LA CONSTRUCCIÓN DE NORMAS GLOBALES, ENTRE EL AVANCE DEL COSMOPOLITISMO BLANDO Y EL RETORNO DE LA GEOPOLÍTICA. LA REGULACIÓN GLOBAL DE LA CIBERSEGURIDAD

The Construction of Global Norms, Between the Advance of Soft Cosmopolitanism and the Return of Geopolitics. Global Regulation of Cybersecurity

Caterina García Segura[1]

RESUMEN: Ante el carácter global de buena parte de las cuestiones que afectan a la seguridad en el contexto de la globalización, la sociedad internacional se ha visto en la necesidad de buscar soluciones de gobernanza global. La construcción de normas

---

1 Catedrática de Relaciones Internacionales en la Universitat PompeuFabra (caterina.garcia@upf.edu).

Esta investigación ha sido realizada en el marco del proyecto "La construcción de normasglobales a examen: el impacto transformador del avance del cosmopolitismo y el resurgir de Westfalia" financiado por el Ministerio de Ciencia, Innovación y Deportes (Proyectos de I+ D, Programa estatal de fomento de investigación científica y técnica de excelencia. 2018-2020, Referencia: DER2017-85800-P).

globales se lleva a cabo en un entorno marcado por dos procesos de signo opuesto: el avance del cosmopolitismo blando y el retorno de la geopolítica, subproducto del fenómeno más general del resurgir del modelo westfaliano. El estudio analiza en un ámbito concreto, el de la ciberseguridad, cómo estos dos procesos contrapuestos influyen y determinan la construcción de normas globales. Se observa que en este ámbito, el cosmopolitismo blando, *Wordfalia*, no se ha impuesto a *Westphalia*. Los intentos de crear una cultura mundial del ciberespacio no han funcionado. Aunque el ciberespacio es un espacio plural y los actores privados participen cada vez más activamente en los procesos regulatorios, estos están controlados por las autoridades estatales ya sean en su formato de regulación nacional, bilateral, regional o multilateral. La concepción de la seguridad en clave tradicional, nacional y no global, es el argumento que lo justifica. La regulación fragmentada, traducida en acuerdos bilaterales y regionales, se ha impuesto de momento a la regulación global.

ABSTRACT: Given the global nature of many of the issues affecting security in the context of globalisation, international society has found it necessary to seek global governance solutions. The construction of global norms takes place in an environment marked by two processes of opposite sign: the advance of soft cosmopolitanism and the return of geopolitics, a by-product of the more general phenomenon of the resurgence of the Westphalian model. The study analyzes in a specific field, that of cybersecurity, how these two opposing processes influence and determine the construction of global norms. It is observed that in this field, the soft cosmopolitanism Wordfalia has not imposed itself on Westphalia. Attempts to create a global culture of cyberspace have not worked. Although cyberspace is a plural space and private actors increasingly participate actively in regulatory processes, these are controlled by state authorities whether in their national, bilateral, regional or multilateral regulatory format. The conception of security in the traditional, national and not global key is the argument that justifies it. Fragmented regulation, translated into bilateral and regional agreements, has so far imposed itself on global regulation.

PALABRAS CLAVE: Normas internacionales. Roles normativos. Ciberespacio. Ciberseguridad. Cosmopolitismo blando. Retorno de la geopolítica. Tensión cosmopolita.

KEY WORDS: International Norms, Normative roles. Cyberspace. Cybersecurity. Soft Cosmopolitanism. Return of Geopolitics. Cosmopolitan tension.

1. INTRODUCCIÓN: LAS TRANSFORMACIONES DEL ORDEN INTERNACIONAL

El marco en el que se desarrollará este estudio es el de las transformaciones del orden internacional. Siguiendo a Hedley Bull, entendemos el orden internacionalcomo el patrón de actividad que rige la actividad internacional y mantiene los objetivos primarios o elementales de la sociedad de Estados o sociedad internacional.[2] El orden ayuda a reducir la inseguridad y a estabilizar las relacio-

2 El patrón de actividad se va conformando progresivamente a través de la suma de diferentes elementos: principios, normas, reglas e instituciones. Los objetivos elementales

nes internacionales[3]. John Ikenberry lo define a partir de sus elementos como el conjunto de acuerdos de gobierno entre Estados que incluyen sus normas, sus principios y sus instituciones.[4] El orden està en constante evolución ya que debe ir adaptándose a los cambios que acontecen en la escena internacional. La dualidad de la naturaleza del orden, a la vez estable –la estabilidad le permite crear expectativas de conducta y reducir la inseguridad– y dinámica –el dinamismo le permite adaptarse a la realidad cambiante– constituye el centro de la definición de Michel Mazarr y sus colaboradores que lo describen como un patrón de relaciones entre Estados que incluye una combinación de elementos que van desde normas emergentes hasta reglas que crean las instituciones de las organizaciones políticas internacionales y los regímenes internacionales.[5]

En determinados periodos históricos la presión de la realidad sobre el orden parece más apremiante que en otros en los que su estabilidad parece garantizada, pero, en mayor o menor grado, la tensión entre cambio y continuidad es constante. La evolución del orden internacional no sólo no es incompatible con su estabilidad sino que ayuda a consolidarla. Para mantenerse estable, es decir, para que sean respetadas la mayoría de sus normas e instituciones, la mayor parte del tiempo, por la práctica totalidad de los actores, todo orden debe tener cierto grado de flexibilidad.[6] La resiliencia, requisito para la supervivencia del orden, exige integrar las exigencias normativas e institucionales derivadas de los cambios y tensiones en las relaciones Internacionales en los elementos básicos del orden –normas, reglas, instituciones– de manera que los principios constituyentes del mismo puedan mantenerse inalterados.[7] Los motivos que impulsan las trasformaciones del orden son muy diversos y muchos de ellos están interrelacionados:

---

del orden son: la preservación de la sociedad de Estados; el mantenimiento de la soberanía externa de los Estados; la limitación de la violència; el mantenimiento de los compromisos adquiridos; y el respeto a las normas de propiedad. BULL, H., *The Anarchical Society. A Study of Order in World Politics,* Londres, Macmillan, 1995 (1ª ed., 1977), p.8 et ss.

3 Pablo Pareja enfatiza la capacidad estabilizadora del orden al definirlo como "el patrón de actividad que limita la frecuencia y la intensidad de la violencia en las interacciones entre los integrantes de un determinado sistema". PAREJA-ALCARAZ, P., "Unidad y pluralismo en el orden internacional: la complementariedad del orden internacional y el orden regional de Asia Oriental", en RODRIGO, Á. y GARCÍA, C. (eds.), *Unidad y pluralismo en el Derecho internacional y la comunidad internacional*, Madrid, Tecnos, 2011, pp. 129-150.

4 IKENBERRY, G.J., *After Victory: Institutions, Strategic Restraint, and the Rebuilding of OrderAfter Major Wars*, Princeton, Princeton University Press, 2001, p. 23.

5 MAZARR, M.J., PRIEBE, M., RADIN, A. y CEVALLOS, S., *Understanding the Current International Order*, Santa Monica, RAND Corporation, 2016, p.7.

6 BULL H., *op. cit,* nota, 2.

7 REUS-SMIT, C., "The Constitutional Structure of International Society and the Nature of Fundamental Institutions", *International Organization*, vol. 51, 1997, núm. 4, pp. 555-589.

entre otros, las variaciones en las relaciones de poder entre las grandes potencias del sistema de Estados; la aparición o el mayor protagonismo de nuevas categorías de actores; el descubrimiento o desarrollo de nuevos recursos de poder, o la escasez de algunos de ellos; y los avances tecnológicos aplicados a diferentes ámbitos –armamento, transportes, comercio, comunicaciones, etc.

Desde hace varias décadas, algunas de las normas, reglas e instituciones del orden internacional liberal[8] surgido tras la Segunda Guerra Mundial se ven impelidas a modificarse ante su disfuncionalidad manifiesta para dar respuestas a los retos de la globalización. Una segunda fuente de transformación proviene de las nuevas potencias emergentes que, insatisfechas por unos mecanismos decisorios que responden a un reparto del poder mundial que nada tiene que ver con el actual, presionan para que estos se adapten a la nueva distribución de capacidades. Finalmente, un tercer origen de cambio se halla en el menosprecio, abandono o violación de las normas e instituciones del orden por parte de la potencia que fue su creadora y/o impulsora, Estados Unidos. El orden internacional está transformándose pero la sociedad internacional, cada vez más plural y compleja, es incapaz de dar una respuesta rápida a los cambios que en ella se operan, por ello el orden está "desajustado" y no es totalmente funcional, lo cual da lugar a una situación de *interregno* o de crisis. A su vez esta situación –entre el reconocimiento de la incapacidad y el desajuste y la readaptación de las normas e instituciones– genera una sensación de temor y confusión que hace que ciertos académicos, políticos y comentaristas hablen de desorden,[9]de caos,[10] de erosión o de colapso del orden.[11]En realidad, en la mayoría de casos, no se refieren a la crisis del orden, de sus normas, reglas e instituciones, sino a la inestabilidad, inseguridad o conflictividad de las relaciones internacionales.[12] Aunque sean conceptos que reflejan realidades cercanas e interrelacionadas, a efectos analíticos es importante distinguir y no usar como sinónimos la estructura de poder (la distribución del poder en el sistema interetatal), el orden (tal como ha sido definido) y las dinámicas de la sociedad internacional (cooperación, conflicto e integración, en sus diferentes grados).

---

8 IKENBERRY, G. J., *Liberal Order and Imperial Ambition,* Cambridge, Polity Press, 2004.

9 HAAS, R., "The Era of Disorder", *Project Syndicate*, 27 de octubre de 2014 y *A World of Disarray. American Foreign Policy and the Crisis of World Order,* Nueva York, Penguin Books, 2018; CARR, E. "World Disorder", *The Economist*, 13 Noviembre 2014, pp. 21-23.

10 KISSINGER, H., *World Order. Reflections on the Character of Nations and the Course of History,*Nueva York, Penguin Books, 2015.

11 En 2015 la Conferencia de Seguridad de Munich –la llamada "Davos de la seguridad", plataforma global de líderes mundiales y expertos en seguridad– titulaba su Informe "Collapsing Order, Reluctant Guardians?"; en 2018 empezaba el informe planteándose si el orden internacional estaba llegando al límite: "Present at the Erosion, International Order on the Brink?".

12 Tal sería el caso de los citados informes de la Conferencia de Seguridad de Munich.

Ante visiones catastrofistas sobre el fin del orden liberal, John Ikenberry argumenta que la crisis del mismo no conduce necesariamente a su descomposición y que no solo sigue vivo sino que está en expansión.[13] Señala que, irónicamente,el inicio de la crisis del orden liberal coincidió con el colapso de la Unión Soviética y con la expansión del internacionalismo liberal. La crisis, puntualiza, reside en el hecho de que los fundamentos sobre los que se erigieron buena parte de las normas, reglas e instituciones del orden están debilitándose, especialmente la distribución del poder mundial en la que Estados Unidos ocupaba una posición hegemónica. Pero también, y más importante, en la renuncia de la superpotencia estadounidense a seguir ejerciendo el liderazgo, el abandono *de facto* de los valores y principios liberales en los que se inspiraba (democracia liberal, protección de los Derechos Humanos, relaciones basadas en normas e instituciones, multilateralismo), y su apuesta por el neoliberalismo económico, el nacionalismo y el unilateralismo.[14] En definitiva, el orden liberal se ha quedado sin "guardián"porque Estados Unidos ha perdido algunos recursos de poder frente al auge de otras potencias pero, sobre todo, porque no tiene interés ni voluntad de defender las normas e instituciones que construyó. Así, aunque los discursos políticos interesados proclamen lo contrario y hablen de amenazas externas al orden liberal,[15] el análisis politológico permite concluir que si el orden internacional es hoy menos americano y menos liberal, lo es por el abandono estadounidense de sus posiciones y responsabilidades anteriores más que por usurpación de estas por parte de las potencias emergentes.

La disputa sobre el orden internacional entre las potencias emergentes y las tradicionales no versa sobre los principios fundamentales del mismo –ya que in-

---

13 IKENBERRY, G.J., *Liberal Leviatan: the origins, crisis and transformation of the American world order*, Princeton, Princeton UniversityPress, 2011a. Una posición diametralmente opuesta a la de G. John Ikenberry es la Amitav Acharya, quien defiende que el orden americano ha llegado a su fin, al margen de la consideración de que Estados Unidos esté o no en declive. ACHARYA, A., *The End of American World Order*, Cambridge, Polity Press, 2014, p. 4.

14 IKENBERRY, G.J., "La crisis del orden liberal mundial", *Anuario Internacional CIDOB 2018*, Barcelona, CIDOB, 2018, pp. 29-36 (33 y 36).

15 El Departamento de Defensa de Estados Unidos identifica el "creciente desorden mundial" (identificado con el "declive del orden internacional de larga duración basado en normas") con el ascenso y el comportamiento de China y Rusia. Añade que existen claros desafíos al orden internacional liberal derivados de la reemergencia de la competición estratégica a largo plazo entre potencias, lo cual crea un entorno de seguridad estratégica global crecientemente complejo. DEPARTMENT OF DEFENSE, *Summary of the 2018 National Defense Strategy of the United States of America. Shapening the American Military's Competitive Edge.* Washington D.C., DoD, 2018.
https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

cluso su promotor está dispuesto a abandonarlos– sino sobre la autoridad y el liderazgo en sus instituciones.[16] Las potencias emergentes son, como veremos, grandes defensoras del orden liberal.[17] El desafío que plantean no es otra cosa que un desafío estratégico en términos de lucha por el poder y en el sentido más tradicional del término. La rivalidad existente entre las potencias tradicionales y las emergentes, especialmente entre Estados Unidos, China y Rusia, y el auge de las cuestiones territoriales (control del espacio terrestre y marítimo) y del poder militar (modernización de los ejércitos) como forma expresión de esta rivalidad han llevado a plantear "el retorno de la geopolítica"[18] cuando parecía que el fin de la Guerra fría la había relegado a un rol menor en las relaciones internacionales.[19] Esto acontece en el tablero del poder mundial. Pero respecto al orden internacional, a pesar de que cierta literatura académica y ciertos discursos políticos defiendan la existencia de tres modelos de orden internacional competitivos, *Westfalia*, *Worldfalia* y *Easfalia*,[20] las potencias emergentes no suponen un auténtico reto para los principios constituyentes del orden internacional. *Eastfalia* es, en este sentido, un mito o un discurso político construido con una intencionalidad determinada, puesto que no hay propuesta asiática alternativa de orden internacional, solo de un nuevo reparto de poder que refleje el peso real de las potencias asiá-

16 IKENBERRY, G.J. "The future of Liberal World Order", *Foreign Affairs,* vol. 11, núm. 3, 2011b, pp. 56-68 (57).

17 MAZARR, M.J., HEAD, T.R. y CEVALLOS A.S., *China and the International Order,* Santa Mónica, Rand Corporation, 2018.

18 MEAD, W.R., "The Return of Geopolitics. The Revenge of the Revisionist Powers", *Foreign Affairs*, vol. 93, 2014, núm. 3, pp. 69-79; PATRICK, S, y BENNET, I., "Geopolitis Is Back-and Global Governance is Out", *The National Interest,* 12 de mayo de 2015. https://nationalinterest.org/blog/the-buzz/geopolitics-back%E2%80%94-global-governance-out-12868.

