Revista de la Facultad de Derecho de México
Tomo LXXII, Número 283, Mayo-Agosto 2022
DOI:http://10.22201/fder.24488933e.2022.283.83165

La legítima defensa preventiva contra los actores no estatales en el ciberespacio: estudio comparativo de las posiciones de los miembros permanentes del Consejo de Seguridad de Naciones Unidas

The legitime defense against non-state actors in cyberspace: comparative study of the positions of the permanent members of the United Nations Security Council

Borja García Vázquez*

Resumen: La tecnología ha permitido que se desarrollen nuevas formas en el ejercicio de la fuerza, alterando con ello las condiciones en que discurrían los conflictos bélicos. El poder ejecutar un ataque en el ciberespacio, sin capacidad de preverlo con antelación, y la posibilidad de encubrir la identidad del atacante, rompen los principios que han regido para el empleo de la legitima defensa. Esta tecnología ha demostrado estar al alcance de actores no estatales que pueden llegar a comprometer la seguridad nacional, constituyendo una amenaza tangible que plantea la necesidad de conocer la postura que sostienen sobre este particular, los miembros permanentes del Consejo de Seguridad de Naciones Unidas, por su posición privilegiada como garantes de la paz y seguridad internacionales.

* Doctor en Métodos Alternos de Solución de Conflictos por la Universidad Autónoma de Nuevo León (UANL). Profesor de Derecho Internacional Público de la Facultad de Derecho y Criminología de la UANL. Investigador Nacional Nivel 1 (SNI-1). (España) Contacto: <borjagarcia131@gmail.com>.
Fecha de recepción: 17/10/2021. Fecha de aprobación: 01/03/2022.

Palabras clave: legítima defensa; ciberespacio; ciberguerra; ciberterrorismo; actores no estatales.

Abstract: Technology has allowed the development of new forms of use of force, thereby altering the conditions in which war conflicts took place. Being able to carry out an attack in cyberspace, without the ability to foresee it in advance, and the possibility of concealing the identity of the attacker, break the principles that have governed the use of legitimate defense. This technology has proven to be available to non-state actors that may compromise national security, constituting a tangible threat that raises the need to know the position that the permanent members of the United Nations Security Council hold on this matter, for their privileged position as guarantors of international peace and security.

Keywords: legitimate defense; cyberspace; cyberwar; cyberterrorism; non-state actors.

I. Introducción

El presente artículo mostrará el análisis del estado normativo en materia de ciberseguridad (las medidas adoptadas para proteger la población y bienes de un Estado) y ciberdefensa (las pautas que han de contemplar las fuerzas armadas de un Estado, al ejercer la fuerza en el ciberespacio), en los Estados miembros permanentes del Consejo de Seguridad de las Naciones Unidas (en adelante, el Consejo); unido a la confrontación entre la política preventiva ejercida por los Estados, en diálogo con la jurisprudencia internacional, con fundamento adicional en las reglas contenidas en el Manual Tallinn 2.0 (en adelante Manual), el cual, si bien no es un documento oficial, ni representa las posiciones de ningún Estado u Organización Internacional[1], goza de plena capacidad de vinculación por su carácter consuetudinario. Esta afirmación se sustenta, adhiriéndonos a los planteamientos de Cesáreo Gutiérrez Espada, razón que nos lleva a considerar que "cuando una regla del Manual refleje normas no escritas del Derecho Internacional, dicha regla «es», «resulta», legalmente vinculante"[2].

El objetivo central de la investigación, está destinado a evidenciar la inseguridad jurídica que origina la falta de unidad internacional (entre los Estados del Consejo) respecto de los límites del uso de la fuerza y el ejercicio de la legítima defensa, frente a las amenazas provenientes del ciberespacio; considerándose como hipótesis vertebral del estudio, el aprovechamiento oportunista que ofrece el vacío jurídico, en la legitimación de acciones preventivas en beneficio de la protección de los intereses nacionales, en perjuicio del ordenamiento internacional.

---

[1] Schmitt, Michael, N., *Tallinn Manual 2.0 on the international law aplicable to cyber operations*, 2ª ed., Cambridge, Cambridge University Press, 2017, p. 2.

[2] Gutiérrez Espada, Cesáreo, *La responsabilidad internacional por el uso de la fuerza en el ciberespacio*, Navarra, Aranzadi, 2020, p. 34.

II. Identificando la amenaza que enfrenta el derecho internacional en un contexto contemporáneo

La guerra preventiva ha tratado de ser explicada, desde un razonamiento entendible como un acto reflejo del cuerpo humano, en el que se ofrece una respuesta a un ataque (cuando se percibe, y antes de que produzca su impacto), en el que la prevención actúa desde preceptos realistas, en detrimento de las cuestiones morales implícitas a la toma de decisión[3]. Comprende una afirmación explícita a la clásica pregunta acerca de si el fin puede o no, justificar los medios empleados. Son numerosos los ejemplos de políticas de Estado en materia de seguridad (y sin respaldo legal), ejercidas con posterioridad a la Carta.

La dificultad se encuentra hoy en el proceso de desestatalización de la guerra. Un retroceso hasta los albores de la Edad Moderna, en el que el Estado no contaba aún con el monopolio de la guerra, y que comparado con la actualidad, se observa nuevamente las semejanzas a los enfrentamientos previos al siglo XVIII, con una sobreposición de actores privados, paraestatales y estatales, en los distintos conflictos de África y Asia[4]; y el auge de las unidades paramilitares, grupos autónomos conformados por militares licenciados y delincuentes, habitualmente creados por los gobiernos para ejercer la violencia sin responsabilidad[5].

