por analogía. Das explica que "falta una práctica estatal inequívoca caracterizando a los ciberataques como usos de la fuerza. Esto se debe a que la prohibición del artículo 2.4 se extiende sólo a la acción estatal. Tan solo unos pocos Estados han sido identificados con

---

[132] En su opinión, "Al definir el arma de información, es útil establecer una analogía con el arma de fuego. Cuando se dispara un arma, la bala viaja a través del espacio y alcanza un objetivo, dañándolo. El arma de fuego por sí misma no puede hacer daño (a menos que sea utilizada como una cachiporra); su función es impulsar la bala a su objetivo. La bala en sí misma no puede hacer daño (a menos de que explote o atraviese la piel); se vuelve mortal sólo en virtud de ser propulsada a alta velocidad por la pistola. Por último, ni el arma ni la bala es efectiva a menos que un combatiente esté presente para cargar la bala en el arma y disparar" (D. Brown, "A Proposal for An International Convention To Regulate the Use of Information Systems in Armed Conflict", Harvard International Law Journal, Vol. 47, Nº 1 (2006), pp. 184-185).

[133] Ibíd., p. 185.

[134] K. Ziolkowski, "Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt Criteria" for Use of Force", en C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 4th International Conference on Cyber Conflict (Tallin: CCD COE, 2012), p. 308.

[135] Ibíd.

certeza como los causantes de ciberoperaciones que han constituido un uso de la fuerza."[136] En su opinión, "la supuesta extensión del ámbito del artículo 2.4 a esas armas no facilitaría la aplicación del artículo 2.4 a los ataques a las redes informáticas en los mismos términos.[137]. Sin embargo, hay además una dificultad adicional, y no pequeña, que dificulta el planteamiento analógico porque "la gran mayoría de las ciberoperaciones no pretenden causar un daño permanente a cualquier sistema. Los ataques generalmente intentan generar una molestia al usuario, negándole la capacidad de utilizar apropiadamente el objeto del ataque."[138]

A la discutida definición del arma cibernética se suma la controversia sobre el alcance y significado de las expresiones utilizadas para designar acciones cibernéticas. En general se distinguen los conceptos de explotación de redes informáticas (CNE, por sus siglas en inglés), operación de redes informáticas (CNO, por sus siglas en inglés) y ataque a las redes informáticas (CNA, por sus siglas en inglés), pero la confusión principal se plantea respecto de los dos últimos[139].

Weissbrodt afirma que las CNO han sido definidas por la doctrina y por autoridades militares estadounidenses como un "ataque, engaño, una degradación, interrupción, negación, explotación y defensa de información electrónica e infraestructura."[140] No obstante, en su opinión, es preferible usar ese término para describir "cualquier tipo de intrusión informática o defensa en línea."[141] Las CNA encajarían, en

---

[136] En su opinión, "Mientras que algunos han argumentado que la Corte Internacional de Justicia ha intentado ampliar la comprensión de la "fuerza" en el derecho internacional para incluir no solo los ataques cinéticos convencionales, sino también los ataques con armas tan variadas como armas químicas, biológicas y nucleares, juristas de la escuela positivista más tradicional creen que una distinción clara puede ser trazada entre dichas armas y la CAN. En primer lugar, este tipo de armas causan la muerte y la devastación a escala masiva. En segundo lugar, operan bajo el mismo principio como una ojiva convencional, es decir, un proyectil con una carga mortal que se lanza a un blanco. Estos dos atributos sitúan efectivamente tales armas en una categoría propia. De hecho, cada uno de estos tipos de armas tiene uno o más tratados que específicamente prohíben o regulan su uso". (Das, supra nota 1, p. 133).

[137] Das considera que "la fuerza militar cinética es simplemente una forma de la fuerza que produce un tipo particular de efecto destructivo. Es la más conocida y, por tanto, la más fácil de observar e identificar. Sin embargo, con el auge de las tecnologías modernas de guerra durante la segunda mitad del siglo pasado, algunos Estados han impulsado la idea de que la 'fuerza' incluye otras formas de presión que ponen en peligro la autonomía del Estado" (Ibíd., p. 125).

[138] Ibíd., p. 135.

[139] Sobre las diferencias entre CNE y CNA, véase M. Libicki, Cyberdeterrence and cyberwar (Santa monica: Rand Corporation, 2009) pp. 23-24. Véase P. A. Johnson, "Is it Time for a Treaty on Information Warfare?", International Law Studies, Vol. 76 (2002), pp. 440-441.

[140] Sobre los tipos de CAN, véase Johnson, supra nota 139, pp. 440-441.

[141] Weissbrodt, supra nota 16, p. 354.

principio, en la primera definición. Zemanek considera que los CNA son "acciones llevadas a cabo a través del uso de redes informáticas para interrumpir, degradar o destruir información que se encuentra en computadoras o en redes informáticas o en computadoras y redes en sí mismas. Los virus, gusanos, troyanos y dispositivos similares destruyen o alteran información y programas, mientras que los ataques a la negación de servicios ('DoS', por sus siglas en inglés) inundan un sitio de internet, un servidor o un enrutador con más solicitudes de información que las que puede procesar para apagarlo."[142]. Sin embargo, Dinstein advierte que una CNA "es comúnmente definida inadecuadamente como la interrupción, negación, degradación o destrucción de información que se encuentra en una red informática o la propia red" cuando, a su juicio, "una predicción fiable de la evolución futura debe partir de la premisa indiscutible de que CNA potenciales (a través de la alimentación de mensajes falsos en un sistema informático de destino) pueden también implicar un sabotaje grave, diseñado para dejar atrás un rastro de muerte y devastación a través de explosiones inducidas y otras averías 'maliciosas'."[143] Dinstein subraya, además, que los CNA "no son todos de la misma naturaleza"[144] y, como explica a su vez Das, "el alcance de la utilización del CNA es inmenso."[145] Además, el CNA " ha surgido como una de las herramientas disponibles más prometedoras para un comandante militar en el cumplimiento de sus misiones y la legítima defensa."[146]

El resultado es que no hay consenso, pero la doctrina mayoritaria apoya el criterio de los efectos para definir el arma cibernética, junto con un concepto amplio no cerrado de los CNA. Esta perspectiva de análisis tiene la ventaja de asumir la polivalencia genética de los ciberataques en la medida en que la misma acción cibernética puede ser un acto criminal, terrorista, de espionaje o bélico en función del autor, la intención y los efectos. No obstante, por otra parte, no permite discriminar a priori las acciones susceptibles de contrariar la prohibición del artículo 2.4 de la Carta, ni tampoco otorgarles el

---

[142] K. Zemanek, "Armed Attack", en Oxford Public International Law, Max Planck Encyclopedia of Public International Law [MPEPIL] (2013) párr. 13.
[143] Y. Dinstein, "Computer Network Attacks and Self-Defence", International Law Studies, Vol. 76 (2002) pp. 102-103.
[144] Ibíd.
[145] Das, supra nota 1, p. 125.
[146] O'Donnell y Kraskam, supra nota 4, p. 395.

calificativo de "armada" requerido para tipificar la conducta prohibida por esa disposición. En cambio, la definición autónoma avalada por el EastWest Institute no plantea esos problemas, probablemente, por ser más genérica. El debate, en cualquier caso, no está cerrado y sigue fluctuando entre quienes privilegian la naturaleza del arma y quienes atienden prioritariamente a sus efectos y objetivo. Conviene recordar, no obstante, que en el caso de la legalidad del uso y de la amenaza de las armas nucleares la CIJ resta relevancia al arma en beneficio de los efectos o el objetivo.

B. El uso de la fuerza

Según el Manual de Tallin, "una ciber operación constituye un uso de la fuerza cuando su escala y efectos son comparables con operaciones no cibernéticas que alcancen el nivel de uso de la fuerza"[147]. Por su parte, con respecto a la amenaza[148], según el Manual de Tallin "una ciber operación, o amenaza de ciberoperaciones constituye una amenaza ilícita de la fuerza cuando la acción amenazante, si fuera llevada a cabo, constituiría un uso ilícito de la fuerza"[149]. El concepto de amenaza no resulta fácil de concretar más allá de que es susceptible de incluir los actos preparatorios previos al uso de la fuerza. Como advierte Kolb, su definición requiere una perspectiva más amplia no sólo objetiva, sino también subjetiva y contextual para determinar los hechos subsumibles en dicha categoría.[150]

Con carácter general, siguiendo a Schmitt, la identificación de una acción cibernética como uso de la fuerza puede hacerse depender de dos criterios: teleológico y funcional. En el primero, "las ciberoperaciones dirigidas a ciertas categorías de objetivos crean la presunción irrebatible de que la fuerza ha sido empleada". El segundo trata de buscar "el equivalente funcional de la destrucción física con el propósito de caracterizar el uso de la fuerza"[151]. Además de esos criterios genéricos, el autor propone utilizar a esos efectos el test de los factores asumido por el Grupo Internacional de Expertos de Tallin que son "severidad, inmediatez, rectitud, invasión, mensurabilidad, carácter