19 Idea defendida por Francis Fukuyama basándose en el fin de las ideologías, tras el triunfo del capitalismo sobre el socialismo. FUKUYAMA, F., *The End of History and the Last Man*, Nueva York, The Free Press, 1992.

20 *Westfalia* es el orden internacional que, desde el siglo XVII, ha desarrollado los principios, normas e instituciones que han consagrado el sistema de Estados soberanos y de cuya evolución resulta el orden internacional liberal. *Worldfalia* sería un nuevo modelo de orden internacional que aún no existe como tal, pero que se deja entrever en la evolución de algunos debates normativos de la sociedad internacional y que se basaría en valores cosmopolitas. Es un modelo liderado, sobre todo, por algunas organizaciones internacionales y por actores de la sociedad civil global, mientras que los Estados responden a las presiones de estos actores líderes articulando una narrativa cosmopolita a la que su conducta no siempre se acomoda. *Eastfalia* sería un hipotético orden internacional que se erigiría sobre la preponderancia de Asia como centro de poder mundial y pivotaría alrededor de supuestos principios y prácticas de origen asiático. Dista de ser una realidad. GARCÍA SEGURA, C., "*Westfalia, Worldfalia, Eastfalia.* El impacto de las transformaciones de la estructura de poder interestatal en el orden internacional", *Revista Española de Derecho Internacional,* vol. 69, 2017, núm. 2, pp. 45-70 (47).

ticas en la economía mundial en los procesos de toma de decisiones. Las nuevas potencias han dejado de ser receptoras pasivas de normas y se han convertido en potencias que alternan los roles de afianzadoras activas y de resistentes creativas frente al impulso de *Worldfalia*, al que también se resisten –*de facto*, que no discursivamente– las potencias occidentales.[21] *Worldfalia* supondría una mayor amenaza al orden internacional puesto que sus planteamientos cosmopolitas cuestionan parte del significado de la soberanía estatal a favor de la defensa del individualismo (el individuo se sitúa en el centro desplazando al Estado), del universalismo (frente al nacionalismo estatal) y de la dignidad humana (protección de los Derechos Humanos),[22] convirtiéndola en responsabilidad de proteger. Su punto débil es la resistencia de las potencias del sistema interestatal, tradicionales y emergentes. Frente a los cambios *worldfalianos*, los supuestos defensores de *Eastfalia* afianzan activa y decididamente los dos pilares del orden internacional: el sistema de Estados soberanos, en su versión *westfaliana* más tradicional, y las instituciones y normas fundamentales del orden liberal en las que se basa su buen desempeño económico.[23] Así pues, la base constitucional, la lógica profunda del orden internacional y sus instituciones fundamentales, están a salvo o, en cualquier caso, si no lo están al cien por cien, no es solo por la presión o el desafío de las potencias asiáticas o emergentes. Las presiones *worldfalianas,*y las propuestas de orden cosmopolita que las inspiran, surgen como consecuencia de las transformaciones operadas en la sociedad y en el orden internacional a partir del fin de la bipolaridad y de la intensificación de los efectos de la globalización, en especial, del reconocimiento de que la naturaleza global de los riesgos y las amenazas que genera una conciencia de futuro colectivo y la necesidad de repensar la comunidad política internacional y sus mecanismos de gobernanza global[24]. Es la comprensión de la sociedad del riesgo global la que lleva a establecer los contornos de una potencial esfera pública global y a desencadenar el impulso de instituciones internacionales cooperativas.[25] Las propuestas de normas e institu-

---

21 ANDREWS, N., "Globalization, Global Governance and Cosmopolitanism: A Critical Exploration of European Practice", *CEU Political Science Journal,* vol. 7, 2012, núm. 4, pp. 411-433 (429). Este autor defiende que, en el caso de la UE, gran defensora retórica de principios cosmopolitas, es poco probable que se avance en su plasmación en las políticas europeas porque no existe la uniformidad ni el consenso suficiente.

22 *Ibíd.,* p. 417.

23 IKENBERRY, G.J., *op. cit.*, nota 16, p. 62.

24 VERTOVEC, S. y COHEN, R. (2002), "Introduction: Conceiving Cosmopolitanism", en VERTOVEC, S. y COHEN, R., *Conceiving Cosmopolitanism. Theory, Context and Practice,* Nueva York, Oxford University Press, 2012, pp. 1-22.

25 BECK, U., *La sociedad del riego global*, Madrid: Siglo XXI de España Editores, 2002 (1ª ed. En inglés, 1999) p. 30 y RUGGIE, J.G., "Reconstituting the Global Public Domain – Issues, Actors and Practices", *European Journal of International Relations,* vol. 10, 2014, núm. 4, pp. 499-531.

ciones de inspiración cosmopolita son pues el resultado de la atención al cambio en el mundo social –desde la expansión de los mercados a los nuevos patrones de lealtad personal y la expansión de nuevas formas de gobernanza.[26] Y las lideran mayoritariamente actores de la sociedad civil global.

Sobre la base de lo afirmado hasta aquí, este trabajo parte de la premisa de que el orden internacional liberal está asistiendo a la trasformación de algunas de sus normas e instituciones como resultado de diferentes hechos: de los cambios de la sociedad internacional que afectan a la estructura de poder, de la dinámica de las relaciones entre las grandes potencias (tradicionales y emergentes) y del carácter global de algunos de los retos generados por la globalización. El objetivo del mismo es analizar cómo se concretan estas transformaciones en el ámbito de la ciberseguridad, un nuevo ámbito de la seguridad cuya gobernanza constituye un reto global. Las hipótesis de las que parte son: en primer lugar, que el cosmopolitismo –en su versión blanda o suave– constituye una realidad asentada, que ha resultado ser más resiliente de lo que auguraron sus detractores, debido al carácter global de los problemas que motivaron su emergencia, y todo ello a pesar del resurgir de concepciones *westfalianas*; en segundo lugar, y como consecuencia de lo anterior, que persisten valores y principios cosmopolitas en la definición y desarrollo de los procesos de construcción de normas globales y en su contenido; en tercer lugar, que el Estado sigue siendo un actor central en la construcción de normas globales pero dista de ser el único y de controlar en exclusiva los procesos normativos; en cuarto lugar defendemos que los procesos normativos globales son plurales y abiertos –los actores no estatales y las autoridades privadas desempeñan un rol creciente y determinante en muchos de ellos; son dinámicos –incluyen no solo la creación y difusión de normas, también su evolución y transformación; y son multidireccionales e híbridos – las normativas de diferentes temas y ámbitos se entrecruzan y solapan; y, en quinto lugar,los procesos normativos en curso en materia de ciberseguridad son el resultado de la tensión cosmopolita[27] existente entre los principios universales propuestos por diferentes actores internacionales para encarar los desafíos globales y garantizar los bienes públicos globales y los principios nacionales destinados a defender los intereses nacionales –geoestratégicos, geopolíticos y geoeconómicos– de los Estados o los intereses particulares de otros actores tales que las empresas del sector de las tecnologías de la información y la comunicación.

Empezaremos nuestro estudio analizando los dos procesos de la sociedad internacional actual que se contraponen y que conforman el trasfondo de las trans-

---

26 NOWICKA, M. y ROVISCO, M., *Cosmopolitanism in Practice. Global Connections,* Farnham, Ashgate, 2008

27 GARCÍA SEGURA, C., (Directora), *La tensión cosmopolita. Avances y límites en la institucionalización del cosmopolitismo*, Madrid, Tecnos, 2016.

formaciones del orden internacional: el avance lento del cosmopolitismo blando o suave vinculado a intereses generales y cooperativos de la sociedad internacional y el supuesto resurgir de la geopolítica identificado con intereses rivales y competitivos de los Estados. A continuación estudiaremos los desarrollos teóricos sobre el proceso de creación de normas globales, lo que nos permitirá aprehender el nuevo rol de las potencias emergentes en la transformación o mantenimiento de las normas e instituciones del orden internacional. Seguidamente analizaremos las características del ciberespacio como nuevo ámbito en el que se desarrollan oportunidades de todo tipo, hasta hace poco impensables, pero también nuevos retos globales a la seguridad (ciberseguridad). Finalmente examinaremos los avances en la regulación global de la ciberseguridad: qué procesos normativos existen, qué intereses y valores se intentan proteger, qué actores los lideran, cuáles son sus características, cuáles los escollos con los que topan y cuáles sus perspectivas de avance. Concluiremos el trabajo con unas reflexiones finales.

2. LA SOCIEDAD INTERNACIONAL ENTRE EL COSMOPOLITISMO BLANDO Y EL RETORNO DE LA GEOPOLÍTICA

Los procesos y dinámicas que se dan en la sociedad internacional pocas veces avanzan en la misma dirección. Las tensiones entre fuerzas centrípetas (integradoras, homogeneizadoras) y centrífugas (desintegradoras, diversificadoras) de diferente naturaleza son una de sus características tradicionales.[28] A medida que la sociedad internacional deviene más plural (nuevos actores) y compleja (mayor número de interacciones, retos y desafíos globales) los procesos y dinámicas se diversifican y las tensiones se amplifican. A finales de los años ochenta del siglo pasado éstas se visibilizaban especialmente a través de los procesos, aparentemente contrapuestos, de la globalización y la regionalización. Su carácter en apariencia opuesto generaba una situación paradójica: por una parte, parecía que esa tensión tanto podia conducir al desorden como a un nuevo orden global. Y, por otra parte, al tiempo que parecían procesos incompatibles y contradictorios, se reforzaban mutuamente. [29]En este mismo sentido, los dos procesos que analizaremos a continuación son una manifestación de dos tendencias de signo

---

28 ARENAL, C. DEL, (2005), "En torno al concepto de sociedad internacional", en RODRÍGUEZ CARRIÓN, A. J. y PÉREZ VERA, E. (coord.), *Soberanía del Estado y Derecho Internacional. Homenaje al Profesor Juan Antonio Carrillo Salcedo*. Sevilla, Universidad de Sevilla, 2005, pp. 453-464.

29 HETNNE, B., "Globalization and the New Regionalism: The Second Great Transformation", en HETNNE, B., INOTAI, A., y SUNKEL, O., *Globalism and the New Regionalism*, Londres, Palgrave Macmillan, 1999, pp. 1-24.

contrario –el cosmopolitismo y el comunitarismo o soberanismo– que coexisten en la sociedad internacional y provocan la tensión cosmopolita. Representan intereses diferentes: los de una comunidad internacional emergente articulada en torno a valores cosmopolitas y los de un sistema de Estados soberanos que, en la defensa de sus intereses nacionales parecen optar, ahora con más fuerza que en décadas anteriores, por la lógica de la lucha por el poder territorial-militar. El primer proceso quiere fortalecer el carácter cooperativo e integrativo de las relaciones internacionales, el segundo subraya el aspecto conflictivo de las mismas.

2.1. El lento avance del cosmopolitismo blando

Desde principios de la década de los noventa, la tensión entre fuerzas centrífugas y centrípetas en la sociedad internacional ha adoptado nuevas formas. Una de ellas es la tensión entre un proyecto de orden mundial, cosmopolita, *Worldfalia,*y el orden internacional existente, de Estados, *Westfalia*.[30] Si bien a lo largo de la historia han existido de forma recurrente diferentes propuestas cosmopolitas, a menudo asociadas proyectos utópicos, en los años noventa el resurgir del cosmopolitismo estuvo directamente asociado a la necesidad de gobernanza global para afrontar los retos y las amenazas globales. Esta toma de conciencia se acompañó de la voluntad de establecer los contornos de una potencial esfera pública global y desencadenó el impulso de instituciones internacionales cooperativas.[31] Era una reacción posibilista que no perseguía la utopía de un gobierno mundial. A pesar de ello, los planteamientos universalistas, en la práctica, toparon con las posiciones opuestas de dos versiones de un mismo enfoque: la comunitarista o pluralista, defensora de la heterogeneidad de los valores comunitarios por encima de la homogeneidad de los valores universales, y la soberanista, más centrada en la defensa de los intereses nacionales por encima de los intereses de la comunidad internacional. En las últimas dos décadas la tensión entre ambos modelos se ha resuelto en un lento avance del *cosmopolitismo blando o suave*[32] que se traduce en una tendencia a la adopción de principios y normas de aspiración universalis-

---

30 Véase la distinción de Hedley Bull entre orden internacional y orden mundial. BULL, H., *op. cit.*, nota 2, pp. 60-73.