A esta coyuntura, debe agregarse el factor del ciberespacio, al permitir la concurrencia de actores no estatales, que pueden ejercer la fuerza sin que sea posible ligarlos a las órdenes de un Estado específico, como una huida de estos ante los posibles ilí-

---

[3] Walzer, Michael, *Just and Unjust Wars,* New York, Basic Books, 4ª ed., 1977, p. 74.

[4] Münkler, Herfried, *Viejas y Nuevas Guerras: asimetría y privatización de la violencia*, Madrid, Siglo XXI Editores, 2005, p. 3.

[5] Kaldor, Mary, *Las nuevas guerras*, España, Kriterios editores, 2001, pp. 122-123.

citos cometidos por tales grupos. En conjunto, las cualidades de estos nuevos enfrentamientos se resumen en el abaratamiento de los mismos, permitiendo la desestatalización o privatización del conflicto; la desigualdad de fuerza de los contendientes, en el que antiguos elementos estratégicos, como las acciones partisanas y el terrorismo, "han adquirido una dimensión estratégica propia"[6], cuyas lógicas de acción son replicables desde el ciberespacio, permitiendo la deslocalización del conflicto.

Entendida esta realidad, debe comenzarse por ilustrar a qué amenaza se enfrentan hoy los Estados. Para ello, adoptando las ideas de Münkler, puede explicarse como las nuevas guerras son libradas predominantemente por actores paraestatales. Estos, sometidos a influencias extranjeras (por encontrarse integrados en un mundo globalizado, en el que la preponderancia económica ha llevado a que estas actividades sean confundidas con el uso de la fuerza), y sirviéndose de la población joven y desempleada (que excluidos de las posibilidades de trabajo y del consumo de la economía de paz, se inclinan a estas acciones, sin atender al derecho de la guerra ni a ningún código militar), participan en conflictos a largo plazo, en que tratan de minar al enemigo, hasta conseguir un equilibrio de fuerza frente a él[7].

Así, reinterpretando los elementos identificados por Robert Taber respecto de las guerrillas, cuyo objetivo se encuentra en la evasión, entendiendo que "evadirse significa ser capaz de no entrar en combate con el enemigo más que en los tiempos y lugares elegidos para ello (…) y poder lograr siempre superioridad local para luchar con eficacia"[8], podría ofrecerse una nueva lectura contemporánea, respecto de los actores no estatales en el ciberespacio, y su inferioridad ante los medios de que dispone un Estado.

---

6 Münkler, Herfried, *op. cit.,* p. 4.

7 Münkler, Herfried, *op. cit.,* pp. 10-25.

8 Taber, Robert, *La guerra de la pulga: guerrilla y contraguerrilla*, Ciudad de México, Biblioteca Era, 1965, p. 154.

La asimetría de poder puede entenderse tomando el ejemplo de la resistencia iraquí, que fue catalogada de enemigo invisible (por desconocerse su estructura orgánica y sus formas de financiación) sin que ello impidiese demostrar la efectividad en los ataques cometidos contra las fuerzas occidentales[9]. De esta experiencia, podemos encontrar un paralelismo a la forma en que actúan los actores no estatales en el ciberespacio.

La opacidad del ciberespacio es idónea para esta realidad, cuya singularidad fue identificada a finales del siglo XX por los coroneles chinos Qiao Liang y Wang Xiangsui, quienes reconocieron cómo se había comprobado que diversos hackers estaban adoptando un estilo en línea, de guerra de guerrillas[10]; hechos evidenciados en aquella época, a través de la conocida como operación Solar Sunrise, un ciberataque perpetrado en febrero de 1998, por adolescentes estadounidenses e israelíes, contra los sistemas del Departamento de Defensa de los EEUU[11], que supuso para las fuerzas armadas de aquel país, la toma de conciencia sobre el peligro que representaban las vulnerabilidades en el plano informático[12].

Finalizada la guerra fría, puede considerarse que la década comprendida entre 1991 y 2001, fue el de completa hegemonía global de los EEUU, cuya debacle comenzó con los atentados terroristas del 11 de septiembre de 2001. Esta acción, unida a la proliferación de guerras intraestatales interminables, los problemas económicos, y la aparición o el resurgimiento de potencias como

---

9 Verstrynge, Jorge, *La guerra periférica y el islam revolucionario*, Madrid, El viejo topo, 2005, p. 46.

10 Liang, Qiao y Xiangsui, Wang, *Unrestricted warfare*, Panama City, Pan American Publishing Company, 2002, p. 45.

11 The Joint Chief Of Staff, *Information Assurance*, Washington, D.C., The Joint Chief of Staff, 4ª ed., 1999, pp. 1-2.

12 National Committee On America Foreign Policy, "American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy", *American Foreign Policy Interests,* vol. 35, 2013, núm. 1, p. 50.

China (incorporada a la Organización Mundial del Comercio en 2001), ha impedido que EEUU mantenga su liderazgo como única superpotencia; habiéndose producido adicionalmente una deslegitimación del ordenamiento internacional, como consecuencia de su vulneración sistemática (cuyo máximo exponente fue la invasión de Irak en 2003), lo que ha motivado a los nuevos actores, a hacer caso omiso en defensa de sus intereses nacionales (como se demuestra el rechazo por China en 2016 al laudo de la Corte Permanente de Arbitraje, en el caso The Republic of the Philippines v. The People´s Republic of China respecto de la delimitación del mar del sur de China, con fundamento legal en la Convención de las Naciones Unidas sobre el derecho del mar).