[147] Regla Nº 11, pp. 45-52.
[148] Weissbrodt, supra nota 16, p. 357.
[149] Regla Nº 12, pp. 52-53.
[150] Kolb, supra nota 89, p. 181.
[151] Schmitt, supra nota 119, p. 281.

militar, involucramiento del Estado, y legalidad presuntiva."[152] La cuestión es que estos factores relacionados por Schmitt para determinar la existencia de un uso de la fuerza han sido seguidos por un amplio sector doctrinal, pero también han sido utilizados, y por una autorizada doctrina, para determinar su calificación como ataque armado cuando, en realidad, se trata de cosas distintas[153], lo que demuestra la confusión que rodea ambos conceptos y su delimitación. Schmitt concluye que "la gravedad por sí sola puede servir para calificar una operación cibernética como un uso de la fuerza."[154]

Gervais se muestra crítico con el modelo de Schmitt porque incorpora elementos ajenos a la coerción armada y porque no establece un criterio sobre el peso específico de cada uno de sus criterios.[155] Para Simonet, "podemos estimar que los ataques cibernéticos podrían clasificar como uso de la fuerza en virtud de la Carta, siempre que los efectos de estos actos sean comparables, en términos de letalidad y destrucción, a las de los ataques convencionales o nucleares, biológicos o químicos (NBC, por sus siglas en inglés)."[156]

Katharina Ziolkowski considera que "se puede suponer que las actividades cibernéticas pueden considerarse como un uso [armado] de la fuerza en el sentido del artículo 2.4 de la Carta de Naciones Unidas si –indirectamente– dan lugar a: 1) la muerte o lesiones físicas de seres vivos y/o la destrucción de la propiedad; 2) la interrupción masiva, a medio o largo plazo de los sistemas de infraestructura crítica de un Estado (si en su efecto es equiparable a la destrucción física de tales sistemas)"[157]. No recibirían esa calificación la destrucción o el robo de datos, porque sus efectos "no pueden ser equiparados con los efectos usualmente causados o pretendidos por las armas convencionales o biológicas y químicas, especialmente no con la destrucción física de objetos".[158]

El desacuerdo doctrinal sobre los criterios de calificación de una acción cibernética como uso de la fuerza contrasta con el consenso jurisprudencial, institucional y doctrinal sobre el hecho de que todos los

[152] Ibíd., p. 280; Ziolkowski, supra nota 132, pp. 295-309.
[153] Hathaway, supra nota 15, pp. 847-848.
[154] Schmitt, supra nota 119, p. 281.
[155] Gervais, supra nota 186, pp 540-541.
[156] L. Simonet, "L'usage de la force dans le cyberspace et le droit international", Revue défense nationale (2012), p. 53.
[157] Ziolkowski, supra nota 132, pp. 173-174.
[158] Ibíd.

ataques armados son uso de la fuerza, pero no todos los usos de la fuerza pueden ser calificados como ataques armados. No obstante, a partir de ahí, también vuelven las discrepancias en torno a la diferenciación entre ambos conceptos.

En el caso Nicaragua, la Corte Internacional de Justicia apunta en esa dirección cuando afirma la necesidad de distinguir "las formas más graves de uso de la fuerza (aquellas que constituyen un ataque armado) de otras formas menos graves", tales como 'un simple incidente fronterizo', basado en la 'escala y efectos' de la fuerza involucrada."[159] En el mismo caso asume la posibilidad de usos indirectos de la fuerza como el hecho de armar o entrenar insurgentes.[160]

En el marco de la OTAN se reconoce, asimismo, "una diferencia conocida entre las mencionadas disposiciones de la Carta es que la prohibición del artículo 2.4 es más amplia que la excepción del artículo 51, que sólo permite contramedidas, incluyendo el uso de la fuerza, cuando se produce un ataque armado."[161]

Entre la doctrina, Schmitt sostiene que "todos los ataques armados son usos de la fuerza [en el sentido del artículo 2], pero no todos los usos de la fuerza califican como ataques armados que es uno de los requisitos previos para una respuesta armada". Según Melzer, "esta terminología sugiere una brecha entre la prohibición de la 'fuerza' del artículo 2.4 y la excepción en el caso de 'ataque armado' del artículo 51 de la Carta de Naciones Unidas. En efecto, el alcance del artículo 2.4 de la Carta de las Naciones Unidas es más amplio que el del artículo 51 porque incluye no solamente usos armados, sino también usos desarmados o indirectos de la fuerza, y no sólo el uso real, sino también la mera amenaza de la fuerza"[162]. En términos similares, remitiéndose al caso concreto de las Reglas de Enfrentamiento (ROE, por sus siglas en inglés), Stinissen et al. sostienen que "la noción de 'uso de la fuerza' de las ROE es potencialmente más amplia que 'ataque' en el derecho de los conflictos armados. En otras palabras, todos los ataques en un contexto de conflicto armado constituyen uso de la fuerza, pero no todo uso de la fuerza es un ataque en el sentido dado por el derecho de los conflictos armados. No obstante, la forma en que el derecho de los conflictos

[159] Supra nota 79.
[160] Ibíd.
[161] NATO Legal Deskbook (MC 362/1 de la OTAN), p. 233.
[162] Melzer, supra nota 74, p. 11.

armados define un ataque puede servir como base para la discusión del uso de la fuerza."[163]

El consenso termina en esa diferenciación entre el todo y la parte o entre lo general y lo especial porque, a partir de ahí, la determinación del criterio aplicable para adscribir una ciberacción a una u otra categoría es objeto de controversia.

Katharina Ziolkowski afirma que el ataque armado se produce en los supuestos de uso de la fuerza armada "mostrando adicionalmente un alcance considerable y una mayor intensidad de los efectos"[164]. La propia autora reconoce que es un criterio "deliberadamente vago."[165] En el mismo sentido se manifiesta Schmitt cuando afirma que, reducidos a lo básico, "el 'criterio Schmitt' representa un reconocimiento de la ambigüedad existente en la norma de uso de la fuerza. Dada la ambigüedad, el margen de decisión de los Estados es amplio. Inevitablemente aprovecharán esta flexibilidad de toma de decisiones a través de la adopción de posiciones legales que optimicen sus intereses nacionales. Los criterios son los que yo creo que son algunas de las influencias extralegales clave en ese proceso complejo. En este sentido, están destinados a ser predictivos, no prescriptivos.[166]

Consciente de esas carencias, Melzer no está conforme con la aplicación del criterio de la escala y los efectos alegando que "En vista de las consecuencias perjudiciales, en lugar de destructivas, de la gran mayoría de los ataques cibernéticos, sigue siendo insatisfactoria, no obstante, para interpretar el criterio de 'escala y efectos' exclusivamente en términos de efectos equivalentes a la destrucción física. El principal problema es que, dependiendo de lo que se considera que es 'equivalente' a la destrucción física, este enfoque terminará o bien siendo demasiado restrictivo (es decir, incluyendo únicamente las operaciones cibernéticas que resultan directamente en destrucción física, pero no, por ejemplo, la 'mera' inhabilitación de todo el sistema nacional de red de energía, red de telecomunicaciones o de defensa aérea) o demasiado expansiva (es decir, incluyendo cualquier ataque de denegación de servicio incluso en contra de proveedores de servicios no

---

[163] Stinissen et al., supra nota 122, p. 19.
[164] Ziolkowski, supra nota 132, p. 308.
[165] Ibíd.
[166] M.N. Schmitt, "The 'Use of Force' in Cyberspace: A Reply to Dr Ziolkowski", en C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 4th International Conference on Cyber Conflict (Tallin: CCD COE, 2012), p. 317.

esenciales de carácter exclusivamente civil, como por ejemplo servicios de compras en línea o directorios telefónicos).[167]

Según Melzer, el criterio para distinguir un ataque armado respecto de formas menos graves de uso de la fuerza "requeriría no sólo el ataque cibernético en cuestión, sino también la intención agresiva inherente al sentido corriente de ataque". Este requisito "no sólo reflejaría la máxima de minimis non curat lex, sino que también evitaría que la propagación accidental de malware sea considerada como un ataque armado basado exclusivamente en la escala y efectos objetivos del accidente."[168] El problema estriba precisamente en demostrar la existencia de esa intencionalidad. En una línea de argumentación próxima, contraria al criterio de la escala y los efectos, Schrijver y Van den Herik excluyen directamente esa opción cuando afirman que el artículo 51 "no incluye un requisito de escala para un ataque armado."[169]