31 BECK, U., *op. cit,* nota 25, p. 30. Véase también, RUGGIE, J.G., *Op. cit.*, nota 25.

32 GOEBEL, W., "Hard and Soft Cosmopolitanism: The Eighteenth Century and After", en GOEBEL, W. y SCHABIO, S. (eds.), *Locating Transnational Ideas,* Nueva York, Routledge, 2010, pp. 126-138. Sobre la distinción entre cosmopolitismo suave y fuerte veáse también: BEARDSWORTH, R., *Cosmopolitanism and International Relations Theory*, Cambridge, Polity Press, 2011. Anteriormente, hemos defendido la existencia de un cosmopolitismo blando en: GARCÍA SEGURA, C. Y PAREJA ALCARAZ, P., "La inspiración cosmopolita de la responsabilidad de proteger: construcción normativa y disensos", en GARCÍA SEGURA, C., *op. cit*. nota 27, pp. 64-116.

ta mediante marcos de negociación multilaterales, a partir de la aceptación del carácter global y transnacional de los principales retos contemporáneos. Si bien los Estados participan en el avance del cosmopolitismo no son sus principales impulsores sino que el espíritu universalista proviene de organizaciones internacionales, como Naciones Unidas, y de actores de la sociedad civil global (oenegés, movimientos sociales transnacionales, activistas) que, en la mayoría de casos, actúan cooperativa y coordinadamente, en campañas transnacionales para conseguir cambios mediante normas de carácter cosmopolita (en ámbitos como el medioambiente, los Derechos Humanos o la Seguridad Humana). El resultado es un cosmopolitismo plural y blando en el que conviven diferentes percepciones, ideologías y criterios. Son estas dos características –pluralidad y suavidad– las que permiten que arraigue en la sociedad internacional y que no sólo actúe como límite discursivo, sino también como marco de referencia para la conducta de los Estados y otros actores. El concepto de cosmopolitismo blando refleja las ambigüedades y complejidad de la tensión cosmopolita y describe una incipiente realidad cosmopolita moderada, limitada y plural situada a medio camino entre las utopías de un gobierno mundial y la defensa estatal del statu quo. Es un cosmopolitismo que se inspira en el *corpus* cosmopolita como ideal o fuente de inspiración más que como guía programática para la acción política. Dista de ser universal y homogéneo. Tiene un desarrollo espacial desigual y está más arraigado en los países occidentales que en las potencias emergentes, las cuales siguen prefiriendo el modelo *westfaliano*. Esta última afirmación debe matizarse ya que los gobiernos occidentales, presionados por la sociedad civil, abrazan un discurso cosmopolita pero, en la práctica, se resisten a elaborar políticas coherentes con él generando un *decalatge* entre la defensa retórica de principios cosmopolitas y su plasmación en normas cosmopolitas.[33] Su carácter blando o suave se plasmaen la no obligatoriedad de las normas que genera: normas no juridificadas y no vinculantes. Se le denomina así por contraposición a un cosmopolitismo duro que se inclinaría por la construcción de un gobierno mundial para gestionar los retos globales. Además, su naturaleza blanda o suave se manifiesta en la conciliación entre la preservación del Estado y de sus intereses como elementos centrales de la sociedad internacional y la paulatina articulación de mecanismos e instrumentos de gobernanza global que responden a la voluntad cosmopolita de ofrecer respuestas universales y centradas en los individuos. El cosmopolitismo suave o blando

33 BOUZA, N., GARCÍA, C. y RODRIGO, A., "Hacia *Wordfalia*? La gobernanza política y jurídica del interés público global", en BOUZA, N., GARCÍA, C. y RODRIGO (eds.), *La gobernanza del interés público global*. Madrid, Tecnos, 2015, pp. 29-53. Consecuencia de este cosmopolitismo blando ha ido articulándose progresivamente un Derecho internacional verdaderamente *público*: un sistema jurídico internacional inclusivo, complejo y abierto, con una estructura comunitaria cada vez más densa e institucionalizada. CASANOVAS, O., "La dimensión pública del Derecho internacional" en *Ibíd.*, pp. 57-75.

refuerza las cuatro condiciones ideacionales que, a juicio de Barry Buzan y George Lawson, fundamentan el nuevo "globalismo descentralizado": la reducción de las tensiones y diferencias ideológicas que, sin embargo, no se traducen en la imposición de una única cosmovisión; la mayor incidencia de las consideraciones de naturaleza geoeconómica frente a las de carácter geopolítico en la toma de decisiones de los actores internacionales (aunque algunos autores lo cuestionan, como veremos a continuación); el afianzamiento de varias instituciones primarias heredadas del período de hegemonía europea como el mercado, el Derecho internacional o la diplomacia; y la existencia de una cierta inclinación normativa favorable al regionalismo.[34]

Los planteamientos cosmopolitistas –aunque suaves o blandos– responden a una visión moral, normativa y cooperativa de las relaciones internacionales que opta por mecanismos de gobernanza global para responder a los retos globales y resolver los conflictos de intereses entre los diferentes actores internacionales. Se contrapone a su contraria: la visión conflictiva de las relaciones internacionales entendidas como lucha por el poder.

2.2. El significado del regreso de la geopolítica: realidad o construcción política

La euforia cosmopolita, impulsada por el fin de la bipolaridad y la pujante globalización, pronto se vio aplacada por el aumento de la conflictividad internacional, una conflictividad de contornos diferentes a la de la post-segunda guerra mundial, pero conflictividad al fin. El multilateralismo que parecía triunfante pocos años antes fue arrinconado por la política unilateralista de la potencia estadounidense[35]. La emergencia de nuevas potencias, que desplazaban progresivamente a las tradicionales en el tablero del poder mundial -Occidente era arrinconado por una Asia dinámica y productiva que adquiría mayor peso en la economía mundial–[36] planteó un escenario de competitividad y rivalidad que fue políticamente interpretado como conflictivo. Del desplazamiento de Estados Unidos en el tablero del poder mundial se derivaba, errónea o intencionadamente, que el orden liberal impulsado por los Estados Unidos llegaba a su fin amenazado por un orden

---

34 BUZAN, B. y LAWSON, G., *The Global Transformation. History, Modernity and the Making of International Relations*, Cambridge, Cambridge University Press, 2015, pp. 275-293.

35 Véase, entre otros, HARDT, M. y NEGRI, A., *Empire*, Cambrige, Harvard University Press, 2000; GARCÍA SEGURA, C. y RODRIGO HERNÁNDEZ, A. (coords,), *El imperio inviable: el orden internacional tras el conflicto de Irak,* Madrid, Tecnos, 2004.

36 BORTHWICK, M., *Pacific Century: The Emergence of Modern Pacific Asia*, Boulder, Westview Press, 1998; HSIUNG, J. C., *Twenty-First Century World Order and the Asia Pacific*, Nueva York, Palgrave, 2001.

no liberal de inspiración asiática.[37] Si en los años noventa se decía que la geoeconomía había desplazado a la geopolítica, con el nuevo siglo se empezó a elaborar el discurso del retorno a la guerra fría y de la geopolítica. Todas estas interpretaciones son narrativas político–ideológicas que, en base a hechos empíricos, focalizan el análisis en un aspecto de la realidad y por ello ofrecen visiones más o menos conflictivas o cooperativas de las relaciones internacionales.

La idea central del remplazo de la geopolítica por la geoeconomía[38] tras la guerra fría defendía que la tradicional rivalidad de las naciones dejaba de ser librada en términos territoriales y a través de medios militares y pasaba a serlo en términos económicos y a través de medios económicos.[39] El discurso, en parte, surgía como una advertencia al gobierno de Estados Unidos, que seguía obstinado en una concepción geoestratégica y militar de su política exterior que le perjudicaba, a la vista del éxito de otros Estados –medido en términos de crecimiento económico– que habían optado por la estrategia geoeconómica. Los Estados que mejor se habían situado en el nuevo escenario geoeconómico eran China y Rusia, principales rivales de Estados Unidos, mientras que este estaba perdiendo terreno precisamente por no haber captado la dirección geoeconómica de la nueva realidad.[40]

---

37 ACHARYA, A., *op. cit.,* nota 13; BORON, T., "Towards a post-Hegemonic Age? The end of Pax Americana", *Security Dialogue*, vol. 25, 1994, núm. 2, pp. 211-221; KUPCHAN, C. A., "After Pax Americana: Benign Power, Regional Integration, and the Sources of a Stable Multipolarity", *International Security,* vol. 23, 1998, núm. 2, pp. 40-79; LAYNE, C., "This Time It's Real: The End of Unipolarity and the Pax Americana", *International Studies Quarterly*, vol. 56, 2012, núm. 1, pp. 203-213. Hemos defendido la idea contraria en GARCIA SEGURA, C., *op. cit.,* nota 20.

38 La geoeconomía puede ser definida como la interacción entre la economía internacional, la geopolítica y la estrategia. También es considerada como una estrategia de política exterior de los Estados. SHOLVIN, S. y WIGELL, M., "Power Politics by economics means: Geoeconomics as an analytical approach and foreign policy practice, *Comparative Strategy*, vol. 37, 2018, núm. 1, pp. 73-84.

39 Este es el argumento central de LUTTWAK, E. N., "From Geopolitics to Geo-Economics, Logic of Conflict, Grammar of Commerce", *The National Interest*, núm. 20, 1990, pp. 7-23.

40 Dos de las referencias más significativas de los años noventa en las que se defienden estas ideas son el artículo de LUTTWAK, *Ibid.* y el libro de BLACKWILL, R.D. y HARRIS, J.M., *War by OtherMeans. Geoeconomics and Statecraft*, Washington y Cambridge, Congress on Foreign Relations y The Belknap Press of Harvard University Press, 1995. Robert Blakwill y Jeniffer Harris argumentaban que la lucha por el liderazgo en Asia se libraba en términos económicos y mientras que China basaba su estrategia en los "palos y zanahorias" económicos, Estados Unidos seguía con su tendencia a "desenfundar demasiado rápido las pistolas". Edward Luttwak sostenía que los Estados Unidos perdían terreno porque, en su estrategia de política exterior, separaban economía y política y estaban limitados por su compromiso con las normas del orden internacional.

Pero el predominio del discurso de la geoeconomía, como el "momento unipolar", duró poco. Ya en la primera década del siglo XXI, se popularizó el discurso del retorno de a la guerra fría.[41] Con él se daba a entender que el juego de poder entre las potencias retomaba las características de tiempos pretéritos en los que las cuestiones territoriales, vinculadas al poder militar,marcaban el curso de las relaciones internacionales. El término nueva guerra fría se ha utilizado para explicar los tensos derroteros de las relaciones entre los Estados Unidos y Rusia tras la llegada de Putin al poder en el 2000 y, por extensión, para calificar las difíciles relaciones comerciales de Estados Unidos con China.[42] Admitamos o no su pertinencia, lo que queda claro es que es un término que se ha utilizado, sobre todo desde la perspectiva estadounidense, para describir el fin del "momento unipolar", en que la superioridad del poder estadounidense era indiscutida y parecía poder dar lugar a una nueva era hegemónica o imperial de contornos diferentes a las hegemonías e imperios históricos (sin dominio territorial, ni necesidad de fuerza militar). El término llevaba implícito el descontento de la superpotencia con la nueva estructura del poder mundial que se perfilaba, una estructura multipolar compleja, en la que debe hacer frente al poder de países como Rusia y China, pero también como Brasil e India y al de otros actores no estatales.[43] La situación que se ha calificado como nueva guerra fría pone en evidencia la incapacidad o la falta de voluntad de las potencias tradicionales para integrar a las potencias emergentes. Quienes afirman que una nueva guerra fría existe se basan en la tensión de las relaciones ruso-estadounidenses desde que la Rusia de Putin se planteó reconquistar su estatus de superpotencia y en la tensión en torno al liderazgo de Asia entre Estados Unidos

41 Varios libros de caràcter periodístico contribuyeron a difundir el término: GADDIS, J.L., *The Cold War: A New History*, Nueva York, Penguin Press, 2005; MACKINNON, M., *The New Cold War: Revolutions, Rigged Elections and Pipeline Politics in the Former Soviet Union*, Nueva York, Carroll & Graf Publishers, 2007; LUCAS, E., *The New Cold War: Putin's Russia and the Threat to the West*, Nueva York, Palgrave Macmillan, 2008. El ámbito académico se hizo eco del término y se inició el debate sobre la existencia o no de una nueva Guerra fría: RYWKIN, M., "Russia: In Quest of Superpower Status", *American ForeignPolicyInterests,* vol. 30, 2008, núm. 1, pp. 13-21; SAKWA, R.,"'New Cold War' or TwentyYears' Crisis? Russia and International Politics", *International Affairs*, Vol. 84, 2008, núm. 2, pp. 241-51; MÜLLERSON, R., "Promoting Democracy without Starting a New Cold War?", *Chinese Journal of International Law*, vol. 7, 2008, núm. 1, pp. 1-31; HARASYMIW, B.,"Rusia, the United States and the New Cold War", *Journal of Military and Strategic Studies*, vol. 12, 2010, núm. 2, pp. 1-31.