El uso de la fuerza debe abordarse desde las coordenadas actuales, en un mundo interconectado y difuso, con múltiples focos de poder e intereses divergentes entre Estados, y elementos ajenos al mismo. Un mundo, en el que en los conflictos se conjugan los caracteres defensivos y ofensivos/ ralentizadores y aceleradores de la postura partisana (dirigida a resistir contra la capacidad de aguante económico y/o político del enemigo), con el terrorismo (que ataca directamente, sirviéndose del miedo que causan sus acciones)[13]; y al que el ciberespacio ofrece una circunstancia agregada, por no precisar de individuos en el escenario de los hechos, posibilitando encubrir la autoría e incluso, pudiendo prescindir del elemento humano para su ejecución, ampliando las oportunidades del elemento sorpresa para atacar, lo que plantea nuevas dudas sobre donde fijar los límites a la legitima defensa.

13 Münkler, Herfried, *op. cit.,* p. 39.

III. La legítima defensa preventiva en un contexto contemporáneo: la posición en ciberdefensa y ciberseguridad de los miembros permanentes del Consejo

EEUU es una nación con experiencia en la amenaza que suponen los ciberataques contra la seguridad nacional, y con amplio recorrido en su estudio académico, entendible por los orígenes de internet en este país. En octubre de 2006, el Bureau of Industry and Security, sufrió un ataque informático identificado como procedente de servidores chinos, que tras obligar a sus trabajadores a desconectar todos los equipos de internet, e impedir la realización de sus funciones, nunca llegó a concretarse la autoría ni la motivación de estos hechos[14]; confirmándose, como si bien el ciberespacio se manifiesta en un plano trascendente a nuestra realidad perceptible, su existencia se sustenta sobre específicos elementos físicos identificables en el territorio de un Estado.

Basándose en este caso, la profesora Susan W. Brenner, expresaba la necesidad de contestar a las siguientes preguntas para ofrecer una respuesta a un ataque, desde el plano de la legalidad: ¿quién lo lanzó?, ¿de qué tipo de ataque se trata?, ¿debe responder al mismo una autoridad civil, militar o ambas?[15]. La réplica a cada formulación, delimitará el rango de acción y la trascendencia de las medidas adoptadas, para llegar a requerir o no, una contestación conforme al legítimo ejercicio de la fuerza. Estas respuestas, serán la ruta de acción para delimitar espacios en el nuevo contexto de zona gris.

En este espacio es donde actualmente transcurren los conflictos, en condiciones de ambigüedad, multidimensionalidad, gradualidad, y confluencia de múltiples intereses interconectados

---

[14] Brenner, Susan W., "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare", *The Journal of Criminal Law & Criminology,* vol. 97, 2007, núm. 2, pp. 379-380.

[15] *Ibidem,* p. 381.

entre sí[16], en tanto que el ciberespacio ha disipado la distinción entre la seguridad externa e interna, representando una amenaza a su conjunto[17]. A ello, debe agregarse la denominada fuerza cero, la situación en que se halla la sociedad internacional, dada la ausencia de liderazgo por un único país, causada por la constante competición entre las naciones, con origen en la inhabilidad de medios políticos y económicos[18].

A pesar de la inexistencia de una autoridad mundial capaz de crear las condiciones de seguridad en este medio, se confirma la necesidad internacional de alcanzar unos mínimos comunes, que garanticen la estabilidad, responsabilidad y transparencia por las actividades en el ciberespacio.

En la *Roundtable Discussion* del *National Committee on America Foreign Policy*, celebrado en octubre de 2012, sus miembros alertaron de cómo "Un ciberataque importante, probablemente estaría asociado con un ataque cinético, y ocurriría bajo un conjunto de circunstancias geopolíticas que indicarían que algo importante está en marcha"[19]; y en todo caso, sin negar las posibilidades devastadoras de un ciberataque de esta magnitud: "Un ataque a este nivel conduciría a las 5D: muerte, destrucción, daño, interrupción y pérdidas económicas devastadoras (death, destruction, damage, disruption, and devastating economic loss)"[20].

En el contexto de los ciberataques, habría de matizar que dependiendo de su graduación y objetivos, podría hablarse de ciberacciones, las cuales, descritas por Sigholm, son consideradas

---

16 Jordán, Javier, "El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo", *Revista española de ciencias políticas,* vol. 48, 2018, pp. 131-133.

17 Brenner, Susan W., *op. cit.,* p. 382.

18 Bremmer, Ian; Roubini, Nouriel, "A G-Zero World", *Foreign Affairs*, 2011. Disponible en: <https://www.foreignaffairs.com/articles/2011-01-31/g-zero-world>.

19 National Committee On America Foreign Policy, *op. cit.,* p. 46.

20 *Ibidem*, p. 51.

como "una colección de actividades predominantemente ilegales en el ciberespacio, llevadas a cabo por actores no estatales, que causan daños o perturbaciones, en la búsqueda de diversos objetivos políticos, económicos o personales"[21]. Se trata del cibercrimen, la comisión de actos criminales aprovechando los sistemas computacionales[22].