Por el momento, mayoritariamente, pero desde la perspectiva del mundo cinético, y a pesar de la dificultad de extrapolarlo al mundo virtual, la clave de la diferenciación entre uso de la fuerza y ataque armado se sigue situando en una cuestión de grado. No hay, sin embargo, acuerdo sobre el punto o el umbral a partir del cual deja de ser sólo uso de la fuerza para convertirse en ataque armado. El uso de la fuerza ascendería a la condición de ataque armado, según Schmitt, cuando la acción "lesiona o mata personas; o daña o destruye la propiedad", en cuyo caso admitiría el recurso a la legítima defensa y, en su caso, la acción del Consejo de Seguridad si considera el ciberataque como una amenaza a la paz, un quebrantamiento de la paz o un acto de agresión. En el Manual de Tallin la calificación se hace depender también de la escala y los efectos.[170] Siguiendo a Kolb, "el único criterio abstracto es decir que necesitamos un uso de la fuerza con un mínimo de coherencia y peligrosidad, que está en algún lugar a medio camino entre lo trivial y lo significativo. Esto debería tratarse de un ataque que afirme la existencia de una política de fuerza (patrón de violencia) contra un Estado y no actos esporádicos de poca intensidad."[171]

En cualquier caso, conviene no olvidar el dato subjetivo clave en la diferenciación entre ambas categorías porque, si la acción procede de un

[167] Melzer, supra nota 74, p. 14.
[168] Ibíd., p. 16.
[169] Schrijver y Herik, supra nota 113, p. 13.
[170] Regla Nº p. 54.
[171] Kolb, supra nota 89, p. 212.

actor no estatal, podrá ser ciberataque armado, pero no uso de la fuerza en el sentido del artículo 2.4.[172] Aunque la jurisprudencia de la CIJ excluye la posibilidad de definir como ataques armados acciones procedentes de agentes diferentes de los Estados, no es esta la práctica internacional seguida por los propios Estados y por el Consejo de Seguridad, tampoco es aceptada por la doctrina[173], ni se atiene a la redacción del artículo 51 de la Carta. Una lectura estricta de la norma permite discriminar en función del autor porque no cabe calificar como uso de la fuerza a los efectos del artículo 2.4 una acción procedente de un agente no estatal, mientras que sí puede atribuírsele la autoría de un ciberataque armado. Este concepto también es objeto de controversia.[174]

C. El ciberataque armado

La categoría "ciberataque armado" se puede concebir como la traslación al espacio cibernético del concepto de "ataque armado" del mundo físico. El ataque armado constituye una modalidad de uso de la fuerza y una excepción a la prohibición de su uso. El artículo 51 de la Carta autoriza el uso de la fuerza en el ejercicio del derecho a la legítima defensa individual o colectiva en caso de ataque armado. De hecho, el desarrollo conceptual de esa categoría se encuentra, generalmente, vinculado a la definición de la legítima defensa de la Carta de Naciones

---

[172] Como explica Zemanek, "En las décadas que siguieron a la fundación de las Naciones Unidas, los ataques por fuerzas irregulares se hicieron más frecuentes y la CIJ reaccionó a ese desarrollo en su sentencia del caso Nicaragua de 1986. Tomando las normas de responsabilidad de los Estados y la definición de la agresión, amplió el término 'atacante' incluyendo 'el envío de o en nombre de un Estado de bandas armadas, grupos irregulares o mercenarios' en la lista de actos que pudieran constituir un ataque armado en el sentido del Art. 51 de la Carta de Naciones Unidas" (Zemanek, supra nota 141, parr. 6). Según Melzer, "el alcance del artículo 51 también podrá ser superior a la del artículo 2.4, es decir, mediante una excepción a las restricciones de la Carta, en todos los casos en que se produzca un ataque armado contra un Estado miembro, con independencia de su imputabilidad a otro Estado. Podría decirse, por lo tanto, que un ataque armado contra un Estado llevado a cabo por actores no estatales en el territorio de otro Estado –aunque no, como tal, prohibido por el artículo 2.4– podría potencialmente justificar la acción de legítima defensa dentro de ese Estado (territorial) como excepción a las restricciones de la Carta. Cabe señalar, sin embargo, que la interpretación de la noción de un ataque armado que incluya los actos llevados a cabo por actores no estatales sigue siendo controvertida y no refleja un consenso universal. "(Melzer, supra nota 74, p. 12).

[173] Kolb, supra nota 89, p. 202.

[174] Schmitt afirma que "El advenimiento de las operaciones cibernéticas desafió este presupuesto porque ahora operaciones que no encajan perfectamente en la idea de un ataque que era 'armado' en el sentido cinético podrían causar graves consecuencias. Si bien la Corte Internacional de Justicia se había pronunciado en su opinión consultiva sobre armas nucleares afirmando que el tipo de arma utilizada es irrelevante para la aplicación de los artículos 2.4 y 51, las ciberoperaciones parecían distantes del concepto de 'arma'" (M.N. Schmitt "Attack" as a Term of Art in International Law: The Cyber Operations Context", en C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 4th International Conference on Cyber Conflict (Tallin: CCD COE, 2012) p. 287).

Unidas que, como se ha visto, no es precisamente una institución pacífica en derecho internacional.

El concepto de ciberataque armado es controvertido por tres motivos principales: en primer lugar, la generalización del término ciberataque para referirse a cualquier acción cibernética desde el mero hacking pasando por toda la escala de posibles acciones ilícitas hasta su expresión extrema en la ciberguerra[175]; en segundo lugar, la dificultad de calificar un ciberataque como un uso o una amenaza de la fuerza al tratarse de nociones con una clara impronta cinética; y, en tercer lugar, en esa misma línea, pero como una complicación adicional, la atribución de un contenido específico a un ciberataque para superar el nivel del simple uso de la fuerza.

La jurisprudencia internacional reconoce que el ataque armado es una forma grave de uso de la fuerza,[176] pero no ofrece soluciones definitivas sobre el concepto mismo de ataque armado, más allá de la afirmación de la irrelevancia del tipo de "arma"[177] y de que está excluidos los usos indirectos de la fuerza por su reconocida menor entidad[178]. Stinissen et al advierten que los términos ataque y ciberataque son usados en sentido amplio, en varios contextos y con diferentes significados[179], circunstancia ésta que dificulta su definición.

En el contexto concreto del derecho internacional de los conflictos armados, ataque tiene un significado específico en los términos del Protocolo Adicional I a los Convenios de Ginebra en cuyo artículo 49 se identifica con "los actos de violencia contra el adversario, sean ofensivos o defensivos". El Manual de Tallin define el ciberataque como "una operación cibernética, ya sea ofensiva o defensiva que se espera razonablemente que cause lesiones o la muerte a personas; o daño o destrucción de objetos."[180] Wilmshurst introduce un componente

---

[175] No hay una definición universalmente aceptada de ciberataque. Sobre las distintas concepciones, véase Moore, supra nota 29, pp. 223-257. Para un análisis pormenorizado de este concepto, véanse Hathaway et al., supra nota 15, pp. 817-885. Para los autores, "Un ciberataque consiste en cualquier acción destinada a debilitar las funciones de una red de ordenadores para un propósito de seguridad política o nacional" (Ibíd., p. 826).

[176] Supra nota 73.

[177] Supra nota 75. Siguiendo a la CIJ, "39. Esas disposiciones no se refieren a armas concretas. Se refieren a cualquier uso de la fuerza, con independencia de las armas empleadas. La Carta ni prohíbe ni autoriza expresamente el uso de un arma concreta, inclusive las armas nucleares. Un arma que ya es ilícita per se, sea en virtud de un tratado o de la costumbre, no se vuelve lícita por utilizarse para un propósito que sea legítimo con arreglo a la Carta" (Ibíd.).

[178] Supra nota 73.

[179] Stinissen et al., supra nota 122, p. 12.

[180] Regla Nº 30, pp. 106-110.

adicional al afirmar que es "una intervención intencional en o contra otro Estado sin el consentimiento de ese Estado o su aquiescencia subsecuente, que no está legalmente justificado". Es, a su juicio, una modalidad de uso de la fuerza armada que se singulariza, no por un nivel de intensidad, sino por la presencia de la intención de atacar[181]. El problema, en este caso, es demostrar que esa intención va más allá del simple uso de la fuerza porque también en ésta, salvo cuando se trata de usos indirectos, hay alguna intencionalidad.

La doctrina propone un test para evaluar cuando un ciberataque es un "ataque armado" a los efectos de activar el derecho de legítima defensa. Hay tres interpretaciones doctrinales que atienden al instrumento, al objetivo y a los efectos. En el primer caso, el enfoque basado en el instrumento, un ciberataque es un ataque armado sólo cuando implica el uso de armas o mecanismos militares. La ventaja de esta teoría es su simplicidad "en tanto los usos de armas y fuerza militares son relativamente fáciles de identificar" pero, por otra parte, en la medida en que los ciberataques "tienen el potencial de causar daños catastróficos sin emplear armas militares tradicionales muchos académicos han rechazado el enfoque basado en el instrumento para la definición de los ataques armados como peligrosamente obsoleta."[182] En el segundo supuesto, el enfoque basado en el objetivo, se trata de un ataque armado cuando el objetivo es una infraestructura crítica o un importante sistema informático para cuya protección se hace imprescindible una legítima defensa preventiva siendo ésta, precisamente, su mayor carencia por el potencial conflictivo que implicaría esa interpretación del ciberataque.[183] En el último, el enfoque basado en la consecuencia, el ciberataque se califica como ataque armado sobre la base de la gravedad de sus efectos.[184]

La teoría de las consecuencias o los efectos es la que recibe mayor apoyo doctrinal. Lewis advierte, sin embargo, que no se debe usar sólo

---

[181] Así, "El término 'ataque armado' requiere que el atacante tenga la intención de atacar. En el caso de las plataformas petrolíferas la CIJ hizo referencia a este requisito cuando se ocupó de la cuestión de si EE.UU. fue capaz de demostrar que algunas de las acciones de Irán fueron 'dirigidas específicamente' hacia los EE.UU. o que Irán tenía 'la intención específica' de dañar a los buques de los Estados Unidos." (E. Wilmshurst, Principles of International Law on the Use of Force by States In Self-Defence, (Londres: Chatham House, 2005), pp. 5-6).