42 WESTAD, O.A., "Has a New Cold War Really Begun? *Foreign Policy,* 27 marzo, 2018, https://www.foreignaffairs.com/articles/china/2018-03-27/has-new-cold-war-really-begun?; KAPLAN, R., "A New Cold War Has Begun", *Foreign Policy*, enero 2019, https://foreignpolicy.com/2019/01/07/a-new-cold-war-has-begun/
WEINSTEIN, K. R., "A New Cold War Between The US and China", *Aspen Review,* núm. 1, 2019, pp. 10-14. https://www.aspen.review/article/2019/new-cold-war-us-china/

43 GARCIA SEGURA, C., *op. cit*, nota 20, pp. 50-51.

y China. Los que niegan que la situación actual se asemeje a la de la guerra fría se apoyan en el fin de la bipolaridad, en la inexistencia de confrontaciones ideológicas entre capitalismo y socialismo y en la pérdida de centralidad del escenario nuclear. Hay tensión entre Estados Unidos y Rusia y entre Estados Unidos y China, pero hay más cambios (política de alineamientos, importancia creciente del *softpower* sobre el *hardpower*) que continuidades (competición energética) respecto a sus relaciones bilaterales de la era de la guerra fría.[44] A pesar de la retórica más o menos alarmista, dura o desafiante de los líderes políticos, las tensiones actuales no pueden plantearse como conflictos absolutos, de suma nula, porque las partes implicadas (sean estas Estados Unidos, Rusia, China o la Unión Europea) saben que la globalización y la interdependencia económica les impone políticas de acomodo y de gestión de las rivalidades en términos de complementariedad. Las potencias emergentes han entendido que, para alcanzar la cuota de poder que ansían, deben convencer más que imponer. De lo contrario, como argumenta Guilio Gallaroti, corren el riesgo de obtener el resultado opuesto y desgastar inútilmente el poder que tienen actualmente. Las potencias emergentes han entendido que para aumentar su influencia deben perseguir el tipo correcto de poder, que este autor denomina el *poder cosmopolita*. Este consiste en un en una correcta combinación de *soft* y *hard power*, que conlleva el fortalecimiento del *softpower*, la reducción del *hardpower* y una diversificación óptima.[45]

Una década más tarde, el discurso político que se hacía eco del empeoramiento de las relaciones internacionales entre las grandes potencias ya no sugería una nueva guerra fría sino un retorno a la geopolítica porque las cuestiones territoriales y las soluciones militares, propias de otros tiempos que se habían dado por superados, reaparecían en escena con fuerza renovada. La crisis de Crimea de 2014, que acabó con la anexión rusa de la península ucraniana es el hecho más representativo del giro geopolítico protagonizado por Rusia. La militarización creciente del Mar del Sur de China, sería el acontecimiento más significativo de contornos geopolíticos protagonizado por la potencia asiática. El artículo de Walter Russell Mead ha popularizado el discurso del retorno a la geopolítica.[46] Su tesis es

---

44 HARASYMIW, B., *op. cit.,* nota 41, pp. 26-31; WEINSTEIN K, R., *op. cit*. nota 42, p. 13.

45 GALLAROTI, G.M, *Cosmopolitan Power in International Relations. A Synthesis of Realism, Neoliberalism and Constructivism,* Cambridge, Cambridge University Press, 2010, pp. 49 et ss. El concepto de *poder cosmopolita* ha sido criticado por apenas diferenciarse del concepto de *smart power* acuñado por Joseph Nye: véase, MATTERN, J.B., "Review: Rethinking National Power? From IR Theory to Foreign Policy Practice", *International Studies Review,* vil. 14, 2012, núm. 2, pp. 358-360). Sobre el concepto de *smart power*, véase: NOSSEL, S., "Smart Power", *Foreign Affairs*, vol. 83, 2004, núm. 2, pp. 131-142; ARMITAGE, R.L. y NYE, J. S., *Commission on Smart Power. A smarter, more secure America*, Washington, CSIS Press, 2007; NYE, J.S., "Get Smart, Combining Hard and Soft Power", *Foreign Affairs*, vol. 88, 2009, núm. 4, pp.160-163.

46 MEAD, W.R., *op. cit.,* nota 18.

que los Estados Unidos y la Unión Europea habrían interpretado mal el significado del colapso de la URSS al identificar el triunfo del capitalismo liberal sobre el comunismo con la obsolescencia del poder duro. Por ello, porque el pretendido "fin de historia" se ha acabado y hemos vuelto a la geopolítica, es necesario adoptar de nuevo una estrategia geopolítica para frenar a las potencias rusa y china.[47] Este autor atribuye a las potencias occidentales una voluntad multilateralista y pacificadora y una inclinación a centrarse en la construcción del orden basado en la liberalización económica, la defensa de los Derechos Humanos y la no proliferación nuclear, a través de la gobernanza global, que sería discutible. En los primeros años de la post-guerra fría, coincidiendo con el resurgir de los planteamientos político-filosóficos cosmopolitas, se pensó que los únicos desafíos al orden liberal vendrían de los "Estados canallas" que no lo aceptaban. Por exceso de optimismo o por falta de perspicacia política, se daba por supuesto que los Estados díscolos caerían por su propio peso a causa de sus disfuncionalidades derivadas de la obsolescencia de sus instituciones políticas y sociales.[48] Por contra, Rusia, China e Irán –que Walter R. Mead califica de "potencias revisionistas", descontentas con los acuerdos geopolíticos de la post-guerra fría– representarían un mayor peligro porque habrían optado por una orientación geopolítica. En realidad, son potencias que ya no se resignan a desempeñar un rol secundario ni en las relaciones internacionales ni en los asuntos regionales. Comparten el convencimiento de que Estados Unidos representa un impedimento a sus ambiciones. China no puede tolerar el dominio estadounidense en el Mar del Sur de China y Rusia no está dispuesta a admitir la penetración estadounidense, o europea, en la que sigue considerando su área de influencia. Ambas potencias coinciden en no estar dispuestas a admitir un mundo dominado por Estados Unidos.[49] El hecho de tener agendas y capacidades muy diferentes hace que no puedan ofrecer una oposición sistemática y global al orden liberal y, en lugar de desafiar frontalmente el statu quo, intenten remover las normas e instituciones que lo sostienen.[50] El resultado

---

47 Walter R. Mead afirma que en Occidente se leyó erróneamente el mensaje del libro de Francis Fukuyama (FUKUYAMA, F., *op. cit.* nota 19): se confundió la que era una declaración sobre la ideología con una declaración sobre el poder y, en consecuencia, se interpretó el fin de la lucha ideológica como el fin de la geopolítica. MEAD, W.R., "The End of the History Ends", *The American Interest,* 2 de diciembre 2013, disponibleenhttps://www.the-american-interest.com/2013/12/02/2013-the-end-of-history-ends-2/

48 *Ibíd*, p. 72. Walter R. Mead añade que los atentados del 11S convirtieron al terrorismo trasnacional en la nueva amenaza del orden liberal pero, nuevo error, se pensó que "la guerra contra el terrorismo", declarada por George W. Bush sería fácil de ganar. *Ibíd*, p.73.

49 COX, R., "No just 'convenient': China and Russias's new strategic partnership in the age of geopolitics", *Comparative Politics*, vol. 1, 2016, núm. 4, pp. 317-334.

50 MEAD, W.R., *op. cit.*, nota 18, p. 74. Consideramos cuestionable esta última afirmación de Walter R. Mead en la que parece no distinguir entre orden y poder. La búsqueda de mayores cuotas de poder en las instituciones del orden existente no debe confundirse con el cambio de los principios e instituciones del orden.

de la opción geopolítica de las potencias revisionistas es, siguiendo a Walter R. Mead, la revitalización de los conflictos geopolíticos en Asia (donde el nacionalismo japonés y el ascenso militar de China se alimentan mutuamente), en Europa (donde la ya mencionada crisis de Crimea es el ejemplo más obvio) y en Oriente Medio (donde los conflictos de larga duración siguen sin resolverse).

Una versión políticamente menos significada y académicamente más elaborada del resurgir de la geopolítica es la ofrecida por Stefano Guzzini y colaboradores. En su opinión, el renacer de la geopolítica se traduce una oleada de reseguritización de la agenda de las relaciones internacionales que había sido "deseguritizada" tras la guerra fría.[51] Su conclusión, lejos de ser determinista y establecer un vínculo directo entre fin de la guerra fría y retorno de la geopolítica, asocia la mayor o menor posibilidad de conductas de carácter geopolítico a las crisis de identidad y a otros factores.[52] Desde posiciones constructivistas cuestionan que los hechos sean los que determinan el retorno a la geopolítica. La clave –de naturaleza ideacional– está en la interpretación que se hace de ellos a través de los discursos.[53] Frente a la idea que la geopolítica reaparece "a pesar del fin de la guerra fría", entendida como el fin de la lucha ideológica y la demostración de la posibilidad histórica de cambio pacífico, afirman que resurge "a causa de ella" y que debe entenderse en el contexto de varias crisis de identidad[54] que genera la desintegración de la Unión Soviética y el fin de la bipolaridad. De los diferentes casos empíricos que analizan,[55] concluyen que el recurso a opciones geopolíticas sirve para responder a la ansiedad ontológica creada por las crisis de identidad que genera el vacío ideacional que sigue a la caída del muro de Berlín. Por otra parte, e indirectamente, establecen un vínculo entre el resurgir del cosmopolitis-

---

51 GUZZINI, S. (ed), *The Return of Geopolitics in Europe? Social Mechanisms and Foreign Policy Identity Crises,* Cambridge, Cambridge University Press, 2013, p. 5

52 La ideología de una potencia insatisfecha y la existencia de una cultura política materialista aumentan la posibilidad de respuestas geopolíticas; la existencia de una tradición de investigación por la paz, de instituciones que garanticen la independencia de los expertos respecto a políticos y militares, y la asistencia de expertos militares y estratégicos la reducen. *Ibíd.* p. 248.

53 *Ibíd.*, p. 3

54 Las crisis de identidad ocurren cuando los discursos sobre la política exterior de un país o sobre el interés nacional tienen problemas de continuidad porque la autoimagen y los roles que se habían dado por supuestos se ven abiertamente desafiados o eventualmente minados. El estudio distingue entre crisis de "no identidad" (como el caso de Rusia en que, tanto su identidad anterior como superpotencia, como la auto-comprensión de su identidad actual –diferente a la URSS y a la Rusia zarista– están amenazadas), crisis porque "la identidad previa ya no puede mantenerse" (que agrupa casos muy diferentes como los de Italia y Turquía, Alemania o República checa) y, finalmente, las crisis de quienes "aun no tienen una identidad" (caso de Estonia). *Ibíd.,* p. 3 y 246-247.

55 Alemania, Estonia, Federación Rusa, Italia, República Checa y Turquía.

mo y la resistencia soberanista y el resurgir de los nacionalismos estatales: "Kant hace posible de nuevo a Hobbes",[56] lo que puede ser interpretado en el sentido de que las ideas cosmopolitas y universalistas de los años noventa, en un contexto de crisis de identidad, generan reacciones realistas de carácter nacionalista en aquellos Estados que temen verse absorbidos por las ideas y las instituciones del orden liberal.

Por lo tanto y como conclusión a este apartado afirmamos que en la actualidad coexisten distintas lecturas de la realidad formuladas en narrativas políticas que reflejan diferentes parcelas de la compleja realidad internacional. En esta coexisten relaciones trasnacionales de inspiración cosmopolita (aunque sea de un cosmopolitismo blando o suave), relaciones internacionales y regionales cooperativas (a las que se tiende dedicar poca atención mediática y académica), relaciones internacionales de rivalidad (en las que el juego del poder entre potencias –tradicionales y emergentes– se desarrolla en un tablero geoeconómico) y relaciones internacionales conflictivas (en las que se vuelve al tradicional tablero geopolítico, sin que por ello, pueda hablarse de nueva guerra fría). Las conexiones de interdependencia intensificadas en el contexto de la globalización impiden planteamientos de suma nula. Y dado que la estabilidad del orden es un requisito para que las potencias emergentes puedan seguir creciendo, estas no tienen ningún interés en desestabilizarlo. Como veremos a continuación, en contraposición al discurso que las tilda de revisionistas, la realidad demuestra que se han convertido en potencias afianzadoras del orden.

3. EL PROCESO DE CREACIÓN DE NORMAS GLOBALES Y LAS POTENCIAS EMERGENTES.

Las normas globales son el resultado de la oleada de retos globales de los años noventa, incluyendo los asociados a las nuevas tecnologías de la información y comunicación (TIC) y a la emergencia de una creciente sociedad civil global. Responden a la necesidad de encararlos con estrategias y tácticas sofisticadas que aprehendan la complejidad de los mismos.[57] Este trabajo parte de una concepción amplia del proceso de creación de normas globales[58] que se caracteriza, en primer lugar, por utilizar una noción de *normas* que se aparta de la clasificación binaria de las mismas como "derecho" y "no-derecho". Utilizamos

---

56 GUZZINI, S., *op. cit,* nota 51, p. 5.

57 MARTINSSON, J., "Global Norms: Creation, Diffusion, and Limits", *CommGAPDiscussion Paper*, agosto 2011, p.2.

58 BRÖLMAN, C. y RADI, Y. "Introduction: International law making in a global world", en-BRÖLLMAN, C. and y RADI, Y. (eds.), *Research Handbook on the Theory and Practice of International Law-Making*, Cheltenham, Edward Elgar Publishing, pp. 1-9 (2).

una concepción sociológica y politológica, propia de las Relaciones Internacionales, que las define como "las expectativas compartidas o estándares de conducta apropiada aceptadas por los estados, las organizaciones internacionales gubernamentales y/o los actores no gubernamentales de tipos diversos".[59] La definición de norma de Peter J. Katzenstein, aún más general, añade sin embargo otro elemento clave ausente en la anterior definición, la identidad compartida: una norma define "las expectativas colectivas sobre la conducta apropiada de los actores que comparten una identidad".[60] Desde la Teoría normativa y constructivista de las Relaciones Internacionales, las normas son concebidas como principios que reúnen dos características interrelacionadas: tienen fuerza prescriptiva (son códigos que definen lo que los actores deben o no hacer en determinadas circunstancias) y evaluativa (son invocadas para aprobar o condenar determinadas conductas) y son ampliamente aceptadas e internalizadas por un comunidad particular. Pueden ser codificadas jurídicamente o pueden ser internalizadas sin haber sido institucionalizadas formalmente.[61] En algunas situaciones, las normas operan como reglas que definen la identidad de los actores, es decir, tienen efectos constitutivos: especifican qué acciones harán que una identidad particular sea reconocida. En otras, las normas funcionan como estándares que especifican la representación de una identidad ya definida. En estos casos las normas tienen efectos regulativos: establecen estándares de conducta correcta.[62] Martha Finnemore y Duncan Hollis desglosan la norma en cuatro elementos constitutivos: la identidad, que hace referencia al grupo al que aplica la norma; la conducta, que identifica las acciones específicas que se requieren de la comunidad; la corrección, que establece las bases sobre las cuales las normas etiquetan una conducta como apropiada o inapropiada; y las expectativas colectivas, que apuntan al carácter social e intersubjetivo de las normas, en tanto que construcciones sociales.[63]

El concepto socio-politológico de norma es a la vez compatible con la idea, proveniente del Derecho, de la normatividad jurídica entendida como una escala

---

59 KHAGRAM, S. J., RIKER, V., y SIKKINK, K., *Restructuring World Politics: Transnational Social Movements, Networks, and Norms*, Minneapolis, University of Minnesota Press, 2002, p. 14.

60 KATZENSTEIN, P.J., "Introduction: Alternative Perspectives on National Security" en KATZENSTEIN, P.J. (ed), *The Culture of National Security: Norms and Identity in WorldPolitics,* Nueva York, Columbia University Press, 1996, pp. 1-27 (5).