La importancia en hacer esta apreciación, responde a lo estipulado por el Manual en su regla 71, párrafo 8: "los actos de recopilación de inteligencia y robo cibernéticos, así como aquellos que implican una interrupción breve o periódica de servicios cibernéticos no esenciales, no califican como ataque armado"[23]. Esto permite diferenciarlo de otros actos, como el ciberterrorismo, que por analogía sería entendible como la utilización de la tecnología de computación para cometer actos terroristas, que pese a no existir una definición unívoca, puede entenderse como:

> Todos aquellos actos delictivos espontáneos o premeditados, que causen muerte, lesiones corporales, destrucción de propiedades públicas y privadas, o que puedan poner en peligro la vida de las personas, con intención de provocar un estado de terror en la sociedad a cualquier escala, sin tener en cuenta las motivaciones étnicas, filosóficas, ideológicas, políticas, raciales, religiosas, o de cualquier otra naturaleza distinta a las anteriormente expuestas, que puedan invocarse para ser justificadas.[24]

La dificultad se encuentra en visibilizar esta distinción, por la concurrencia de actuaciones entre el ámbito criminal y el terrorista, sirviendo de ejemplo la toma masiva de rehenes, una técnica

---

21 Sigholm, Johan, "Non-State Actors in Cyberspace Operations", *Journal of Military Studies,* vol. 4, 2016, núm. 1, p. 6.

22 Brenner, Susan W., *op. cit.,* p. 384.

23 Schmitt, Michael, N., *op. cit.,* p. 341.

24 García Vázquez, Borja, *Vademécum de Derecho Internacional Público,* Ciudad de México, Tirant Lo Blanch, 2020, p. 135.

ya empleada por el terrorismo desde el siglo XIX, con el secuestro en 1859 del pueblo de Harpers Ferry (Virginia), o su modalidad aérea desde la década de 1970[25], que reproduce nuevamente su lógica en el ciberespacio. Nos referimos a los ataques *ransomware*, equivalente a un secuestro electrónico, en los que utilizando un código malicioso (malware), se impide la utilización de un equipo informático hasta no ser pagada una cantidad monetaria establecida por los secuestradores, que permita desbloquear el dispositivo.

Estos hechos se comprueban con el ataque a la ciudad estadounidense de Atlanta (Georgia), en 2018, que ante la demanda de los secuestradores por valor de 50.000 dólares, causó un gasto en las arcas públicas superior a 2 millones de dólares[26], o a la ciudad de Baltimore (Maryland), en 2019, con una pérdida que oscilaría entre los 10 y los 18 millones de dólares[27]. Si en vez de tratarse de la inutilización de los sistemas computacionales de gestión de una ciudad, fuesen los sistemas de guerra electrónica de un Estado (habiendo sido confirmado ser susceptibles de cibersecuestro[28]), se comprende la gravedad de tales actos. Como expresa Remiro Brotóns estas acciones cibernéticas son constitutivas de ataque ar-

---

25 Boot, Max, *Invisible armies*, New York, Liveright, 2013, p. 261.

26 Hay Newman, Lily, "Atlanta Spent $2.6 M to Recover From a $ 52.000 Ransomware Scare", *Wired,* 2018. Disponible en: <https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/> (8 de mayo de 2021).

27 Panda Security, "RobbinHood: the ransomware that exploits its own reputation", *Panda,* 2019. Disponible en: <https://www.pandasecurity.com/en/mediacenter/news/robbinhood-ransomware-notoriety/> (8 de mayo de 2021).

28 Chatham House, *Cybersecurity of Nuclear Weapons Systems*, 2018. Disponible en: <https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf> (9 de mayo de 2021).

mado[29], opinión que secundamos, en la medida en que estas causen la inoperatividad de sectores vitales para el funcionamiento de la sociedad, o amenacen con perturbar el orden público.

La aparente distinción entre un grupo criminal (caracterizado por el predominio de la motivación pecuniaria), frente a uno terrorista (cuyo objetivo es el cumplimiento de un proyecto político o religioso), se difumina dado que ambas figuras delictivas se han servido mutuamente tantos en los medios, como en los fines a conseguir, por lo que la demarcación deberá encontrarse en otros parámetros, atendiendo al ciberespacio; motivo que nos lleva a proponer la magnitud y el respaldo internacional al acto, como elementos calificadores del mismo, ya que dependiendo del grado de afectación de estos a la seguridad nacional (con independencia de la intencionalidad originaria), permitirá diferenciar el ciberdelito, del ciberterrorismo.

El Manual establece la definición del uso de la fuerza en las ciberoperaciones, en la regla 69, entendiendo que: "Una operación cibernética constituye un uso de la fuerza cuando su escala y sus efectos son comparables a las operaciones no cibernéticas que se elevan al nivel de uso de la fuerza"[30]. La graduación de los conflictos tradicionales es igualmente legitima en medios electrónicos, no obstante a los cambios en la percepción causadas por el ámbito digital, que en ningún caso habilitan para actos ilegítimos de la fuerza. Así lo reconoce la regla 70 del Manual, al decir que: "Una ciberoperación, o una operación cibernética de amenaza, constituye un uso ilegitimo de fuerza amenazadora, y si se lleva a cabo, sería un uso ilegal de la fuerza"[31]. La dificultad se da cuando no se conoce la identidad del sujeto que ejercita la fuerza, sin que se produzca una advertencia previa.

---

[29] Remiro Brotóns, Antonio, Riquelme Cortado, Rosa; Orihuela Calatayud, Esperanza, Díez-Hochleitner, Javier, Pérez-Prat Durbán, Luis, *Derecho internacional,* Valencia, Tirant Lo Blanch, 2010, p. 690.

[30] Schmitt, Michael, N., *op. cit.,* p. 330.

[31] *Ibidem*, p. 338.