[182] Hathaway et al., supra nota 15, p. 846. Para Moore, el artículo 51 de la Carta responde a esta interpretación (Moore, supra nota 29, pp. 223-257, pp. 247-248).

[183] Ibíd., pp. 845-846.

[184] Ibíd., p. 847. En el mismo sentido, Weissbrodt, supra nota 16, p. 363.

la perspectiva del daño físico porque "las redes de mando y control son un objetivo importante y los ataques a ellas no necesitan producir daños físicos."[185] Sin embargo, aquella tesis es también controvertida porque coincide con el criterio del uso de la fuerza y no hay acuerdo sobre si dicho criterio sirve para calificar la existencia de un ataque armado o de un uso de la fuerza o, si lo es para ambos, donde sitúa el límite entre uno y otro. Gervais entiende que se produce el primero si hay destrucción de vidas o de objetos.[186] Dinstein sostiene que "cada vez que un resultado letal para los seres humanos o grave destrucción a la propiedad es engendrada por un uso ilegal de la fuerza por el Estado A contra el Estado B, ese uso de la fuerza se va a calificar como un ataque armado"[187]. En su opinión, "desde un punto de vista jurídico, no hay ninguna razón para diferenciar entre los medios de ataque electrónicos y cinéticos"[188]. Robertson sostiene también que "Es indiferente si el modo de ataque es cinético o electrónico, aunque el primero puede ser más objetivable, ya que es más destructivo y puede causar efectos más duraderos"[189]. No es, en cualquier caso, un tema resuelto a diferencia de lo que ocurre con la agresión que concita un mayor grado de consenso.

D. La agresión

La agresión es una modalidad de uso de la fuerza prohibida por el derecho internacional que ha sido objeto de definición en 2010 en la Conferencia de Kampala[190]. Con anterioridad, además de los trabajos de la Comisión de Derecho Internacional[191], la resolución 3314 (XXIX) de la AGNU define en su artículo 1 la agresión como "el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de Naciones Unidas, tal como se enuncia en la presente definición."[192]El artículo 3 ejemplifica los casos posibles

[185] Lewis, supra nota 5, p. 8.
[186] M. Gervais, "Cyber Attacks and the Laws of War", Berkeley Journal of International Law, Vol. 30 (2012), p. 543.
[187] Dinstein, supra nota 142, p. 100.
[188] Ibíd., p. 103.
[189] Robertson, supra nota 120, p. 132.
[190] Sobre este tema puede verse E. Salmón y L. Bazay, El crimen de agresión después de Kampala: soberanía de los estados y lucha contra la impunidad (Lima: Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú (IDEHPUCP) 2011). Online: http://www.iccnow.org/documents/El_crimen_de_agresion_despues_de_Kampala.pdf.
[191] Ibíd., p. 35.
[192] Según el artículo 2, "El primer uso de la fuerza armada por un Estado en contravención de la

subrayando que son independientes de la existencia o no de declaración de guerra. No se trata, como indica el artículo 4, de una enumeración exhaustiva porque el Consejo de Seguridad podrá determinar otros actos constitutivos de agresión. Esta previsión se justifica porque, en realidad, la competencia para proceder a esa calificación corresponde al Consejo de Seguridad, de conformidad con la Carta de Naciones Unidas. Por ello, la declaración de la AGNU definiendo y tipificando algunos de los supuestos de agresión posibilita la existencia de desacuerdos o de escasas coincidencias en la práctica entre los criterios de la AGNU y la actuación del Consejo de Seguridad. Ni se puede excluir que este órgano califique como agresión un acto no contemplado en la resolución, porque obviamente puede hacerlo, ni el Consejo de Seguridad va a seguir necesariamente los parámetros establecidos en la misma, entre otros motivos, porque para calificar la agresión necesita el voto favorable de nueve de sus miembros incluidos los permanentes.

Esta situación se complica tras la Conferencia de Kampala.[193] La reforma del artículo 8 bis relativo al crimen de agresión del Estatuto de Roma reproduce la declaración de la AGNU. Son dos las consecuencias principales: una, pasa a ser una disposición de un tratado obligatorio para sus Estados Parte que no son todos los del Consejo de Seguridad; y, dos, dentro del mismo, se atribuye a la CPI la competencia para determinar la existencia del crimen de agresión. Ello supone que, simultáneamente, pueden darse tres órdenes de problemas en cuanto a la conciliación de las funciones de los órganos implicados. El primero, menos complicado porque se sitúa entre el contenido de una resolución y el de la Carta y se resuelve a favor del órgano competente, entre lo que opina la AGNU y el Consejo de Seguridad. El segundo es algo más complejo porque se trata de dos acuerdos internacionales, aunque la Carta tiene primacía y el Estatuto no obliga aún a todos los miembros del Consejo de Seguridad, entre este órgano y la CPI; y el tercero, no hay que descartarlo, un desacuerdo a tres bandas entre esas instituciones sobre la calificación o no de un hecho como agresión. La lectura de las

---

Carta constituirá prueba prima facie de un acto de agresión, aunque el Consejo de Seguridad puede concluir, de conformidad con la Carta, que la determinación de que se ha cometido un acto de agresión no estaría justificada a la luz de otras circunstancias pertinentes, incluido el hecho de que los actos de que se trata o sus consecuencias no son de suficiente gravedad".

[193] H.H. Koh y T.F. Buchwald, "The Crime of Aggression: The United States Perspective", The American Journal of International Law, Vol. 109, No. 2 (Abril 2015), pp. 257-295. DOI: 10.5305/amerjintelaw.109.2.0257.

disposiciones contenidas en los artículos 15 bis y 15 ter del Estatuto de Roma sobre el ejercicio de la competencia respecto del crimen de agresión ilustran sobre la compleja cohabitación entre la CPI y el Consejo de Seguridad. Aunque la competencia de la CPI se circunscribe a la responsabilidad penal individual, mientras que el Consejo de Seguridad es competente para declarar la existencia de un acto de agresión, no ha de extrañar que se puedan producir solapamientos, incluso, contradicciones entre la actuación de una y de otro, aunque sólo sea por el mero hecho de que son órganos distintos en su origen, composición, naturaleza, funciones y objetivos. Sin embargo, hay, al menos, en este caso, una definición formalizada jurídicamente en un tratado.

El nuevo artículo 8 bis del Estatuto de Roma define el crimen de agresión en los siguientes términos: "una persona comete un "crimen de agresión" cuando, estando en condiciones de controlar o dirigir efectivamente la acción política o militar de un Estado, dicha persona planifica, prepara, inicia o realiza un acto de agresión que por sus características, gravedad y escala constituya una violación manifiesta de la Carta de Naciones Unidas". El apartado 2 contiene el concepto de "acto de agresión" de la resolución 3314 (XXIX). La diferenciación entre acto y crimen de agresión permite individualizar las responsabilidades respectivas del Estado y del individuo, siendo ésta una línea de actuación que podría explorarse en las demás dimensiones del uso de la fuerza, y no sólo la agresión, por las posibilidades que ofrece de otorgar un trato diferenciado a cada uno de esos actores, conforme a sus respectivos estatutos jurídicos, respecto de una acción igualmente reprobable en ambos casos, pero desde distintas perspectivas.