61 ERSKINE, T. y CARR, M., "Beyond 'Quasi-Norms': The Challenges and Potenctial of Engaging with Norms in Cyberspace", en OSULA, A-M. y RÕIGAS(eds,), *International CyberNorms. Legal, Policy & Industry perspectives,* Estonia, NATO CCDCOE, 2016, pp. 87-109 (89 et ss.).

62 *Ibíd*.

63 FINNEMORE, M. y HOLLIS, D.B., "Constructing Norms for Global Cybersecurity", *The American Journal of International Law,* vol. 11, 2016, núm. 2, pp. 425-479 (439-443).

progresiva,[64] de gran utilidad para identificar una gradación en los efectos jurídicos. Esta concepción resulta idónea para examinar tanto los procesos de creación de normas jurídicas más formalizados (tratados internacionales), como aquellos en los que se adoptan normas generales de conducta no formalizadas o que no crean obligaciones jurídicas vinculantes (por ejemplo, códigos de conducta o proyectos de conclusiones).

La concepción de norma de la que partimos entiende que su *creación* incluye una diversidad de vías de generación y de procesos de adopción de normas tales que: el establecimiento de normas jurídicas; las iniciativas de participación múltiple; las redes normativas globales; y las coaliciones transnacionales de promoción de intereses.[65] La creación de normas jurídicas incluye a su vez: los procedimientos formalizados de creación de normas jurídicas internacionales como son los tratados internacionales o las resoluciones de las organizaciones internacionales; otros procesos difusos de interacción entre actores jurídicos como estándares, códigos de conductas, etc.; yprocesos sociales que pueden inducir consecuencias jurídicas de determinadas prácticas sociales (costumbre internacional). Martha Finnemore y Duncan Hollis conceden una centralidad fundamental al proceso de creación de las normas. Según estos autores, el poder real de las normas reside en el *proceso* por el cual se forman y evolucionan: "el viaje importa tanto como el destino" ya que da forma al contenido y carácter de la norma.[66] En el análisis de una norma, afirman, no sólo importa el contenido (qué dice la norma) sino quién la acepta (qué comunidad, qué identidad) y dónde es aceptada (en qué contexto político-institucional). Por ello, conocer cómo se construyen las normas, captar el carácter social, dinámico y evolutivo de las normas, así como su interacción con otras normas y contextos, es clave para una correcta comprensión de las mismas.

El calificativo *globales* que acompaña al término *normas* significa, por una parte, que la actividad normativa a la que nos referimos trasciende las fronteras jurídicas nacionales; por otra parte, que no está limitado al marco de las relaciones interestatales; y, por último, que pretende aprehender o dar cabida a la aspiración de universalidad de las normas destinadas a regular y proteger el interés público global y los valores cosmopolitas.[67]

---

64 CHINKIN, C.M., "The Challenge of Soft Law: Development and Change in International Law", *International and Comparative Law Quarterly*, vol. 38, 1989, núm. 4, pp. 850-866 (850).

65 MARTINSSON, J., *op. cit.*, nota 57, p.3.

66 FINNEMORE, M. y HOLLIS, D.B., *op. cit.*, nota 63, p. 429.

67 Los conceptos básicos utilizados en este apartado son los establecidos en: GARCÍA, C., PAREJA, P. y RODRIGO, A. J, "La creación de normas globales: entre el cosmopolitismo *soft* y el resurgir de *Westfalia.* Concept paper*", Orbis Working Paper,* 2019/1. https://www.upf.edu/web/orbis/orbis-working-papers.

A continuación, vamos a examinar, desde la perspectiva de las Relaciones Internacionales, la dinámica de los procesos de creación de normas y los roles normativos de los diferentes actores, así como la naturaleza y el carácter del rol de las potencias emergentes en el proceso de creación normativa.

3.1. Los procesos normativos y los roles normativos en el orden internacional[68]

El interés por las normas, consideradas instrumentos de la política mundial[69], se introdujo en la disciplina de las Relaciones Internacionales de la mano del "giro constructivista".[70] Antes, la disciplina, dominada por el realismo y el neorrealismo, no les había prestado atención, centrada como estaba en los instrumentos de poder político-militares. El Derecho y las normas no eran considerados sino meros instrumentos del poder. Desde los años setenta del siglo pasado, el liberalismo y el neoliberalismo habían introducido el estudio de los regímenes internacionales, y con ellos el de las normas, pero solo en tanto que uno de sus elementos constitutivos.[71]Los liberales entendían los regímenes como elementos del orden internacional que regulaban las acciones de los actores en un ámbito determinado, creando expectativas de conducta y, por tanto, reduciendo la incertidumbre y la inseguridad en las áreas que regulaban. El carácter cooperativo y pacificador de las relaciones internacionales que los análisis liberales les atribuían contrastaba con las posiciones críticas que los interpretaban como mero resultado de las relaciones de poder sin capacidad transformadora de la conflictividad internacional.[72] En cualquier caso, los estudios se centraban sobre todo en la descripción de los regímenes más que en su formación. No sería hasta los años noventa que se iniciarían los estudios centrados en la dinámica de las normas ("primera ola"), orientados a destacar la importancia de las mismas, como construcciones

---

68 Una primera formulación de las ideas contenidas en este apartado y el siguiente se encuentra en GARCÍA SEGURA, C., *op. cit.*, nota 20.

69 FINNEMORE, M. y K. SIKKINK, "International Norm Dynamics and Political Change", *International Organization,* vol. 52, 1998, núm.4, pp. 887-917 (891).

70 CHECKEL, J. T., 'The constructivist turn in International Relations theory', *World Politics*, vol. 50, 1998, núm. 2, pp. 324-348.

71 Aunque autores como John G. Ruggie (RUGGIE, J., "International Responses to Technology: Concepts and Trends", *International Organization,* vol. 29, 1975, núm. 3, pp. 557-583) o Robert Keohane y Joseph Nye (KEOHANE, R. O. y NYE, J.S., *Trasnational Relations and World Politics,* Cambridge, Harvard UniversityPress, 1973) habían utilizado el concepto de regímenes internacionales una década antes, fue la publicación de la obra de Stephen Krasner, en 1983, la que popularizó el concepto y el estudio de los regímenes internacionales. KRASNER, S. (ed.), *International Regimes,* Ithaca, Cornell University Press, 1983.

72 STRANGE, S., "Cave! Hic Dragons: A Critique of Regime Analysis", *International Organization,* vol. 36, 1982, núm. 2, pp. 479-496.

sociales, explicativas de las relaciones internacionales, frente a la lógica realista basada exclusivamente en el poder interestatal.[73] Estos primeros estudios tenían un enfoque estático: analizaban el resultado, es decir, el contenido de las normas, no en el proceso que las había generado, y menos en su evolución.[74] El trabajo seminal de Martha Finnerore y Kathryn Sikkink, que sigue siendo un referente, introdujo una perspectiva dinámica al plantear el estudio del ciclo de las normas. El ciclo de una norma, afirman, se compone de tres estadios: la emergencia de la norma, su expansión (cascada normativa) y su internalización.[75] Muy celebrado en su momento, posteriormente ha sido criticado por sus opciones analíticas y por las premisas ideológicas que lo inspiran. En el primer orden de críticas se le acusa de tratar las normas como variables independientes, relativamente estáticas;[76] de asumir que las categorías de creadores y de receptores de normas son fijas y los actores no cambian de roles; y de asumir que a través de la socialización, los receptores se integran pasivamente en la comunidad de Estados occidentales. Las críticas de orden ideológico aluden al sesgo liberal derivado de centrarse exclusivamente en la difusión de normas liberales y cosmopolitas; al hecho de establecer, indirecta e implícitamente, valores a las categorías de creadores (élite ilustrada) y receptores (mayoría no ilustrada de seguidores); a que operan sobre la base de una idea lineal del progreso que se plasma en la presentación de los casos de resistencia al cambio normativo liberal como fracasos;[77] y, en definitiva, a que, al no contemplar la contestación, parecen dar a entender que la resistencia a las normas cosmopolitas es ilegítima o immoral.[78]

Los trabajos posteriores de estas autoras, así como aquellos que se consideran parte de la "segunda ola" de trabajos sobre las normas, ya incluyen el estudio del

---

73 CORTELL, A. P, y DAVIS, J. W. "Understanding the Domestic Impact of International Norms". A Research Agenda", *International Studies Review*, vol. 2, 2000, núm. 1, pp. 65-87, p. 66; HOFFMAN, M., "Norms and Social Constructivism in International Relations" en DENEMARK, R. A., y MARLIN-BENNETT, E. (eds.), *The International Studies Encyclopedia*, Nueva York, Wiley-Blackwell, 2017 (versión en línea), pp. 1-19, p. 3.

74 WUNDERLICH, C., "Theoretical Approaches in Norms Dynamics", en MÜLLER, H. y WUNDERLICH, C. (eds.), *Norms Dynamics in Multilateral Arms Control: Interests, Conflicts and Justice,* Athens, Georgia University Press, 2013, pp. 20-47, p. 20.

75 FINNEMORE, M. y SIKKINK, K., *op. cit,* nota 69, pp. 895 et ss.

76 Una concepción más dinámica define el proceso normativo como aquel por el que las normas y los regímenes se forman, se difunden, se internalizan y, una vez establecidos, se trasforman reforzándose, debilitándose o erosionándose. WUNDERLICH, C., *op. cit.,* nota 74, p. 24.

77 BLOOMFIELD, A., "Norm antipreneurs and theorising resistance to normative change", *Review of International Studies,* vol. 42, 2016, núm. 2, pp. 310-333, (313-314).

78 ACHARYA, A. "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism", *International Organization*, vol. 58, 2004, núm.2, pp. 239-275, p. 242 y *Rethinking Power, Institutions and Ideas in World Politics. Whose IR?*, Nueva York, Routledge, 2014.

proceso de creación normativa desde una perspectiva dinàmica –evolución, cambio y transformación– y abordan las cuestiones normativas de una forma abierta: qué normas importan[79], cómo, cuándo y por qué las normas cambian y hasta qué punto lo hacen.[80] Para Martha Finnemore y Duncan Hollis, el dinamismo, el proceso, ha pasado a ser un rasgo central del ciclo normativo: el cambio, o el potencial de cambio, es un rasgo inherente a todas las normas, cualquiera que sea su etapa de desarrollo. Aunque el "cultivo" de una norma culmina cuando su contenido se da por sentado, ello no implica que sea el final del ciclo y mucho menos hay que asumir que la norma ha quedado fijada de una vez por todas y que ya no cambiará. Al contrario, afirman, las normas están en constante evolución ya que cada vez que un actor sigue una norma la está interpretando. Así asumen que las normas cambian con los grupos sociales a los que se aplican. En este sentido las normas son productos y el proceso es parte de la norma.[81] En la línea de los trabajos de Wayne Sandholtz sobre el cambio normativo y de Antje Wiener sobre la contestación,[82] los trabajos de la "segunda ola" entienden los sistemas normativos como sistemas dinámicos en los que las normas evolucionan a través de la interacción con el contexto[83] y pueden transformarse a lo largo del proceso de difusión.[84] Por otra parte, las etapas del ciclo normativo no son compartimentos estancos, claramente delimitados. Por ejemplo, la etapa de emergencia de una nueva norma puede identificarse con la transformación de una anterior y no únicamente la creación de una norma *ex novo*. En segundo lugar, en los análisis de la "segunda ola", las normas pasan a tener un carácter plural en tanto que resultado de una variedad de procesos llevados a cabo por actores con múltiples identidades. Los trabajos más recientes también amplían las categorías de actores en referencia a las normas y añaden a los roles tradicionales (creadores o emprendedores y receptores normativos) los de

---

79 ACHARYA, A., *Whose Ideas Matter? Agency and Power in Asian Regionalism,* Ithaca, Cornell University Press, 2009.

80 Se consideran autores de la segunda ola, entre otros, Antje Wiener, Alan Bloomfield y Shirley Scott, Wayne Shandholtz y Amitav Acharya. La clasificación corresponde a: CORTELL, A. P, y DAVIS, J. W. *op.cit,* nota 73.

81 FINNEMORE, M. y HOLLIS, D., *op. cit.*, nota 63, pp. 453-454.

82 La contestación –actividad social que implica objeción– es un elemento explicativo clave de la dinámica normativa. Engloba una gama de prácticas sociales que, discursivamente, expresan desacuerdo con las normas y que varían mucho en la modalidad que adoptan. WIENER, A., *A Theory of Contestation,* Nueva York, Springer, 2014, véase especialmente el cap. 1, pp. 1-15; SANDHOLTZ, W., 'Dynamics of international norm change: Rules against wartime plunder', *European Journal of International Relations*, vol. 14, 2008, núm, 1, pp. 101–131, (103 et ss).

83 WIENER, A., "Contested Meanings of Norms: A Research Framework", Comparative European Politics, vol. 1, 2007, núm. 5, pp. 1-17, pp. 7-10 (6).