La regulación del uso de la fuerza en la comunidad internacional, queda regido por lo estipulado en los artículos 2.4 y los preceptos del Capítulo VII de la Carta, junto a lo reconocido por la resolución 3314 (XXIX) de la Asamblea General, al definir la agresión. Teniendo en cuenta estas bases, la regla 71 del Manual dispone como ha de ejercerse el derecho a la legítima defensa: "Un Estado que sea objetivo de una operación cibernética que se eleve al nivel de un ataque armado, puede ejercer su derecho inherente a la legítima defensa. Si una operación cibernética constituye un ataque armado, depende de su escala y efectos"[32]. Si bien a priori no hace referencia a los actores no estatales, el comentario 19 de la regla 71, reconoce como "La práctica estatal ha establecido un derecho de legítima defensa en la fase de operaciones cibernéticas a nivel de ataque armado por parte de actores no estatales que actúan sin la participación de un Estado, como grupos terroristas o rebeldes"[33].

Como expresa Gutiérrez Espada, con esta exposición el Manual aparenta desviarse de lo instituido por el ordenamiento internacional, habiendo autores identificados por él, que critican esta posición por no contemplar una exigencia de mínimos al ejercicio de la fuerza, como sería la ejecución de ciberataques a gran escala[34]. Posicionándonos con el autor, consideramos un error sostener dicha argumentación, en la medida en que las condiciones de los enfrentamientos han mutado, como demuestra el que las acciones tradicionales a gran escala han dado paso a infinitas microacciones, insertas en planes a largo plazo en el nuevo escenario de zona gris.

Una amenaza que es contemplada por los miembros permanentes del Consejo, caracterizado por el reconocimiento común a la importancia que desempeña el ciberespacio y sus tecnologías

---

32 Schmitt, Michael, N., *op. cit.,* p. 339.

33 Schmitt, Michael, N., *op. cit.,* p. 345.

34 Gutiérrez Espada, Cesáreo, *De la legítima defensa en el ciberespacio*, Granada, Comares, 2020, p. 50.

asociadas, en los cambios producidos en el mundo a través de su impacto económico, con la generación de nuevos modelos de negocio, la modernización de las formas de gobierno, y los riesgos hacia los Estados que pueden emanar desde este medio, siendo una variable común a los miembros del Consejo. Esto se deduce del análisis de sus Estrategias de Defensa y Seguridad Nacional, distintos documentos orientadores de la política gubernamental, que establecen los objetivos a lograr y los medios necesarios a emplear, en materia de seguridad y defensa, delimitando la actividad legislativa de los Estados.

La doctrina de los publicistas ha reconocido inherentes al ejercicio de la legitima defensa, los principios de necesidad, proporcionalidad e inmediatez[35], dotados de ambigüedad al no disponer de una declaración unívoca respecto del contenido y límites a los mismos. La argumentación a nuestras palabras, se encuentra en la sentencia de la Corte Internacional de Justicia, caso Nicaragua v. EEUU, de 1986, en cuyo párrafo 237, analizando las actividades de los EEUU, negó la licitud de sus actuaciones respecto de los principios de proporcionalidad y necesidad, ligando este último con el principio de inmediatez, al expresar como las acciones emprendidas por los estadounidenses, habían surtido efecto "varios meses después de que la gran ofensiva de la oposición armada contra el gobierno de El Salvador hubiese sido totalmente rechazada"[36].

Los modos y medios que se dan en los nuevos conflictos, lleva a una fractura en la percepción de estos principios. Esto podría causar que las potencias que dispongan de medios cibernéticos, se sirvan de las nuevas condiciones formuladas por el desvanecimiento de la inmediatez, con la amenaza de incurrir en un uso abusivo de la legitima defensa, debiendo reformularse desde el

35 Remiro Brotóns, Antonio, *op. cit.,* p. 690.

36 International Court Of Justice, *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), judgment of 27 june 1986,* p. 112.

plano jurídico, una concreción de tales principios acorde a las necesidades del ciberespacio.

A) Estados Unidos de América

El liderazgo tecnológico de EEUU en las dos primeras décadas del siglo XXI, ha sido indudable, habiendo tenido paralelamente su consecuente impacto en el plano regulatorio. Sin embargo, la mejora en los sistemas disponibles no basta para garantizar resultados positivos. El desarrollo y la accesibilidad a la tecnología, ha quebrado el paradigma internacional de seguridad, hecho evidenciado en las últimas décadas con la proliferación de actores no estatales.

El Estado Islámico de Irak y el Levante (DAESH o ISIS, de las siglas en árabe o inglés, respectivamente), supuso una novedad respecto de las organizaciones terroristas tradicionales, al constituirse como un proto-Estado con la proclamación por su líder, Abu Bakr al-Baghdadi, del Califato del Estado Islámico, el 26 de junio de 2014; que mediante una estructura teórica logró un control territorial efectivo en espacios de Siria e Irak, con instituciones basadas en su ideario, que permitieron la venta de petróleo y otros recursos extraídos de estos territorios, llegando incluso a acuñar simbólicamente monedas de oro.

Se trató de una situación extraordinaria, como previamente habían supuesto en 2001 los atentados de Nueva York y Washington, definidos por algunos autores como "hiperterrorismo", por el daño mundial masivo causado por estos actos[37]; cuya gravedad originó la aprobación de la resolución del Congreso de EEUU, denominada Authorization for the Use of Force, el 18 de septiembre de 2001, a través del cual se habilitó al presidente estadounidense al empleo de "toda la fuerza necesaria y apropiada" en ejercicio del

[37] Diez De Velasco Vallejo, Manuel, *Instituciones de Derecho Internacional Público,* Madrid, Tecnos, 18ª ed., 2013, p. 1072.

derecho a la legítima defensa en protección de sus ciudadanos[38], razón por la que las ciberoperaciones se engloban dentro de sus facultades[39]. Este acto legislativo fue la consolidación del carácter unilateral, adoptado por EEUU en materia internacional desde el final de la guerra fría, alcanzando su culminación con la invasión a Irak en 2003[40]. Desde entonces, ha sido ejercido sucesivamente por sus presidentes, cuya última representación fue el asesinato selectivo del comandante iraní Qassam Soleimani, con la aprobación por Donald Trump de un ataque aéreo sobre Bagdad, el 3 de enero de 2020[41].