Desde ese marco normativo, la posibilidad de calificar un ciberataque como un acto de agresión depende de las siguientes variables. Desde el punto de vista subjetivo, los autores de esa calificación pueden ser el Consejo de Seguridad que tiene la competencia para determinar la existencia de un acto de agresión y la CPI que decide sobre el crimen de agresión. No hay que descartar un pronunciamiento de la CIJ, pero habría de ser en un contexto en el que no interfiera con las competencias de la CPI. Desde el punto de vista del contenido, los actos susceptibles de ser calificados como agresión a título ilustrativo en la declaración de la AGNU y en el Estatuto de Roma están descritos en clave cinética pensando en el mundo físico y no son

fácilmente extrapolables al contexto virtual. La lectura de esas disposiciones recogidas en el artículo 8 bis .2 permite identificar tres posibles situaciones:

Acciones que, en principio, sólo pueden ser cinéticas y parece excluida la modalidad cibernética. Es el caso de las que se encuentran en el apartado e) ("La utilización de fuerzas armadas de un Estado, que se encuentran en el territorio de otro Estado con el acuerdo del Estado receptor, en violación de las condiciones establecidas en el acuerdo o toda prolongación de su presencia en dicho territorio después de terminado el acuerdo") y en el apartado g) ("El envío por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación en dichos actos");

Acciones cuyo componente físico territorial tiene una presencia tan significativa que, salvo una interpretación muy extensiva, resulta difícil imaginar una dimensión cibernética como ocurre en el caso del apartado a) ("La invasión o el ataque por las fuerzas armadas de un Estado del territorio de otro Estado, o toda ocupación militar, aun temporal, que resulte de dicha invasión o ataque, o toda anexión, mediante el uso de la fuerza, del territorio de otro Estado o de parte de él") y el apartado f) ("La acción de un Estado que permite que su territorio, que ha puesto a disposición de otro Estado, sea utilizado por ese otro Estado para perpetrar un acto de agresión contra un tercer Estado"); y

Acciones en las que una interpretación analógica de la norma permitiría englobar la opción cibernética en los apartados b) ("El bombardeo, por las fuerzas armadas de un Estado, del territorio de otro Estado, o el empleo de cualesquiera armas por un Estado contra el territorio de otro Estado bombardeo"), c) ("El bloqueo de los puertos o de las costas de un Estado por las fuerzas armadas de otro Estado") y d) ("El ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres, navales o aéreas de otro Estado, o contra su flota mercante o aérea").

A pesar de ser una categoría definida jurídicamente, lo que refleja un consenso estimable, el concepto de agresión no está exento de problemas y plantea algunos adicionales en el caso del ciberespacio por la dificultad de extrapolar los supuestos ejemplificados en la norma a

este otro contexto. Esa dificultad, a su vez, sólo puede complicar aún más la calificación misma de un acto cibernético como agresión, ya sea acto o crimen, en el marco del tripartito institucional que, de un modo y otro, se puede pronunciar en ese sentido. Si es difícil que exista una proximidad o una coincidencia de pareceres en el mundo físico, será indudablemente más complejo en el mundo virtual.

En realidad, y con independencia del valor evidente que tiene a otros efectos, la articulación de los conceptos de acto de agresión y de crimen de agresión constituye una solución potencialmente extrapolable al problema que plantea el ascenso de los actores no estatales al terreno de la conflictividad internacional y la necesidad de diferenciar su estatuto respecto al de los Estados. Es preciso articular una fórmula más adecuada que la desarrollada hasta ahora mediante la interpretación extensiva de las excepciones al principio de prohibición del uso de la fuerza porque tampoco la dimensión subjetiva de este principio está exenta de problemas.

VII. EL ELEMENTO SUBJETIVO

El principio del artículo 2.4 se dirige a los Estados y se sitúa en el ámbito concreto de sus relaciones internacionales, esto es, debe tratarse de una acción atribuible a un Estado y dirigida contra otro Estado. Como explica Melzer, "el uso de la fuerza (incluso a través ciberoperaciones) por hackers individuales y otros actores no estatales puede ser relevante en virtud del derecho internacional humanitario y, en algunos casos, el derecho penal internacional, pero no está prohibido por el artículo 2.4 de la Carta de Naciones Unidas."[194] Moore añade que "los actores no estatales no pueden violar normas del derecho internacional consuetudinario en contra del uso de la fuerza justificada por el artículo 2.4 de la Carta de Naciones Unidas a menos que se pueda demostrar una clara relación con un Estado."[195]

En realidad, aunque el discurso se ha extendido a los actores no estatales como una respuesta al terrorismo internacional[196], pueden ser autores de un ciberataque armado y de un crimen de agresión, pero no se les puede atribuir la autoría de una amenaza o un uso de la fuerza en el sentido del artículo 2.4 de la Carta porque, para ello, el autor y la

[194] Melzer, supra nota 74, p. 10.
[195] Moore, supra nota 29, p. 244.
[196] Supra nota 109.

víctima han de ser Estados. Cada una de esas dimensiones plantea una problemática distinta en el ciberespacio por sus propias características y funcionamiento.

A. El ciberataque contra un Estado

El uso o la amenaza de la fuerza deben tener como destinatario a un Estado para encajar en la previsión del artículo 2.4. Partiendo de la base de la presencia del componente objetivo de ese principio -que es un ciberataque considerado uso o amenaza de la fuerza-, el destinatario de la acción puede ser cualquiera de los componentes del Estados, esto es, su organización, su territorio y su población. El Estado es víctima en el sentido del artículo 2.4 en los siguientes supuestos:

El ciberataque se dirige contra la organización del Estado tanto interna, como externa. El conjunto de los componentes y bienes materiales que forman la organización del Estado es relativamente fácil de identificar de manera que una acción cibernética dirigida contra ellos convierte en víctima al Estado. Ello incluye las estructuras físicas que sustentan la actividad cibernética del Estado y, por analogía, se aplicaría también a sus componentes virtuales, tanto si se encuentran en el propio territorio, como si se localizan fuera o se proyectan en el mundo virtual.

El ciberataque se realiza sobre o contra su territorio o, incluso, a través de su territorio en la medida en que constituye una invasión de su soberanía territorial. Las competencias territoriales son soberanas, exclusivas y excluyentes de manera que la afectación del territorio por cualquier acción cibernética de uso o amenaza de la fuerza convierte al Estado en víctima. El concepto de territorio se extiende al espacio terrestre comprendido dentro de los límites de la frontera, al mar territorial y al espacio aéreo suprayacente. Se incluyen, asimismo, las aguas interiores y archipelágicas y la plataforma continental con sus particularidades. En el resto de los espacios marinos, zona contigua y zona económica exclusiva, el Estado podría considerarse víctima del ciberataque si se produce una afectación de las competencias funcionales que tiene reconocidas en esos ámbitos.

El ciberataque se realiza contra la población de un Estado. Como primera providencia, la población del Estado se beneficia de la protección dispensada como consecuencia del ejercicio de las competencias territoriales que se extiende a las personas físicas y

jurídicas, así como a los bienes que se encuentran en el territorio. Un ciberataque contra un miembro de la población del Estado es un ataque a la soberanía territorial del Estado sin otro criterio de distinción. A partir de ahí, hay que diferenciar entre nacionales y extranjeros.

El ciberataque contra el nacional de un Estado, sea persona física o jurídica, y con independencia del lugar de realización, es un ataque al Estado porque, según una normativa consolidada, todos los Estados tienen el derecho a que se respete el Derecho internacional en la persona de sus nacionales. La protección diplomática es el mecanismo que traduce esa ficción jurídica que hace que el daño causado a un nacional se defina como un daño al Estado y que el ejercicio o no de esa protección sea, en Derecho Internacional, desde el punto de vista de su naturaleza, un derecho del Estado y no del particular afectado en cuestión.

En cambio, como es lógico, el ciberataque contra un extranjero fuera del territorio del Estado no puede ser un acto contra el Estado, salvo que, con conocimiento, estuviese actuando en nombre y por cuenta de dicho Estado en cuyo caso se aplicarían las reglas correspondientes de atribución de la responsabilidad.[197]

B. <u>El ciberataque de un Estado</u>

La autoría del ciberataque debe corresponder a un Estado. Melzer explica que "no puede excluirse que el uso de la fuerza por parte de actores no estatales puede constituir una amenaza para la paz y la seguridad internacionales y requiera del Consejo de Seguridad para que adopte o autorice medidas de implementación colectiva. Sin embargo, la prohibición del empleo de la fuerza por y entre los actores no estatales es generalmente una cuestión de derecho penal interno y desde luego no es el objetivo del artículo 2.4 de la Carta de Naciones Unidas."[198]

A esos efectos, la normativa sobre responsabilidad internacional establece los supuestos en los que los actos de agentes, instituciones y órganos del Estado son atribuibles al Estado y determina, también, los casos en los que se le pueden atribuir los actos realizados por particulares. Siguiendo el Manual de Tallin, "el Estado tiene la responsabilidad legal internacional por operaciones cibernéticas

[197] Sobre los CNA realizados contra corporaciones privadas e individuos puede verse Dinstein, supra nota 142, pp. 106-107.
[198] Melzer, supra nota 74, p. 11.

atribuibles a sí mismo y que constituyan una violación de una obligación internacional."[199] El Estado sería el sujeto activo en el sentido 2.4 de la Carta en los siguientes supuestos:

Los ciberataques realizados por sus órganos o agentes cuando tienen esa condición y actúan ejerciendo esa función convierten en autor al Estado. Es una norma consolidada consuetudinariamente y no controvertida.[200] Moore explica que "cuando un agente del gobierno actúa, aun si esos actos no están autorizados, el Estado es legalmente responsable por el efecto de los actos. Un agente de Estado incluye "todas las entidades individuales o colectivas que conforman la organización del Estado y actúan en su nombre."[201]

Los ciberataques realizados por órganos o agentes de otro Estado que han sido puestos a disposición del Estado en cuestión, siempre y cuando tengan esa condición y actúen ejerciendo esa función. Es una regla aceptada de responsabilidad internacional.