84 BLOOMFIELD, A. y S COTT, S.W., "Norms antipreneurs in world politics", en BLOOMFIELD, A. Y SCOTT, S.W. (eds.), *Norms Antipreneurs and the Politics of Resistance to Global Normative Change,* Londres, Routledge, 2017, pp. 1-19.

anti-emprendedores normativos, adoptado por Alan Boomfield, Shirley Scott y colaboradores, y de *resistentes creativos,* utilizado por Malcolm Campbell-Verduyn.[85] El primero aplica a los actores que se resisten al cambio y favorecen la continuidad de las normas existentes[86] y el segundo a aquellos que, admitiendo parte del cambio propuesto por los emprendedores, contestan ciertos aspectos y proponen otras versiones del mismo con planteamientos más "positivos" que los de los anti-emprendedores.[87] Estos trabajos, además, comparten la idea de que el proceso normativo no es unidireccional y de que las potencias emergentes, y en general los países no occidentales, pueden tener otras visiones de la conformación y contenido de las normas globales.[88] La socialización normativa deja de ser concebida como un proceso unidireccional a través del cual las potencias occidentales socializan a los Estados no occidentales y pasa a ser entendida como un proceso bidireccional en el que los Estados no occidentales son también agentes activos que influyen sobre el contenido y los resultados de los procesos normativos.[89] Estos Estados pueden intervenir en las diferentes fases del proceso normativo, desde la emergencia de la norma hasta la internalización de la misma. Al internalizar la norma, los Estados periféricos la "localizan". La localización consiste en la adaptación de las normas a las tradiciones y prácticas propias. Las ideas/normas que mejor encajan con las tradiciones locales son las mejor recibidas.[90] Cuando las normas universales topan con la resistencia de algunos Estados es porque son incompatibles con normas regionales o locales profundamente arraigadas en los sistemas regionales o estatales a las que los Estados y las sociedades no quieren renunciar. En la misma dirección Johanna Martinsson sostiene que muchas iniciativas normativas globales son exitosas en primera instancia en tanto que consiguen situar las normas en la agenda global, pero que pocas de ellas se acaban traduciendo en un cambio real porque al formarse no tuvieron en cuenta las diferencias culturales, económicas y políticas o porque los Estados no las consideran relevantes para su contexto interno.[91] Desde la perspectiva del Sur global, Amitav Acharya discute la asunción liberal implícita

---

85 CAMPBELL-VERDUYN, M., "Additional categories of agency. 'Creatives resisters' to normative change in post-crisis global financial governance", en BLOOMFIELD, A. y S. V. SCOTT, *Ibíd.,* nota 84, pp. 140-158.

86 BLOOMFIELD, A. y SCOTT, S., *op. cit.,* nota 84. Alan Bloomfield distingue varios tipos de anti-emprendedores según su posición respecto a los extremos del eje cambio-resistencia normativa: emprendedores puros, emprendedores competidores, resistentes creativos y anti-emprendedores puros. BLOOMFIELD, A., *op. cit.,* nota 80.

87 CAMPBELL-VERDUYN, M., *op. cit.,* nota 85 p. 146.

88 XIAOYU, P., "Socialization as a Two-way Process: Emerging Powers and the Diffusion of International Norms", *The Chinese Journal of International Norms",* vol. 5, 2012, núm. 4, pp. 341-367, (341 y 344-345).

89 *Ibíd.,* p. 348.

90 ACHARYA, A., *op.cit,* nota 78, p, 244.

91 MARTINSSON, J., *op. cit*., nota 57, p. 15.

de que las normas universales son morales y legítimas y las regionales inmorales e ilegítimas.[92] Las normas globales no se difunden por basarse en un criterio de autoridad sino de legitimidad. Su éxito depende de cuan relevantes sean para la agenda global y de que en su formulación hayan participado cooperativamente múltiples actores provenientes de los ámbitos global, regional y local.[93]

3.2. El rol de las potencias asiáticas emergentes en los procesos normativos del orden internacional

Como hemos visto, la literatura más reciente sobre la creación de normas globales, admite el carácter dinámico y plural del proceso normativo. Considerar el dinamismo y el pluralismo supone admitir, primero, que las normas evolucionan y se transforman sin seguir necesariamente un proceso lineal y, segundo, que cada vez hay más Estados y actores participando de los procesos normativos. Esta situación puede ser interpretada como un signo de democratización de las relaciones internacionales y como una mejora de los mecanismos e instrumentos de gobernanza global. Pero las potencias tradicionales, que asisten temerosas al cambio en la estructura de poder promovido por las potencias emergentes (especialmente por las asiáticas), trasladan su inquietud al ámbito normativo y temen que el dominio occidental pueda también ser retado en el ámbito de las ideas y las normas[94] ya que asumen que tendrá un efecto homogéneo y perjudicial.[95] Sin embargo, el análisis de la realidad demuestra que no es así. Las potencias emergentes no rechazan las normas del sistema sino que articulan diferentes preferencias dentro de él que pueden desafiar la visión europea y estadounidense, o la que se supone que es esta, a menudo a través de una reafirmación del papel del Estado. Como ya hemos argumentado en el apartado segundo, se trata de una pugna por cuotas de poder en las instituciones del orden. Lo que rechazan son las jerarquías que se dan en ellas, que no reflejan la situación del reparto del poder actual y que las perjudican.[96] Cuando, puntualmente, se oponen a algunas normas, se oponen a las propuestas normativas *post-wesfalianas*, de carácter cosmopolita.[97]

---

92 ACHARYA, A., *op.cit,* nota 78,

93 MARTINSSON, J., *op. cit*., nota 57, p. 22.

94 MCLAUCHLIN, T., "Great power accommodation and the processes of international politics", en PAUL, T. V. (ed.), *Accommodating Rising Powers. Past, Present, and Future,* Cambridge, Cambridge University Press, 2016*,* pp. 293-313, p. 306; XIAOYU, P., *op. cit*., nota 88, p. 365.

95 BURKE-WHITE, W. W., "Power Shifts in International Law: Structural Realignment and Substantive Pluralism", *Harvard International Law Journal,* vol. 56, 2015, núm. 1, pp. 1-79, (2).

96 STUENKEL, O., *Post-Western World. How Emerging Powers Are Remaking Global order,* Cambridge, Polity Press, 2016.

97 TERHALLE, M., *The Transition of Global Order. Legitimacy and Contestation,* Basingstoke/Nueva York, Palgrave/Macmillan, 2015.

La voluntad de estos países de participar de una manera más firme en la creación de normas es relativamente reciente, finales de la primera década del presente siglo, ya que es posterior a su despegue económico. El giro hacia una mayor asertividad normativa de las potencias emergentes se identifica con la actitud de China ante la crisis financiera de 2008, con el desafío de las potencias emergentes a Occidente en la Cumbre de Copenhague de 2009 y con su apuesta por convertir el Grupo de los 20 (G20) en el foro más importante de cooperación económica internacional. Las potencias emergentes no actúan en bloque ni defienden los mismos intereses. No obstante, sí que se observa una tendencia común, respecto a las normas globales, caracterizada por la resistencia y contestación de aquellas que suponen una delegación de autoridad a entidades supranacionales o un refuerzo de la estructura liberal de gobernanza en los diversos ámbitos que se plantee (económico, financiero, medioambiental). Por el contrario se muestran favorables a las normas que refuerzan una concepción dura de la soberanía nacional.[98] En este sentido, el mayor protagonismo de estos Estados, puede resultar problemático para algunos regímenes –Derechos Humanos, medioambiente– pero no para el orden en su conjunto.[99] Por otra parte, cabe señalar que la oposición de las potencias emergentes a las normas de inspiración cosmopolita difiere más en la forma que en el fondo respecto a la posición de Estados Unidos y de algunas potencias occidentales. Las nuevas normas cuyos actores emprendedores son, en muchas ocasiones, actores transnacionales no estatales, son lideradas discursivamente por los Estados occidentales que, a menudo, las invalidan con su práctica política.[100] Juegan a la vez un rol de emprendedores y de anti-emprendedores. Las potencias emergentes de Asia, en cambio, adoptan una posición más coherente –el discurso y la práctica coinciden– y abierta –los gobiernos no se sienten obligados ante la presión de su opinión pública, asumiendo claramente el rol de anti-emprendedores o de resistentes creativos. Desde su nueva posición de poder, frenan algunos impulsos transformadores con propuestas alternativas. Las potencias emergentes, especialmente China, están insatisfechas con el carácter hegemónico del orden, pero no están preparadas para ofrecer una visión alternativa, ni dispuestas a asumir los costes que exigiría, incluido el del liderazgo de las iniciativas normativas. Les resulta más rentable la "estrategia del gandul" que les permite seguir obteniendo rédito del orden actual sin aumentar sus responsabilidades internacionales. Combinan su tradicional rol de receptores normativos, especialmente en el ámbito económico,[101] con su nuevo rol de creadores-moldeadores de normas sin cuestionar las reglas fundamentales del juego. No actúan como actores subversivos. En otros ámbitos,

98 TERHALLE, M., "Reciprocal Socialization: Rising Powers and the West", *International Studies Perspectives,* vol. 12, 2011, núm. 4, pp. 341-361, (341).

99 BURKE-WHITE, W. W., *op. cit.*, nota 95, p. 8.

100 Véase GARCÍA SEGURA, C., *op. cit.,* nota 20.

101 XIAOYU, P., *op. cit.,* nota 88, pp. 356 y 360-361, y ACHARYA, A., *op. cit.*, nota 13, p. 5.

su nueva posición de poder les permite devenir afianzadores activos y promotores y, entonces, pasan a defender activamente su posición contraria a opciones cosmopolitas. Contestan la premisa de que las normas occidentales universalistas son superiores y reivindican su participación en la atribución de legitimidad a las normas e instituciones del orden internacional.

Como consecuencia de los cambios en la estructura de poder, el sistema jurídico internacional, flexible y resiliente, también se transforma. Algunos procesos normativos migran hacia los subsistemas regionales, a menudo a expensas de las alternativas globales. Además, se dan diferentes interpretaciones de los principios, normas e instituciones como resultado del pluralismo. Y, finalmente, se refuerza *Westfalia* gracias a los Estados que, supuestamente, debían impulsar *Eastfalia* y gracias al comportamiento incoherente de los que, teóricamente, impulsaban *Worldfalia*. El resultado es que acaba imponiéndose una visión más estatocéntrica y tradicional del Derecho internacional que reafirma la soberanía, basa la legitimidad en los procesos e instituciones que se sustentan en la igualdad soberana y resitúa al Estado en el centro del proceso de desarrollo económico. Supone un retroceso en la individualización del Derecho internacional,[102] un regreso a la estatalización de las relaciones internacionales y un freno al avance de *Worldfalia* y de las normas de carácter cosmopolita. Pero en absoluto supone una amenaza real al orden internacional existente. Este ha demostrado ser altamente "pegajoso".[103] A la vez, los principios cosmopolitas blandos resisten el envite y coexisten en tensión con los soberanistas porque otros actores de la sociedad civil global los defienden. Por esto, no resulta contradictorio afirmar que la dirección y la dinámica de los procesos de creación y difusión de normas globales, y los de transformación y sustitución de las mismas, pueden ser interpretadas como un paso más en la estabilización de un orden internacional cada vez menos estatocéntrico (pluralidad de actores), quizás menos occidental (mayor peso de los países emergentes), pero no por ello menos sólido.[104] El análisis de algunos de los procesos de construcción de normas globales demuestra que estas ayudan a la consolidación y a la resiliencia de la dimensión pública del orden internacional, del Derecho internacional y de los elementos de cosmopolitismo blando del orden internacional. Este es el caso de la creación de normas en el ámbito de la ciberseguridad que analizaremos a continuación.

4. EL CIBERESPACIO Y LA CIBERSEGURIDAD

Una de las mayores transformaciones de las últimas décadas del siglo anterior fue, sin duda, la llamada revolución de las TIC cuyo inicio puede situarse en

---

102 BURKE-WHITE, W. W., *op. cit.*, nota 95, pp. 76 et ss.

103 IKENBERRY, J., *op. cit.,* nota 13.

104 GARCIA C., PAREJA, P. y RODRIGO, A., *op. cit.*, nota 67.

la década de los setenta. El término TIC empezó a ser utilizado por la comunidad académica en la década de los ochenta y se popularizó a finales de la de los noventa cuando el impacto de la revolución era ya muy evidente. La naturaleza revolucionaria de los Desarrollos científicos y tecnológicos que se llevaron a cabo en el ámbito de la información y la comunicación, especialmente en la microelectrónica y la optoelectrónica, se manifiesta en dos rasgos que comparten con anteriores revoluciones científicas y en un tercero que es singular: la aplicación de las innovaciones tecnológicas a distintos ámbitos de la actividad humana; el hecho de generar no solo nuevos productos sino nuevos procesos de producción; y finalmente, y es lo que le concede la singularidad, el hecho de que los desarrollos tecnológicos operan sobre la información, su procesamiento y su transmisión.[105] Las TIC son tecnologías sistémicas porque sus aplicaciones y sus efectos se expanden a todos los ámbitos de la economía, la política y la sociedad y alteran radicalmente la forma en que el tiempo y la distancia afecta a los procesos económicos, productivos, políticos, culturales, sociales y comunicacionales.[106] Las distancias y los espacios pasan a tener un significado distinto gracias al acercamiento virtual (ideas, informaciones, datos) que permiten las TIC. Su expansión creciente y sus múltiples aplicaciones a todos los ámbitos de la vida pública y privada ha creado enormes oportunidades, apenas unos años antes impensables, que permiten mejorar los procesos, los servicios y la calidad de vida de los ciudadanos que tienen acceso a ellas. Al mismo tiempo ha generado riesgos, también antes inimaginables que, por el hecho de ser tecnologías sistémicas, afectan a todos los ámbitos materiales y espaciales. El impacto –en términos de oportunidades y de riesgos– es desigual según las regiones, el acceso de los ciudadanos y gobiernos a las TIC y el control sobre las mismas por parte de actores públicos y privados. En las siguientes páginas analizaremos su impacto en el ámbito de la ciberseguridad. La ciberseguridad está vinculada a la emergencia de un nuevo espacio de contornos imprecisos, el ciberespacio, en el que, como vamos a ver, son necesarias normas globales.

4.1. La definición y caracterización del ciberespacio: ¿un espacio más o un Recurso Común Global?

El término ciberespacio, en su uso popular, se refiere al entorno virtual relacionado con la información y las interacciones entre las personas. También puede definirse como "la infraestructura digital de la información y las comunicaciones

105 CASTELLS, M., *La era de la información: Economía, sociedad y cultura (vol.1). La sociedad red*, Madrid, Alianza editorial, 1997.