Desde la academia estadounidense se ha argumentado en favor de la legítima defensa, con amparo en el artículo 51 de la Carta, cuando es en defensa de actores no estatales, como sucedió en el supuesto pre 11-S con la intervención de la OTAN en los Balcanes, para garantizar la supervivencia de los kosovares frente a las acciones de los serbios[42]. Hoy, en el ámbito anglosajón, aunque de forma testimonial, se encuentra alguna voz que aboga por el ejercicio de ciberataques contra los campos de prisioneros uigures, en la región china de Xinjiang, como elemento de presión hacia el país asiático, al permitir enviar un mensaje de forma velada (por medio de actos de sabotaje de los elementos de seguridad de esta área, sin que pueda demostrarse la autoría), para poner fin a lo

38 Estados Unidos de América, Ley Pública 107-40 (18/09/2011).

39 Ney Jr., Paul C., "Some considerations for conducting legal reviews of U.S. military cyberoperations", *Harvard International Law Journal Online,* vol. 62, 2020, p. 8.

40 Remiro Brotóns, Antonio, *op. cit.,* p.52.

41 Kraska, James; Saito, Yusuke, "The law of military operations and self-defense in the U.S.-Japan Alliance", *Naval War College Review,* vol. 73, 2020, núm.3, p. 90.

42 Ohlin, Jens David, "The Doctrine of Legitimate Defense", *International Law Studies,* vol. 91, 2015, p. 150.

que algunos han calificado de genocidio cultural contra los integrantes de esta etnia[43].

Cabría preguntarse por contra, cuál sería la alegación favorable a ejercitar la legítima defensa contra actores no estatales. En el plano interno encontramos la Directiva de política presidencial PPD-20, de 2012, hecho público a través de la red Wikileaks[44], que definía las operaciones ofensivas de efectos cibernéticos, reconociéndoles "capacidades únicas y no convencionales para promover los objetivos nacionales de los EEUU, en todo el mundo, con poca o ninguna advertencia al adversario o al objetivo, y con efectos potenciales que van desde lo sutil a lo muy dañino"[45]; si esto es puesto en diálogo con la Estrategia de Ciberseguridad de 2018, en la que se identificaba la amenaza que representan los actores no estatales[46], de acuerdo a lo ejercido por los presidentes estadounidenses, puede entenderse que es reconocido el empleo de un ciberataque, desde una visión de práctica del derecho a la legítima defensa, con una finalidad preventiva contra cualquier actor no estatal, que suponga una amenaza a los intereses del país norteamericano.

---

43 Simhony, Limor, "Could Cyberattacks Stop the Cultural Genocide in Xinjiang?", *Foreing Policy,* 2020. Disponible en: <https://foreignpolicy.com/2020/10/16/could-cyberattacks-stop-cultural-genocide-xinjiang-china-uighur-internment-camp/>.

44 Chatham House, *op. cit.,* 2018.

45 Federation Of American Scientist, *Presidential Policy Directive/PPD-20*, 2012. Disponible en: <https://fas.org/irp/offdocs/ppd/ppd-20.pdf> (11 de mayo de 2021).

46 The White House, *National Cyber Strategy*, 2015. Disponible en: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

B) Rusia

Con la información pública disponible, la Federación de Rusia no ha aprobado formalmente una Estrategia de Ciberseguridad. Lo más parecido es el proyecto de la misma, el Concepto de Estrategia de Ciberseguridad de la Federación de Rusia, de 2011[47], en el que se distingue la importancia central que ocupa el ciberespacio, para el desarrollo y la modernización económica del país, ofreciendo oportunidades a la población, pero también riesgos por los daños que puedan causar los ciberdelincuentes y ciberterroristas.

A destacar en este documento, se encuentra una singularidad no encontrada en los otros países miembros del Consejo, entre los conceptos de espacio de información (como actividad de creación, almacenamiento, transmisión, y uso de datos con impacto en la sociedad) y ciberespacio (espacio conformado por las redes de telecomunicaciones y sus infraestructuras), así como de seguridad de la información (estado de protección de los bienes y personas, respecto de los usos perniciosos del espacio de información) y ciberseguridad (condiciones que garantizan la protección de las amenazas del ciberespacio).

Si se analiza su Estrategia de Seguridad Nacional de 2015, efectúa un reconocimiento al surgimiento de nuevas actividades ilegales a través de la tecnología (apartado 22), admitiendo asimismo el peligro que representa el retraso tecnológico, así como las sanciones unilaterales contra sus organizaciones científicas y educativas (apartado 68), declarando la necesidad de crear alianzas entre el sector público y privado, para generar profesionales capaces de aumentar el nivel de seguridad tecnológica del país (apartado 69)[48].

---

[47] RUSIA, *Concepto de Estrategia de Ciberseguridad de la Federación de Rusia*, 2011. Disponible en: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>. (15 de mayo de 2021).