Los ciberataques realizados por actores no estatales no son, en principio, atribuibles al Estado. Sin embargo, esta afirmación requiere matizaciones en aquellos supuestos en los que el Estado usa a agentes no estatales que están bajo su control (a), presta asistencia mediante la puesta disposición de su territorio, expresa o implícitamente, (b) o contribuye con otro tipo de asistencia o apoyo (c).

El primer caso obliga a distinguir entre dos grandes categorías: los actores no estatales que actúan de facto como agentes estatales con un vínculo real, aunque no formal, con el Estado y los actores no estatales que actúan a título propio, sin conexión aparente con un país determinado, pero apoyando o siguiendo informalmente sus directrices o líneas de actuación. En este segundo supuesto es prácticamente imposible atribuir responsabilidad al Estado salvo en la medida en que no haya cumplido con su deber de diligencia para evitar las consecuencias eventualmente ilícitas de esa situación.

El primer caso es más complejo. Según Melzer, este supuesto no se puede confundir con los usos "indirectos" de la fuerza porque "el uso de la fuerza por agentes de facto del Estado se atribuye directamente al Estado en cuyo nombre actúan" mientras que "el uso indirecto de la fuerza denota una forma de apoyo por un Estado para los actores no

[199] Regla Nº 6, pp. 29-34.
[200] Gervais, supra nota 186, p. 545.
[201] Weissbrodt, supra nota 16, p. 374.

estatales que utilizan la fuerza en su propio nombre. En consecuencia, el Estado que apoya es internacionalmente responsable por la asistencia prestada, pero no por la fuerza utilizada por las entidades o personas que reciben asistencia"[202]. Por su parte, Weissbrodt sostiene que la clave es el control, que es un término definido jurisprudencialmente, pero sin una respuesta uniforme. En el asunto de las actividades militares y paramilitares en Nicaragua y contra Nicaragua, la CIJ afirma que existe cuando hay una completa dependencia del Estado.[203] En cambio, el Tribunal Penal Internacional para la Antigua Yugoslavia, en el asunto Tadic, considera que "un Estado tiene el control, o las acciones de actores no estatales son atribuibles al Estado, cuando el Estado tiene un rol en la organización, coordinación y prestación de apoyo para el grupo."[204] Moore insiste en la idea de que "las normas de responsabilidad de los Estados afirman que la conducta dirigida o controlada por un Estado será considerada como un acto de un Estado… si la persona o grupo de personas está, de hecho, actuando sobre las instrucciones, o bajo la dirección o control de ese Estado en la realización de esa conducta."[205]

Como explica Kolb, es difícil comparar los criterios de control efectivo de Nicaragua y de control global de Tadic aunque, en realidad, son diferentes porque la operación jurídica en la que se inscriben también lo es, razón por la cual se justifica esa diferenciación de apreciación[206]. No se trata, además, de criterios cerrados sino flexibles, pero que no permiten aventurar los supuestos concretos de atribución o exclusión de la responsabilidad. No obstante, son casos diferentes de aquellos que escapan directamente al control del Estado, incluso, a sus obligaciones de diligencia debida, porque son actos realizados por particulares apoyando unilateralmente una política estatal sin tener ningún vínculo ni conexión con el Estado cuya causa han decidido

---

[202] Melzer, supra nota 74, p. 11.
[203] Weissbrodt, supra nota 16, p. 374.
[204] Ibíd.
[205] En su opinión, "Tiene que haber una relación de hecho específica entre el actor no estatal y el Estado para que sus acciones sean atribuibles al Estado. Puede existir una relación de esa naturaleza cuando los órganos estatales complementan su propia acción mediante el reclutamiento o la instigación de los particulares o grupos que actúan como "auxiliares" manteniéndose fuera de la estructura oficial del Estado. Por lo tanto, 'atribución' requiere (1) actos que califiquen como un ataque armado y (2) que el Estado haya enviado a los actores no estatales o esté involucrado de forma considerable en las operaciones" (Moore, supra nota 29, p. 244).
[206] Kolb, supra nota 89, p. 210.

apoyar mediante las acciones cibernéticas. En este punto, el ciberespacio crea una situación diferente a la del mundo físico porque el entramado y los medios cibernéticos permiten a cualquier individuo intervenir en favor de la causa de un Estado sin apoyo o asistencia del mismo o, incluso, en contra de la opinión de dicho Estado.

En el segundo caso, la afirmación de un posible incumplimiento de sus obligaciones por parte del Estado cuando se trata de ciberataques realizados utilizando su territorio se está convirtiendo en uno de los principales puntos de acuerdo entre los Estados. La idea es combinar la afirmación de la soberanía cibernética y el hecho de que, aún siendo virtual, los componentes físicos del ciberespacio están localizados desde esa perspectiva, para aplicar un principio que "haría que cada persona, compañía, IP, y país sea responsable de la seguridad de su pedazo de ciberespacio."[207] El Manual de Tallin asume esa regla indicando que un Estado "no permitirá que, a sabiendas, la infraestructura cibernética ubicada en su territorio o bajo su control gubernamental exclusivo sea utilizada para los actos que afectan de manera adversa e ilegalmente a otros Estados". Esta regla se aplica con independencia de la atribución del hecho al Estado porque "no importaría si el Estado estuvo involucrado o es responsable por el ciberataque; el Estado sería responsable incluso si fuera simplemente un santuario para los ataques cibernéticos ilegales contra otros Estados."[208] Gervais considera que el Estado tiene, en esos casos, la obligación "de responder rápidamente a los requerimientos de investigaciones internacionales, embargar y preservar el servidor o los registros del enrutador, permitir y facilitar a las investigaciones internacionales, poner a disposición sus ciudadanos para ser interrogados y procesar a los ciudadanos por delitos específicos"[209].

El informe del GEG de 2015 también asume esta idea que se concreta en dos acuerdos de principio: el primero es que los Estados "no deberían permitir deliberadamente que su territorio fuera utilizado para la comisión de hechos internacionalmente ilícitos mediante la utilización de las TICs"; y el segundo que "deberían atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada con las TICs originada en su territorio contra infraestructuras

[207] Moore, supra nota 29, p. 223.
[208] Regla Nº 5, pp. 26-29.
[209] Moore, supra nota 29, p. 223.

fundamentales de otro Estado, teniendo debidamente en cuenta la soberanía."[210] No obstante, el informe precisa que "la determinación de que cierta actividad relacionada con las TICs se ha puesto en marcha o se ha originado de alguna manera en el territorio o en la infraestructura de las TICs de un Estado podría no ser suficiente en sí misma para atribuir dicha actividad a ese Estado". Por ese motivo se acuerda que "las acusaciones de organizar y cometer hechos ilícitos dirigidas contra los Estados deberían estar fundamentadas."[211]

En el tercer supuesto se plantea si son atribuibles al Estado los actos realizados con su simple apoyo por parte de actores no estatales. Melzer sostiene que "mientras que los Estados que proporcionan apoyo a este tipo de actores no estatales en general, no se hacen responsables de las operaciones cibernéticas llevadas a cabo por este último, su ayuda puede en sí misma equivale a un uso "indirecto" de la fuerza en contravención del artículo 2.4 la Carta de Naciones Unidas y el principio de no intervención"[212]. En este sentido, Moore deja claro que "las normas de responsabilidad internacional no tienen en cuenta acciones llevadas a cabo por actores no estatales que actúan fuera del ámbito de un Estado, como las organizaciones terroristas como Al Qaeda o los activistas colectivos como Anonymous". Sin embargo, como advierte el autor, ello no excluye la obligación de diligencia debida que implica que "un Estado puede ser considerado responsable por los actos de actores no estatales que se producen dentro de su Estado cuando no toma medidas razonablemente disponibles para detener tales actos en violación de sus obligaciones con otros Estados"[213]. En ese sentido se pronuncia también Gervais para quien "la respuesta internacional también puede ser explicada en base a que proteger a los autores de los ataques del 11- S es similar a respaldar sus acciones, lo que implica que el Estado es consciente de que está violando su obligación de prevenir ataques desde su territorio."[214]

Por su parte, el informe del GEG de 2015 recoge varios puntos de consenso que ponen de relieve la importancia acordada al tema[215],

[210] A/70/174, 22 de julio de 2015, pp. 10-11.
[211] Ibíd., p. 17.
[212] Moore, supra nota 29, p. 244.
[213] Ibíd., p. 245.
[214] Gervais, supra nota 186, p. 549.
[215] En particular, destacan los siguientes: Un Estado no debería realizar ni apoyar de forma deliberada actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañaran intencionadamente infraestructuras fundamentales

destacando, en concreto, dos compromisos que se proponen a los Estados: por una parte, no deben recurrir a terceros para cometer hechos internacionalmente ilícitos mediante las TICs y; por otra, deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar en virtud del derecho internacional. Efectivamente, el problema dista mucho de estar resuelto con estas reglas generales porque en el ciberespacio convergen los problemas de atribución y trazabilidad de los ciberataques.[216]

C. Trazabilidad y atribución

A diferencia de lo que ocurre con carácter general en el marco del Derecho internacional Público, donde la autoría determina la atribución que, a su vez, establece la responsabilidad, en el mundo virtual, la situación es más compleja.