106 MANSELL, R., "Information and Communications Technology Policy Research in the United Kindom: A perspective", *Canadian Journal of Communication,* vol. 19, 1994, num. 1, pp. 23-40.

conectada globalmente".[107] A veces se asocia erróneamente el ciberespacio a la infraestructura global de comunicaciones que es Internet. El ciberespacio es más que Internet e Internet es más que una infraestructura global de comunicaciones global.[108] El grupo internacional de expertos que, a instancias de la OTAN, elaboró el Manual de Tallín sobre el Derecho internacional aplicable a la ciberguerra (ver apartado 5.2.2. a) lo define como "el entorno formado por componentes físicos y no físicos, caracterizado por el uso de ordenadores y el espectro electromágnético para almacenar, modificar e intercambiar datos usando redes de ordenadores.[109] Una definición más precisa es la utilizada en la *Política de ciberseguridad* de Estados Unidos que describe el ciberespacio como "la red interdependiente de las infraestructuras de las tecnologías de la información que incluyen Internet, las redes de telecomunicaciones, los sistemas informáticos, los procesadores y controladores incrustados en las industrias críticas".[110]

El ciberespacio alcanza prácticamente a cualquier cosa y a cualquier persona y las actividades que en él se desarrollan pueden generar efectos positivos o negativos sobre personas, sociedades y gobiernos. En la vertiente positiva, el ciberespacio es una plataforma para la innovación y la prosperidad y provee de medios para mejorar el bienestar en cualquier lugar del planeta. En su vertiente negativa,puede generar grandes riesgos para los intereses, públicos y privados, de todos los que lo habitan.El peligro está vinculado, parcialmente, al hecho de que el ciberespacio es, aun hoy, un espacio poco regulado.[111]

---

107 THE WHITE HOUSE, *Ciberspace Policy Review. Assuring a Trusted and Resilient Information and Communication Infrastructure*, Washington, 29 de mayo de 2009. https://fas.org/irp/eprint/cyber-review.pdf, p. 1.

108 Internet es el sistema global de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP para transmitir datos a través de diferentes tipos de medios. La *World Wide Web* (www) e Internet no son lo mismo, a pesar de que se usen comúnmente como sinónimos. La www es un sistema de información que permite el intercambio de paquetes de datos mediante el protocolo http. Internet incluye el hardware y la infraestructura de comunicaciones así como muchos sistemas de información (Telnet, acceso remoto a ordenadores; FPP, sistema de transferencia de archivos, POP y STMP, sistemas de correo electrónicos, P2P, sistema de intercambio de archivos; o los chats o conversaciones on line) de los que la www es uno más. LEINER, B. et al., *Brief History of Internet,* Reston, Internet Society, 1999, https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf. KHAN, R.E. y CERF, V.G., "What is Internet (and What Makes it Work)", http://www.policyscience.net/cerf.pdf.

109 SCHMITT, M.N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge, Cambridge University Press, 2013, p. 211.

110 THE WHITE HOUSE, *National Security Presidential Directive/54*, Washington, 8 de enero de 2008, https://fas.org/irp/offdocs/nspd/nspd-54.pdf, p. 3.

111 THE WHITE HOUSE, *op. cit.,* nota 107, p. i.

Los desarrollos en el ámbito de las TIC y la importancia de las comunicaciones globales han hecho del ciberespacio un nuevo campo de acción de las relaciones internacionales. Diferentes actores lo utilizan para aumentar su cuota de poder o para amenazar a otros actores. Los ciberataques han dejado de ser ciencia ficción y son ya una realidad que plantea nuevas problemáticas de seguridad para los Estados, las empresas y los individuos. Garantizar la ciberseguridad se ha convertido en una necesidad acuciante y, con ella, la creación de cibernormas para regular el ciberespacio desde el que se genera la "ciberinseguridad". Ello exige un consenso previo sobre qué tipo de espacio es el ciberespacio. Los Estados ya hablan del ciberespacio como un quinto y nuevo espacio territorial, incluso como "el quinto campo de batalla".[112] Estados Unidos lo considera "un campo operativo" en el que, al igual que en la tierra, el mar o el aire, la defensa americana debe poder prevenir o rechazar una agresión. Una concepción muy similar es la de Francia para quien el ciberespacio es un nuevo campo de acción en el cual ya tienen lugar operaciones militares y en el que el Estado francés debe desarrollar sus capacidades. También Rusia comparte esta visión y reclama el derecho legítimo de los Estados a recurrir a la fuerza en caso de una utilización hostil de las tecnologías de la información y la comunicación.[113] Pero, al margen de la reivindicación del derecho de defensa ante un ciberataque, no existe acuerdo ni doctrinal ni político, sobre la naturaleza del ciberespacio. Algunos autores destacan su singularidad y defienden que el ciberespacio es un espacio diferente porque es el único que es completamente fruto de la acción humana: es creado, mantenido, gestionado colectivamente por diversos actores públicos y privados.[114] Otros le restan singularidad y señalan que sus tres rasgos definitorios son comunes a otros ámbitos. Así el ciberespacio es un espacio caracterizado por la rapidez de los cambios tecnológicos, pero esa rapidez se manifiesta igualmente, por ejemplo, en el ámbito de la salud global (extensión de las pandemiase); por la escala geográfica y humana que alcanzan estos cambios, rasgo también propio del ámbito medioambiental (cambio climático); y por el secretismo, igualmente muy extendido en el ámbito de la seguridad.[115]

El debate planteado actualmente gira en torno a dos opciones: la primera es que el ciberespacio sea considerado una arena sobre la cual los Estados puedan ejercer la soberanía; la segunda es que se trate el ciberespacio como un recurso

---

112 "Ciberespace, 5ème champ de bataille" era el título de un dossier de la revista francesa *Armées d'aujourd'hui,* núm 365 de 2011, (disponible en https://es.calameo.com/read/0003316270ac92b146c2d)

113 SIMONET, L., "L'usage de la force dans le cyberespace et le Droit international", *Annuaire Français de Droit International*, LVIII, 2012, pp. 117-143, p.118.

114 MELZER, N., "Ciberwarfare and International Law", *UNIDIR Resources,* Washington, CSIC/UNIDIR, 2011, p. 5.

115 FINNEMORE, M. y HOLLIS, D., *op. cit*., nota 63, pp. 456-458.

común (*commons*) de información sobre el que ningún Estado pueda reclamar la jurisdicción –como ocurre con los fondos marinos, el océano Antártico o el espacio ultraterrestre. En este caso, no se podría regular a no ser que se llegara a una posición de compromiso y se aplicara el principio de Patrimonio Común de la Humanidad. Puede parecer una opción tentadora pero en realidad presenta serias dificultades de aplicación ya que a diferencia de los demás*global commons,* el ciberespacio no es un recurso físico.[116] La primera concepción del ciberespacio se identifica con el resurgir de *Westfalia* –los Estados reclaman el control soberano de las infraestructuras del ciberespacio– y con una aproximación geopolítica –el ciberespacio es un "territorio" más desde el que el Estado puede proyectar su poder. La segunda se alinea con el cosmopolitismo blando y el tímido e inestable avance de *Worldfalia* y conllevaría la creación de mecanismos multilaterales de gobernanza global para gestionar el ciberespacio como recurso común global. El debate en torno a la naturaleza del ciberespacio es un escenario más en el que se pone de manifiesto la tensión cosmopolita. Como veremos más adelante, a pesar del sustrato cosmopolita que inspira todas las reflexiones sobre la necesidad de regular el ciberespacio, *Westfalia* se ha impuesto a *Wordfalia*. Desde 2013, el "Grupo de Expertos Gubernamentales (GEG) de Naciones Unidas sobre los Desarrollos en el Ámbito de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional" definió el ciberespacio como un espacio en el que aplica el principio de soberanía estatal (ver apartado 5.2.1). Se abandonó la "ilusión"–creada por la facilidad y rapidez de la conectividad que permitía Internet– del ciberespacio como un espacio sin fronteras y se aceptó que Internet y el ciberespacio tienen"fronteras" y dependen de la infraestructura física que está sujeta al control soberano de los Estados.[117]

4.2. La complejidad de la ciberseguridad

La ciberinseguridad es una realidad muy diversa y compleja que se empezó asociando a los hackers adolescentes que penetraban los sistemas de seguridad de gobiernos y empresas como divertimento informático para demostrar sus habilitades y que se ha ido ampliando progresivamente a actividades muy variadas que realizan una gran diversidad de actores (Estados, "hackeractivistas" –hackers con un objetivo político, ciberterroristas, y cibercriminales). Sus objetivos son igualmente muy variados: defender una causa política, atacar a un rival político o económico, obtener beneficios económicos, obtener información industrial

---

116 SHACKELFORD, S.J., "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law,* vol. 27, 2009, núm. 1, pp. 193-251 (211 et ss).

117 LEWIS, J. (con el apoyo de VIGNARD, K.), *Report of the International Security Cyber Issues,* UNIDIR/CSIS, Ginebra/Whasington, Workshop Series, 2016, pp. 6 y 9.

secreta, política o de seguridad. etc. Sus víctimas son igualmente muy diversas (Estados, empresas, organizaciones o individuos). La preocupación por la ciberseguridad se ha disparado a medida que ha aumentado el número de ciberataques[118] y que los actores han tomado consciencia de su vulnerabilidad.[119] Los ciberataques provocan unas pérdidas económicas globales de 600 mil millones de dólares anuales.[120] Se calcula que esta cifra en 2021 alcanzará los 6 trillones de dólares.[121] Uno de los ciberataques que mayores pérdidas ha ocasionado fue el que sufrió la compañía petrolera nacional saudí Aramco en 2012. El ataque fue reivindicado por el grupo *Cutting Sword of Justice,* aunque la mayoría de analistas lo atribuyen a Irán, que lo habría realizado en respuesta al que había sufrido en 2010.[122] A través del virus Shamoon fueron afectados 35.000 ordenadores, las tres cuartas partes del total de los de la empresa. A la par que inhabilitó los sistemas de gestión y pagos de la misma, el ciberataque provocó la subida de precios de los discos duros ante la demanda masiva generada por Aramco que necesitó sustituir con urgencia todos los discos afectados.[123]

Pero las pérdidas económicas son solo un efecto de los ciberataques. Los ciberataques pueden ponen en jaque la seguridad nacional, desprestigiar la credibilidad o la reputación de un gobierno o de una empresa, o causar daños físicos, si

---

118 Véase el registro realizado por el Centre for Strategic and International Studies (CSIS) de Washington desde 2006 (https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity). Aunque en este registro solo se computan los "Significant Cyber Events", aquellos que provocan pérdidas por valor de más de un millón de dólares, sirve para dar una idea de la progresión de los ciberataques (de 5 registrados en 2006 a 104 en 2018).

119 LÉTÉ, B. Y CHASE, P., "Shaping Responsible State Behaviour in Cyberspace", *Workshop Briefing Paper,* Washington, German Mashall Fund of the United States, 2018, p. 4.

120 LEWIS, J., *Economic Impact of Cibercrime –No Slowing Down,* Washington /Santa Clara, CSIS/McAfee, 2018, p. 6, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf. El autor cita estimaciones del CSIS y reconoce que es muy difícil calcular el coste del cibercrimen debido a la ausencia de datos suficientes y a la existencia de diferentes modelos de medición. Además, muchos de los cibercrímenes no son denunciados (el mismo informe recoge que en el Reino Unido se estima que solo se reportan el 13%, p. 8).

121 POGGI, N., "24 estadísticas de seguridad informática que importan en el 2019", 3 de diciembre de 2018, BlogPreyNation,https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

122 En 2010, un gusano informático, Stuxnet, infectó mil máquinas enriquecedoras de uranio de la central nuclear iraní de Natanz. Más de 60.000 ordenadores se autrodestruyeron. Nadie se atribuyó la autoría. Israel y Estados Unidos, países altamente interesados en frenar la capacidad nuclear iraní, parecían los máximos sospechosos, aunque no se ha podido comprobar su participación en el ciberataque. https://www.theguardian.com/technology/2010/nov/16/stuxnet-worm-iran-nuclear

123 https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

afectan a infraestructuras críticas de las que dependen el bienestar o la seguridad de los ciudadanos. Un caso emblemático de ciberataque que consiguió colapsar un país, fue el sufrido por Estonia en 2007. Un ataque de denegación de servicio(-DoS) –envío masivo de spam a través de redes de ordenadores– afectó y bloqueó simultáneamente las redes informáticas del parlamento, ministerios, bancos, empresas, periódicos y otros medios de comunicación estonios, provocando el colapso total de los servicios de estas instituciones. La autoría, aunque atribuida a Rusia, no pudo ser probada.[124]

A mayor uso de Internet, mayor vulnerabilidad de aquellos actores (Estados, empresas, organizaciones de la sociedad civil, individuos, etc) y sectores (seguridad, salud, finanzas, administraciones públicas, etc.) que dependen de la conectividad para realizar sus funciones y garantizar los servicios que de ellos dependen.[125] Se da la paradoja de que cuanto más ciberconectado está un Estado, lo que puede ser considerado como un signo de su desarrollo y capacidad tecnológica, más dependiente es de las TIC y, por ende, más vulnerable a los ciberataques. Por ello, la mayoría de potencias consideran hoy día los ciberataques como una de las amenazas más importantes a las que se enfrentan.[126] En 2010 el Reino Unido pasó a considerarlos una de las cuatro amenazas de nivel 1 (junto al terrorismo internacional, las crisis militares entre Estados y las catástrofes naturales) y la Estrategia Nacional de Seguridad estadounidense, del mismo año, los calificaba como uno de los más serios retos a la seguridad nacional.[127] A la vez, los Estados son los actores que tienen mayores capacidades financieras y técnicas para causar daños en el ciberespacio, lo que no excluye que otros actores (hackeractivistas, ciberdelincuentes, ciberterroristas) puedan causarlos. Las Naciones Unidas asumieron la preocupación por la ciberseguridad como propia en 1998. A través de una serie de resoluciones, la Asamblea General de Naciones Unidas ha ido reconociendo que la expansión del uso de las TICs afecta a los intereses

---

124 Estonia y Rusia tenían un conflicto abierto a raíz del desplazamiento del monumento a los soldados rusos caídos en la lucha contra el nazismo, que muchos estonios consideran un monumento a los ocupantes del país. Véase: https://www.bbc.com/mundo/noticias-39800133

125 El número actual de usuarios de internet se cifra en 3,9 mil millones, equivalente a la mitad de la población mundial. Se estima que en 2023, el 70% estará conectado. *Global CybersecurityIndex (GSI) 2018,* ITU, Ginebra, 2019,https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

126 Un estudio del CSIS, publicado en 2011, señalaba que 33 Estados incluían la ciberguerra en su planificación y organización militar, mientras que otros 36 seguían delegando la ciberseguridad (misiones internas, seguridad de los ordenadores, vigilancia del cumplimiento de la ley) a agencias civiles. LEWIS, J.A. y TIMLIN, K., "Cybersecurity and Cyberwarfare", *UNIDIR Resources,* Washington, CSIC/UNIDIR, 2011, p. 3.