[48] Consejo De Seguridad de la Federación De Rusia, Estrategia de Seguridad Nacional de la Federación de Rusia, aprobado por el Decreto del

Por otra parte, el Decreto del Presidente de la Federación de Rusia Nº 203, de 09/05/2017, sobre la estrategia para el desarrollo de la sociedad de la información en la Federación de Rusia para 2017-2030, cuyo apartado III. 21. B) establece que su objetivo es garantizar la seguridad de los ciudadanos y el Estado, pero desde una perspectiva interna y no internacional, al disponer distintas medidas en su articulado tendentes a conseguir este objetivo, a través de reformas legales y la creación de las necesarias estructuras que permitan su consecución, exaltando la importancia de consolidar los intereses nacionales en este medio[49], pero sin hacer una mención expresa a la ciberseguridad del país, ni a las capacidades en el ejercicio de la legítima defensa en este espacio.

C) China

La Estrategia militar de China, de mayo de 2015[50], reconocía la consolidación del ciberespacio como un elemento estratégico entre las potencias mundiales, por lo que expresaba la creciente importancia en la salvaguardia de su seguridad por este medio. En atención a este ámbito, se aprobó la Estrategia Nacional de Seguridad en el Ciberespacio, de 27 de diciembre de 2016[51], con un lenguaje más politizado en contraposición al documento de 2015, al contener alusiones a algunos de los paradigmas programáticos de su actual presidente, como la política de los cuatro principios, y

---

Presidente de la Federación de Rusia, Nº 683 (31/12/2015)

[49] Rusia, Decreto del Presidente de la Federación de Rusia Nº 203 (09/05/2017).

[50] The State Council The People´S Republic Of China, China´s Military Strategy (full text). Disponible en: <http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm> (21 de mayo de 2021).

[51] Cyberspace Administration Of China, Estrategia Nacional de Seguridad en el Ciberespacio. Disponible en: <http://www.cac.gov.cn/2016-12/27/c_1120195926.htm>. (21 de mayo de 2021).

las cinco proposiciones; pero en todo caso, expresando el reconocimiento al ciberespacio como un nuevo campo de expresión de la soberanía estatal, y de idéntica magnitud para el mismo, como son la tierra, el mar, el cielo y el espacio.

Entendidas las especiales características de China, el documento hace énfasis a cómo los ciberataques representan por el siguiente orden: un peligro político (por miedo a la instigación de revueltas y actos subversivos desde el extranjero); económico (los actos contra sus infraestructuras críticas); cultural (contenidos considerados contrarios a los valores socialistas); y social (aludiendo esencialmente a las actividades terroristas y separatistas).

Destaca el reconocimiento expreso a Naciones Unidas, como sujeto que ha de liderar la creación de normas internacionales, destinadas a su aceptación universal, para mejorar la seguridad en el ciberespacio y la lucha contra el terrorismo en estos sistemas, así como dar respuesta a emergencias en infraestructuras críticas de la información; y dentro de esta perspectiva internacionalista (no registrada en otros Estados), China alienta a la promoción en la utilización de Internet por los países emergentes, en pos de reducir la brecha digital, pero sin olvidar la necesidad de promocionar su iniciativa de la nueva ruta de la seda.

Con anterioridad, el 7 de noviembre de 2016 China promulgó la Ley de Ciberseguridad, que entró en vigor el 1 de junio de 2017[52], en la cual se equipara la ciberseguridad a la seguridad nacional[53]. Ello puede extraerse de la lectura de algunos de sus preceptos, como el segundo párrafo del artículo 12, que indica que no debe utilizarse internet para poner en peligro la seguridad nacional; el artículo 31, referente a las infraestructuras críticas, cuyos daños, pérdida de funciones o datos, pueda poner en grave peligro

[52] República Popular China, Ley de Ciberseguridad de la República Popular China (07/11/2016).

[53] LI, Yuwen , BIAN, Cheng, "A new dimension of foreign investment law in China – evolution and impacts of the national security review system", *Asia Pacific Law Review,* vol. 24, 2016, núm. 2, pp. 149-175.

la seguridad nacional; y el artículo 55, que manifiesta como ante amenazas a la ciberseguridad "se exigirá a los operadores de red que tomen todas las medidas necesarias para eliminarlas".

D) Reino Unido

La Estrategia de Ciberseguridad Nacional 2016-2021, indica que:

> Gran parte del software y el hardware que se crean originalmente para facilitar este entorno digital interconectado han dado prioridad a la eficiencia, el costo y la conveniencia para el usuario, pero no siempre han incluido la seguridad desde su incepción. Actores malintencionados, estados hostiles, individuos y organizaciones criminales o terroristas, pueden explotar esta brecha entre la conveniencia y la seguridad. Reducir esta brecha es una prioridad nacional. [54]

La originalidad de este documento se encuentra al aludir a figuras distintas de los ciberdelincuentes (mayoritariamente dedicados al fraude, robo y extorsión, desde África occidental, Europa oriental, y el sur de Asia), y terroristas (que aunque disponen de una baja capacidad técnica, su impacto "hasta la fecha ha sido desmesuradamente elevado"), como son los hacktivistas (grupos descentralizados, motivados por un objetivo de carácter "justiciero") y los script kiddies (personas que sin los necesarios conocimientos técnicos para crear su propio malware, emplean el de otros desarrolladores para ejecutar ciberataques por afán de protagonismo, pudiendo "tener un impacto desproporcionadamente perjudicial en las organizaciones afectadas"), que en conjunto representen in-

[54] United Kingdom Government, National Cyber Security Strategy 2016. Disponible en: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf>. (14 de mayo de 2021).

DOI:http://10.22201/fder.24488933e.2022.283.83165

dividuos que directamente o indirectamente estén patrocinados por otros Estados.