El ciberespacio complica la determinación de la autoría porque, además de caracterizarse en términos generales por la presencia del anonimato y la opacidad, exige dos operaciones y presenta dos aspectos diferentes: la trazabilidad, de carácter técnico y la atribución de naturaleza jurídica.[217]

La trazabilidad constituye un problema principal en la determinación de la autoría de un Estado. Como explica Moore, "Si bien puede parecer bastante sencillo que un Estado sea responsable por la acción de sus agentes, la dificultad radica en la naturaleza sutil de los ataques cibernéticos. Por ejemplo, las tecnologías de ataque cibernético no son tan fácilmente detectables como lo son las armas químicas o nucleares. En cambio, 'una nación [puede] ocultar sus armas informáticas en memorias USB o CD en cualquier parte del país.' Tal vez por esta razón, hasta la fecha, ningún ataque cibernético se ha atribuido a un Estado de

---

que prestan servicios al público o dificultaran de otro modo su utilización y funcionamiento; Los Estados deberían tratar de evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TICs, así como el uso de funciones ocultas y dañinas; Los Estados no deberían realizar ni apoyar de forma deliberada actividades que dañaran los sistemas de información de los equipos autorizados de respuesta a emergencias (a veces conocidos como equipos de respuesta a emergencias cibernéticas o equipos de respuesta a incidentes de seguridad informática) de otro Estado. Un Estado no debería utilizar equipos autorizados de respuesta a emergencias para participar en una actividad internacional malintencionada. (A/70/174, 22 de julio de 2015, pp. 10-11).

[216] Ibíd., p. 17.

[217] Sobre los problemas de atribución y responsabilidad, véase Shackelford, supra nota 21, pp. 231 y ss.; S.J. Shackelford y R.B.M. Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", Georgetown Journal of International Law, vol. 42 (2011), pp. 971-1016.

forma concluyente. (…) La comunidad internacional también debe abordar cómo los Estados neutrales están implicados cuando los agentes de un Estado utilizan las redes de un Estado neutral."[218]

La preocupación de los Estados sobre este problema es puesta de relieve en sus observaciones a la AGNU. EEUU advierte, en particular, que "La ocultación de la identidad se ve agravada por la ocultación del motivo que inspira la intrusión en el ciberespacio. La delincuencia organizada y otros individuos o grupos pueden actuar para promover sus propios intereses, pero también pueden ser captados por actores estatales y no estatales, para que sirvan como sustitutos visibles. El hecho de que en un momento concreto no se pueda atribuir un grado elevado de confianza y pueda haber suplantación de identidad crearía incertidumbre y confusión para los gobiernos, con el consiguiente aumento del potencial de inestabilidad ante la crisis, respuestas mal orientadas y la pérdida de control de la escalada en los incidentes cibernéticos graves"[219]. En sus observaciones identifica cuatro actores: los Estados, los delincuentes, los terroristas y, finalmente, los llamados "sustitutos" que se definen como "los individuos o grupos que ejecutan actividades malintencionadas en línea en nombre de otros, sean actores estatales o no estatales, con fines lucrativos o por motivación nacionalista o de otra índole política."[220] La doctrina incluye las siguientes categorías: usuarios, operadores y administradores, hackers hostiles y no hostiles, ciber combatientes, cibercriminales, ciberterroristas, ONG, gobiernos.[221]

---

[218] Moore, supra nota 29, p. 243.
[219] Observaciones EEUU a la AGNU; doc A/66/152, p. 13.
[220] Observaciones EEUU a la AGNU; doc A/66/152, p. 14.
[221] Son definidos del siguiente modo: "Usuarios, operadores, administradores: Estos grupos no tienen una influencia negativa sobre la seguridad cibernética. Son actores que proporcionan legalmente recursos del ciberespacio o los consumen. Los hackers no hostiles: Como regla general, sin intención tienen un impacto negativo sobre la seguridad cibernética, si lo están haciendo 'sólo por diversión' (por una apuesta o disputa, por ejemplo) o para presumir. Los hackers hostiles: Sus motivos incluyen la venganza, la envidia y el interés propio. Los combatientes de la red: Pueden tener un impacto positivo o negativo sobre la seguridad cibernética para sus propios fines. En la aplicación de la ley en la red, las actividades son prescritas por la ley y financiadas por el Estado. Otros combatientes pueden ser financiados secretamente por entidades públicas o privadas que tienen agendas encubiertas. Los criminales cibernéticos: son criminales que utilizan las armas cibernéticas como sus armas preferidas. Los terroristas cibernéticos: son terroristas que utilizan las armas cibernéticas como sus armas preferidas. Los gobiernos: órganos del Estado que pueden utilizar el ciberespacio para fines político-militares. Las organizaciones no gubernamentales: Grupos que pueden utilizar el ciberespacio para promover sus agendas políticas". (T. Lan, Z. Xin, H. Raduege, D.I. Grigoriev, P. Duggal y S. Schjølberg, Global Cyber Deterrence. Views from China, the U.S., Russia, India, and Norway (Nueva York: EastWest Institute, 2010) p. 6).
http://www.eastwest.ngo/sites/default/files/ideas-files/CyberDeterrenceWeb.pdf.

Desde esta perspectiva, hay dos cuestiones abiertas: la situación de los actores no estatales que, como ya se ha dicho, habría que encauzar a través de modalidades específicas de persecución y sanción; y la necesidad de articular mecanismos también específicos para resolver los problemas que plantea la atribución de las acciones cibernéticas a los Estados.

VIII. CONCLUSIONES

La aplicación del principio de prohibición del uso y de la amenaza de la fuerza a través del ciberespacio plantea problemas jurídicos, políticos y técnicos cuya solución no sólo es necesaria sino absolutamente ineludible.

El análisis de la experiencia internacional muestra la existencia de diversas modalidades de acción cibernética susceptibles de ser consideradas amenaza o uso de la fuerza. A pesar de las dificultades que plantea la atribución de esos ciberataques a los Estados, cabe identificar cuatro categorías diferentes en su contenido y en sus consecuencias. El uso subrepticio del arma cibernética es una práctica cuyo mayor peligro reside precisamente en el hecho de que propicia el recurso por parte de los Estados a medios poco ortodoxos de solución de la conflictividad interestatal y sacraliza la impunidad cibernética por tratarse del supuesto en el que, a pesar de las fundadas sospechas, resulta más difícil la atribución de los hechos a un Estado. El uso paralelo de la acción cibernética en el marco de un conflicto armado supone una cierta ruptura o, al menos, exclusión de la aplicación del derecho internacional de los conflictos armados no sólo en cuanto al estatuto de los particulares autores de ciberataques bajo el control o no de alguna de las partes en conflicto sino, también, cuanto a las reglas de neutralidad y los principios de distinción o de proporcionalidad, entre otros. El uso combinado del ciberataque admite una calificación más rápida y automática como uso de la fuerza cuando concluye en la acción cinética, pero, cuando no es así, también plantearía problemas de categorización, incluso, siendo un supuesto claro de uso de la fuerza, si sus efectos no son equiparables a los actos de naturaleza cinética. Por último, el uso alternativo del arma cibernética plantea el inconveniente de la calificación que, para el autor, se suma a la ventaja de su efectividad

convirtiéndola en una opción mucho más atractiva que el arma convencional, lo que, a su vez, propicia una generalización en su uso sin que se hayan arbitrado los mecanismos necesarios para proceder a su identificación como modalidad prohibida de uso de la fuerza.

El estudio del debate político sobre el alcance y el contenido de la normativa internacional en el ciberespacio ponen de manifiesto que los Estados han confirmado la aplicación de los principios estructurales recogidos en la Carta de Naciones Unidas. Sin embargo, la prohibición del uso o de la amenaza de la fuerza no ha merecido la misma atención que otros, ni ha obtenido el grado de consenso que sería deseable a esos efectos. Las referencias son escasas y apuntan en mayor medida a la defensa de la interpretación propia de las excepciones a ese principio que a la adaptación del mismo al contexto ciberespacial.

Esa situación se explica porque es un principio extremadamente controvertido en el discurso jurídico-político donde coexisten, sin ser coincidentes o llegando, incluso, a ser incompatibles, diferentes concepciones del mismo principio y de sus excepciones. La interpretación político-institucional se ha situado más en el terreno de la justificación de las excepciones a la prohibición del uso de la fuerza que en la afirmación de su validez mediante su adaptación a las nuevas condiciones que impone el ciberespacio. La articulación de doctrinas, como la legítima defensa anticipatoria o el ascenso de los particulares a la categoría de destinatarios del ejercicio del derecho a la legítima defensa, entre otras, ofrecen una respuesta coyuntural a un problema que se adivina estructural y conduce a una cierta subversión del sistema porque modela el principio y sus excepciones en función de parámetros no interestatales pero que, a la postre, acabarán también siendo extrapolados al marco interestatal. La interpretación pretoriana no es seguida en la práctica estatal e institucional del Consejo de Seguridad. La doctrina bascula entre la revalorización del principio y la justificación de sus excepciones tratando, en ocasiones, de legitimar el discurso político.