Es interesante observar, como desde el documento se expresa que dentro del combate a los actores extranjeros hostiles, si bien se sostendrá la defensa del derecho internacional, en coordinación con los Estados socios en el marco de cooperación, disuasión y seguridad, que permita su pertenencia a la OTAN, "gran parte de esta acción no se llevará a cabo en el dominio público", lo que abre la posibilidad a una delegación del uso de la fuerza en el ciberespacio al sector privado.

En el ámbito normativo destaca la Computer Misuse Act de 1990, enmendada por última vez en 2015[55], en cuya sección 3ZA, desglosa los elementos que demarcan la culpabilidad de una persona por la comisión de actos cibernéticos, comprendiendo aquellos que causen o generen el riesgo de originar daños a las personas (pérdida de vida, lesiones, interrupciones en los suministros básicos), al medio ambiente, la economía y la seguridad nacional. Asimismo, el 10 de mayo de 2018 entró en vigencia The Network and Information Systems Regulations 2018[56], en la cual se incluye una graduación que podría ser extrapolada para la determinación y delimitación de la gravedad de un ciberataque[57].

E) Francia

A pesar de no encontrarse recogido en una norma interna, de los países expuestos, Francia es el país que más sólidamente ha delimitado el rango de ejercicio de la legítima defensa en el ciberespacio.

---

55 Reino Unido, Computer Misuse Act 1990.

56 Reino Unido, The Network and Information Systems Regulations 2018 (19/04/2018).

57 "Para determinar la importancia del impacto de un incidente, un OSE (operador de servicios esenciales), debe tener en cuenta los siguientes factores: (a)el número de usuarios afectados por la interrupción del servicio esencial; (b) la duración del incidente; y (c) el área geográfica afectada por el incidente".

A través de una declaración del Ministerio de defensa galo, de 9 de septiembre de 2019, reconoció tajantemente la obligación internacional de respetar el cumplimiento de la Carta, manifestando como se reserva el derecho a responder a cualquier ciberataque que infrinja el derecho internacional (cuya calificación como uso de la fuerza dependerá de los efectos que ocasione, aun cuando estos no sean de carácter físico), aunque sea realizado por un actor no estatal, y siempre que responda a las órdenes de un Estado, (de lo contrario no se reconocerá el derecho a la legítima defensa contra tales acciones), ya que a pesar de haber invocado esta potestad contra el ISIS, la excepcionalidad de este supuesto no puede servir de precedente extrapolable al ciberespacio[58].

A diferencia de lo manifestado en la regla 71 del Manual, que expresaba la definición en la concreción de una ciberoperación como ataque armado, de acuerdo a la escala y efecto que ocasione, motivando la legítima defensa contra actores no estatales cuando actúen sin apoyo de un país (conforme a lo contenido en su comentario 19)[59]; siguiendo su razonamiento argumental, de la excepcionalidad del terrorismo alcanzado por ISIS, la declaración ministerial de 2019 se opone a este postulado, negando el reconocimiento a ejercitar la legitima defensa contra un actor no estatal, que opera de forma independiente en el territorio de un Estado, que es incapaz de detener dichas acciones[60].

---

58 Ministére Des Armmées, *International Law applied to operations in cyberspace*, 2019. Disponible en: <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf> (16 de mayo de 2021).

59 Schmitt, Michael, N., *op. cit.,* p. 345.

60 Ministére Des Armmées, *op. cit.*, 2019.

IV. Conclusiones: el desvanecimiento de la inminencia y la probabilidad, como elementos condicionantes de la legalidad

El artículo objeto de exposición, ha confirmado el status secular de *nihil novum sub sole*, en el que se encuentra la comprensión de la legitima defensa internacional, debiendo matizarse como esta se ha readaptado en el adagio non nova, sed nove; sin que por ello sea posible afirmar si el Derecho Internacional público se mantendrá en los parámetros que han regido desde el final de la segunda guerra mundial, o si se encuentra ante un momento grociano de cambio de las circunstancias, que origine una nueva costumbre internacional de ejercicio de la fuerza preventiva ante las amenazas del ciberespacio, o si por el contrario se trata de un acercamiento al desuetudo, por el abandono de la práctica a no ejercer la fuerza contra actores no estatales.

Se ha comprobado como la práctica internacional de los Estados policía, remite al sentido común, habiéndose mantenido una postura exigente respecto al uso de la fuerza ante las nuevas circunstancias del ciberespacio. Aun desconociéndose la posición exacta defendida por China y Rusia en torno a esta cuestión, se aprecia el notable distanciamiento de visiones defendidas por el mundo anglosajón y francófono. Frente a la defensa estadounidense, de atención a las necesidades y el empleo proporcional de los medios disponibles, acorde a las circunstancias del escenario de conflicto, y el peligro a que debe enfrentarse (con independencia de la naturaleza estatal o no de la amenaza), el país galo se opone al ejercicio de la legitima defensa contra las fuerzas no estatales que actúen desde un tercer Estado.

En conjunto, se ha evidenciado la necesidad de alcanzar un instrumento internacional que delimite la aplicación de los nuevos sistemas, y la responsabilidad de los Estados detentadores y productores de ellos, garantizando la seguridad mundial al impedir el acceso a estos medios por actores no estatales. El trabajo del Manual podría servir de modelo a seguir en la generación de

convenios internacionales, pero la falta de reconocimiento desde Estados no occidentales dificulta esta labor; precisándose la generación del conveniente debate académico, que pueda llevar al acercamiento de posturas, y a la conclusión de un Tratado que efectivamente logre un uso pacífico y de intervención armada restringida en el ciberespacio.