Más allá de lo irrazonable de esta situación, por sí misma, el problema de fondo radica en que ese debate no parece reconocer la magnitud de los cambios que se están produciendo globalmente en el marco de la seguridad internacional y que advierten sobre nuevas y

diferentes modalidades de conflictividad política y social[222] respecto de las cuales la prohibición del uso y de la amenaza de la fuerza sólo puede ser parcialmente efectiva. Es efectiva sólo en la medida en que dirige una prohibición a los Estados que, siendo lógicamente importantes, no son ya los únicos actores. No obstante, poco puede hacer frente a los actores no estatales como tampoco puede hacer mucho el recurso al ejercicio de la legítima defensa respecto de ellos cuando es un mecanismo pensado para un contexto interestatal. La interpretación extensiva de las excepciones a ese principio para conjurar esas otras amenazas, que caracteriza la práctica de los Estados con cierto apoyo doctrinal, debe dejar paso a una interpretación más cercana a la letra y al espíritu de la norma. Esta interpretación, además de concitar por principio un mayor acuerdo, puede servir para avalar la necesidad de crear mecanismos nuevos específicos para hacer frente a las amenazas procedentes de los actores no estatales desde una perspectiva transnacional en lugar de otorgarles un estatuto cualificado a nivel internacional.

Una vez circunscrito el alcance y el contenido del principio a sus términos primigenios, la determinación de su contenido material en el ciberespacio es también una cuestión controvertida. La calificación del arma cibernética es un paso previo que, sin embargo, no contribuye decisivamente a resolver los dos problemas principales identificados en este contexto: la calificación de las acciones como uso de la fuerza, ataque armado o agresión y la diferenciación entre cada una de esas categorías. No hay acuerdo en sede doctrinal entre las diversas opciones que, al final, se reconocen dotadas de la suficiente relatividad para permitir un margen de apreciación tan amplio que las hace poco operativas. El caso de la agresión, sin embargo, es diferente porque se articula a través de dos conceptos, el acto y el crimen, que permiten calificar una realidad materialmente similar, pero subjetivamente diferenciada al atribuir un estatuto distinto a los actores estatales y no estatales. La necesidad de una aproximación similar en el caso del uso de la fuerza y del ataque armado se pone de manifiesto analizando el elemento subjetivo de dicho principio.

---

[222] M. ROBLES CARRILLO, "El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico", Boletín del Instituto Español de Estudios Estratégicos (IEEE), Nº 124 (2015), pp. 6-12.

Desde esa perspectiva, el artículo 2.4 se sitúa en un marco interestatal prohibiendo un ciberataque de un Estado contra otro Estado. Prohíbe el ciberataque dirigido contra la organización misma o los bienes del Estado, su población o su territorio que cubre todo lo que se encuentra dentro del mismo. Prohíbe el ciberataque realizado por un Estado siendo la determinación de su autoría complicada por razones técnicas derivadas de la problemática de la trazabilidad y jurídicas por la atribución de la responsabilidad. Los ciberataques dirigidos contra la población o contra los nacionales de un Estado encajan dentro de la prohibición del artículo 2.4 porque, en el primer caso, afectarían a sus competencias territoriales, mientras que en el segundo lo harían con las personales con independencia del lugar de comisión de la acción. La situación es diferente cuando se trata del autor y no de la víctima.

El ciberataque realizado por un actor no estatal no es contrario al principio de prohibición del uso y de la amenaza de la fuerza del artículo 2.4 de la Carta, aunque sí puede legitimar el ejercicio del derecho a la legítima defensa individual o colectiva porque el artículo 51 de la Carta no precisa la autoría. La práctica en materia de lucha contra el terrorismo internacional se fundamenta básicamente en esa disposición. Hay que plantearse, no obstante, que lamentablemente se trata de un fenómeno que ya no es nuevo ni tampoco aislado y que, además, en no pocas ocasiones implica a nacionales del propio Estado. Hay que preguntarse si, en ese contexto, el recurso de los Estados a la legítima defensa, como excepción a la prohibición del uso de la fuerza, es realmente una solución válida, eficaz y potencialmente duradera o si, por el contrario, ha llegado el momento de arbitrar modalidades específicas de acción no sólo contra el terrorismo, sino frente al conjunto de la criminalidad internacional que constituye una de las expresiones negativas más graves y preocupantes en el ciberespacio.

La gravedad de esas acciones no justifica un cambio de los parámetros de organización social en torno al modelo del Estado y a un ordenamiento jurídico internacional estructurado sobre el principio de que sus sujetos son los Estados, mientras que los actores no estatales, en particular, los individuos, están sometidos a un régimen jurídico distinto. Este régimen combina normas nacionales, normas internacionales como la Convención sobre la Ciberdelincuencia del Consejo de Europa y normas transnacionales como aquellas que articulan una cooperación transfronteriza en la lucha contra la

delincuencia internacional, por ejemplo, en el marco de Naciones Unidas. Es necesario mejorar esas normas y los mecanismos de garantía de las mismas. Como primera providencia sería preciso articular un sistema de delimitación horizontal de competencias entre los Estados para la determinación de la jurisdicción competente en caso de que se produzcan conflictos positivos o negativos en el ejercicio de esa jurisdicción y sería aconsejable, asimismo, la creación de un tribunal ad hoc o, en su caso, la extensión de las competencias de la CPI, ejerciendo una jurisdicción subsidiaria y complementaria respecto de los Estados en relación con las acciones de naturaleza coercitiva de los actores no estatales.

Entiendo que desvirtuar el principio de prohibición del uso y de la amenaza de la fuerza ampliando sus excepciones para hacer frente a las amenazas procedentes de los actores no estatales es una solución errónea, coyuntural y escasamente efectiva que, además, impide centrarse en la cuestión realmente importante desde esa perspectiva que es establecer el diseño de ese principio en el ciberespacio.

El debate internacional sobre la prohibición del uso y de la amenaza de la fuerza en el ciberespacio se encuentra lastrado, desde hace años, por las diferencias de interpretación ya existentes en el mundo físico en torno a ese principio y sus excepciones[223]. El problema es que el ciberespacio introduce un cambio de paradigma en dicho principio que exige plantearse y resolver aspectos esenciales del mismo tanto en su dimensión objetiva, articulando los conceptos de arma cibernética, uso de la fuerza armada o ciberataque armado y la diferenciación entre cada una de esas categorías, como en su dimensión subjetiva, estableciendo los mecanismos para la atribución y la determinación de la responsabilidad por las acciones cibernéticas. Es urgente abordar ese debate cambiando el planteamiento seguido hasta ahora porque, como subraya acertadamente Das, "cuanto más tarde la comunidad internacional en resolver esta controversia, más atractivas y lucrativas se tornarán, para los Estados beligerantes y los actores no estatales , las

[223] Lotrionte afirma que "Hay un creciente consenso internacional de que las cuestiones del derecho internacional se aplican en el dominio cibernético, pero la mayoría de los detalles acerca de cómo se aplican permanece indeterminado. Muchos Estados han considerado la aplicación de las leyes existentes, incluida la Carta de Naciones Unidas y el derecho de los conflictos armados. Y mientras está firmemente establecido en los EE.UU. que la Carta de Naciones Unidas y el derecho de los conflictos armados se aplican a la guerra cibernética, el reto es determinar exactamente cómo se aplica y conseguir un acuerdo internacional sobre estas cuestiones" (Lotrionte, supra nota 5, p. 14).

operaciones cibernéticas ofensivas que socavan el umbral de 'uso de la fuerza'"[224].

El ciberespacio impone la necesidad de un cambio en la interpretación del principio de prohibición del uso y de la amenaza de la fuerza realizada, fundamentalmente, en las dos últimas décadas. Esa línea de actuación, contradictoria y controvertida, está sustentando un debate que impide reconocer el problema de fondo que plantea el ciberespacio, esto es, un uso creciente de las capacidades y de la fuerza cibernética que no es objeto de una regulación atendiendo a sus propias singularidades, a pesar de que los componentes esenciales de ese principio no son objeto de un consenso y a pesar, también, de que su uso constituye una serie y creciente amenaza para la paz y la seguridad internacional. El discurso ha de centrarse, mejor pronto que tarde, en la determinación de los conceptos de uso y amenaza de la fuerza, ciberataque y ciber agresión, así como en sus diferencias y, paralelamente, en la definición de procedimientos de trazabilidad y atribución que permitan actuar eficazmente contra la amenaza y el uso de la fuerza en el ciberespacio.

[224] Das, supra nota 1, p. 138.