127 SCHMITT, M.N., *op. cit*., nota 109, p. 16.

de la comunidad internacional y que el uso criminal de las mismas puede tener un impacto negativo en todos los Estados si se utilizan de manera contraria a los objetivos internacionales del mantenimiento de la paz y seguridad.[128]

Al hablar de ciberseguridad se usan, de manera no siempre muy precisa conceptos vinculados: algunos de ellos son conceptos genéricos que incluyen a otros más precisos. Así, las *ciberoperaciones* son operaciones en las que se utilizan las capacidades del ciberespacio para alcanzar objetivos determinados.[129] Las *ciberamenazas* son amenazas que contemplan el uso del ciberespacio y de medios e instrumentos electrónicos. Los *ciberataques* son actos de hostilidad realizados en el ciberespacio, por parte de un Estado, o de agentes o entidades cuyas acciones pueden ser atribuidas a los Estados, que comportan medidas informáticas coercitivas destinadas a perturbar seriamente o a dañar las estructuras esenciales de otro Estado, sean estas militares, financieras, sanitarias o sociales.[130] Cuando los ciberataques los llevan a cabo individuos o entidades privadas se suele hablar de ciberdelitos y cibercrímenes. En este caso la diferencia entre ambos la marca la gravedad del delito. Mientras que los *ciberdelitos* son trangresiones leves de la ley realizadas a través del ciberespacio, los *cibercrímenes* son delitos graves contra la confidencialidad, integridad y accesibilidad de datos y sistemas informáticos cometidos por individuos o entidades privadas para su beneficio personal.[131] El *ciberespionaje* es un delito específico de obtención encubierta de datos o de información confidencial, realizado a través de medios informáticos. Finalmente, el concepto más controvertido es el de *ciberguerra* por las implicaciones del mismo respecto al derecho a la legítima defensa y al uso de la fuerza (ver apartado 5). Aunque el término goza de amplia difusión mediática, los juristas prefieren hablar de ciberconflicto armado. Se habla de ciberguerra para calificar las hostilidades llevadas a cabo en conflictos armados a través del uso de las cibertecnologías.[132] Lo distintivo de la ciberguerra es el uso de las TIC como método o instrumento de guerra. Así, una infección del sistema de ordenadores de un adversario beligerante con un virus malicioso sería considerada un acto de ciberguerra mientras que un bombardeo aéreo de un cibercomando militar no lo sería. Del mismo modo, se incluirían ataques a personas cuya vida, o a objetos cuya funcionalidad, depende de sistemas de ordenadores (tales como ataques a centrales eléctricas, a medios de transportes o a personas dependientes de sistemas electrónicos de asistencia

---

128 ROSCINI, M., *Cyber Operations and the Use of Force in International Law,* Oxford, Oxford UniversityPress, 2014, p. 2.

129 Marco Roscini toma prestado el concepto del *Dictionary of Military and Associated Terms*del Departamento de Defensa de Estados Unidos. *Ibíd.,* p. 11.

130 SIMONET, L., *op. cit.,* nota 113, p. 122

131 ROSCINI, M., *op. cit.,* nota 128, p.4.

132 *Ibíd.* Y SCHMITT, M. y VIHUL, L., "The Nature of International Law Cyber Norms" en OSULA, A-M. y RÕIGAS, H. *op. cit.*, nota 61, pp. 23-47, p. 27.

médica o de respiración artificial).[133] Existe consenso en torno a la idea de que para que los ciberataques sean considerados como ciberguerra y, por tanto, equivalentes al uso de la fuerza, deben causar destrucción física, heridos o víctimas mortales. En la actualidad, estos representan un porcentaje muy bajo del total. Los datos apuntan a que de entre los miles de ciberincidentes, principalmente de ciberespionaje y cibercrimen que afectan mayoritariamente a empresas e instituciones financieras, solo una docena serían incidentes en los que los Estados han utilizado el ciberespacio para presionar políticamente a otros Estados y tan solo tres o cuatro podrían ser considerados equivalentes al uso de la fuerza.[134]

Ante la ciberinseguridad provocada por las ciberamenazas y ciberataques de todo tipo, la ciberseguridad puede definirse como la capacidad y la habilidad de proteger (o las actividades o procesos que consiguen proteger) los sistemas de información y comunicación y la información que contienen o defenderlos contra daños, uso, modificaciones o explotación no autorizados. Esta definición implica la existencia de un adversario, de una amenaza intencionada (excluye los daños provocados de forma no intencionada: errores de ordenadores o problemas de interoperatividad) y no entra en los contenidos de las TIC (contenidos políticamente subversivos, pornografía infantil, etc.).[135] Los efectos son múltiples y diferentes según los actores a los que afecta. Los ciberataques pueden provocar la pérdida de confidencialidad y de integridad: acceso a datos privados, manipulación y destrucción de datos, etc; afectar a la disponibilidad de los sistemas: páralisis por colapso, sobrecarga por envío masivo de spam (DoS), apagones digitales, etc; y una gran variedad de efectos indirectos: un país que ve colapsado su sistema bancario o penetrado su sistema de Seguridad, además de sufrir grandes pérdidas económicas, ve cuestionada su imagen y reputación, interna e internacionalmente. Los daños económicos directos se transforman en daños políticos indirectos.

5. LA REGULACIÓN GLOBAL DE LA CIBERSEGURIDAD.

La preocupación por la ciberinseguridad y la toma de conciencia sobre la importancia de la ciberseguridad ha llevado a la articulación de procesos normativos de carácter diverso para controlar las ciberamenazas. Aunque es corriente que los hackers, las organizaciones terroristas y los grupos del crimen organizado sean los actores con los que el imaginario social asocia las ciberamenazas, en realidad

133 MELZER, N., *op. cit.*, nota 114, pp. 4-5.

134 *Ibíd.*

135 FINNEMORE, M. Y HOLLIS, D., *op. cit*, nota 63, p. 431 y NICCS, "Explore Terms: A Glosary of Common Cybersecurity Terminology", https://niccs.us-cert.gov/about-niccs/glossary#C.

son los Estados quienes tienen más recursos, mayores capacidades financieras y técnicas, para causar daños desde el ciberespacio y a quienes se atribuye la autoría (no demostrada) de la mayor parte de los ciberataques. No es extraño que sean ellos también, conscientes de sus capacidades y de sus vulnerabilidades, los que protagonizan la mayor parte de iniciativas normativas para intentar reducir la ciberinseguridad. En paralelo se desarrollan, cada vez más, iniciativas que lideran actores no estatales e iniciativas de participación múltiple. Antes de entrar el contenido de las principales iniciativas normativas, nos referiremos a la caracterización general de la regulación del ciberespacio y de las cibernormas.

5.1. Características y dificultades de la regulación en materia de ciberseguridad: las cibernormas

La regulación en materia de ciberseguridad es relativamente reciente ya que también lo es la toma de conciencia sobre la problemática de la ciberinseguridad. A pesar de ello, desde la disciplina de las Relaciones Internacionales, la producción de normas en el ciberespacio ha sido estudiada por la Teoría normativa y el Constructivismo y ya ha producido un corpus de conocimiento sobre la naturaleza de las cibernormas que ofrece una concepción matizada de las mismas y un relato sobre cómo deben ser interpretadas en un contexto tan desafiante como el ciberespacio. Estos estudios sugieren que no basta prestar atención a los principios o códigos de conducta que se proponen como normas sino que hay que analizar los sistemas de valores que los informan y en los que están incrustados puesto que las cibernormas son el resultado de la negociación y la contestación en un contexto de prácticas cambiantes, de sistemas de valores en conflicto y de intereses públicos y privados en contraposición.[136]

La naturaleza compleja del ciberespacio exigiría una regulación que arrancara de un análisis multidisciplinar de las problemáticas y de las oportunidades que en él y desde él se generan. Para regular eficazmente el ciberespacio habría que establecer el nexo entre tecnología, derecho, psicología, sociología, economía, ciencia política y diplomacia. Sin embargo, esto implica una amplitud de miras de la que a menudo carecen los actores, aferrados a sus intereses y planteamientos particulares y corporativos. La regulación en este ámbito comparte características con los procesos normativos en otros ámbitos a la vez que tiene algunas específicas, vinculadas a la naturaleza singular del ciberespacio.

En primer lugar, la regulación en materia de ciberseguridad se enfrenta a la *existencia de una gran variedad de intereses, identidades y culturas de los diferentes grupos de actores*, que se traducen en enfoques normativos distintos y a veces

136 ERSKINE, T. y CARR, M., *op. cit.*, nota 61, pp. 108-109.

contrapuestos que dificultan la regulación. Sin embargo, en perspectiva histórica, esta circunstancia no es particularmente extraordinaria ya que es habitual que los Estados inviertan mucho tiempo y esfuerzos en regular los desafíos planteados por las nuevas tecnologías y los nuevos medios de coerción.[137] Las culturas e intereses juegan un papel clave en la conformación de los elementos constitutivos de las cibernormas mientras que el derecho apenas interviene. Las cibernormas con las que se identifican los miembros de una comunidad o grupo que comparte una identidad son diferentes a las resultantes de otra cultura ya que no comparten los mismos criterios de corrección y por tanto no prohíben o permiten las mismas conductas. Por ejemplo, los Estados entienden el ciberespacio como un espacio territorial más y se interesan por controlarlo a fin de combatir las amenazas que pueden llegar a través de él. Las empresas del sector lo conciben como un espacio de libertad y su mayor preocupación es proteger la privacidad de los usuarios, básica para seguir manteniendo su confianza, por ende su prestigio y, sobre todo, su negocio. Los actores de la sociedad civil (onegés, activistas, comunidad académica y técnica) estiman que la ciberseguridad debe abordarse en clave de defensa y protección de derechos y libertades (libertad de expresión, acceso a la información y al conocimiento, protección de datos, derecho al desarrollo). Un ejemplo claro es la contraposición entre la llamada "cultura de Silicon Valley" (de las empresas TIC) y la cultura de los Estados y de los servicios de seguridad nacional a propósito de las llamadas puertas traseras –mecanismos ocultos de acceso a los productos de software y hardware que debilitan la encriptación. La primera defiende el principio de integridad tecnológica, que propone medidas de protección de la privacidad y rechaza mecanismos de funcionalidades ocultas, y la libertad en el ciberespacio. La segunda propone cibernormas que antepongan la seguridad a la privacidad. En consecuencia, mientras que las empresas de software se niegan a crear puertas traseras, a fin de proteger la privacidad de sus usuarios, los gobiernos presionan para que las creen a fin de perseguir los cibercrímenes o el ciberterrorismo.[138]

---

137 HENRIKSEN, A., "The end of the road for the UN GGE process: The future regulation of cyberspace", *Journal of Cybersecurity*, 2019, nº 1, pp. 1-9 (p.2).

138 Un caso de enfrentamiento resultado estas culturas diferentes lo protagonizaron el FBI y la empresa Apple a propósito del requerimiento del FBI de desbloquear el sistema de encriptación del iPhone de uno de los autores de la Matanza de San Bernardino, California, en 2015. Una orden judicial de California requirió a la empresa que le facilitara la puerta trasera. La empresa se negó a hacerlo. Su postura recibió el apoyo público de otras compañías como Google, WhastApp y Twitter. Finalmente el FBI consiguió desbloquear el teléfono acudiendo a los servicios de una tercera compañía (se especula que la israelí Cellebrite), por los que se dice que pago 900.000$. Apple basaba su negativa en otra resolución de un juzgado de Nueva York a su favor que le permitió no entregar al FBI el código de acceso a un iPhone vinculado con un caso de narcotráfico. https://www.bbc.

Por otra parte, los grupos de actores tampoco son monolíticos: los Estados mantienen enfoques diferentes respecto a la regulación de la ciberseguridad que derivan de su concepción de la problemática en este ámbito. Rusia y China, potencias no occidentales, enfocan la seguridad en el ciberespacio como un problema de seguridad de la información mientras que las potencias occidentales, especialmente representadas por Estados Unidos y el Reino Unido, pero incluyendo también a los Estados de la UE y Japón, lo enfocan como un problema de ciberseguridad (cibercímenes y ciberdelitos). Para Rusia y China y sus aliados de la Organización para la Cooperación de Shanghai el peligro deriva de la difusión masiva de información nociva destinada a minar el sistema económico y social de otros Estados y a manipular masivamente a la sociedad de cara a desestabilizarla y, con ello, desestabilitzar también al Estado.[139] Ven las TIC como amenazas potenciales cuyo mal uso puede invalidar los principios de igualdad y respeto mutuo y facilitar la intervención en los asuntos internos de otros países.[140] En concreto, temen la interferencia extranjera en sus redes domésticas para promover la disidencia política. Por ello mismo reclaman la soberanía sobre el ciberespacio, defienden el derecho de cada país a gestionar el ciberespacio de acuerdo con su legislación nacional y la idea de que la libre circulación de información debe garantizarse al tiempo que se protegen la soberanía y la seguridad nacional y se respetan las diferencias políticas y culturales entre países. Quizás los temores rusos deriven de su buen conocimiento de las posibilidades disruptivas de la desinformación a través de las redes ya que sobre el Departamento Central de Inteligencia ruso pesan sospechas y acusaciones de intervenir en diferentes procesos políticos europeos (Brexit, independentismo catalán) con el fin de desestabilizar al Reino Unido y a España y, por extensión, a Europa.[141]

---

com/mundo/noticias/2016/03/160329_tecnologia_fbi_como_desbloqueo_iphone_san_bernardino_apple_ch

139 ROBERTS, A., *Is International Law International?*, Nueva York, Oxford University Press, p.306. En el *Acuerdo entre los Gobiernos de los Estados miembros de la OCS sobre cooperación en materia de garantía de información internacional* de 2009 (anexo 2) se describen cinco categorías de amenazas, todas ellas relacionadas con la ciberseguridad informativa: el desarrollo y uso de armas informativas y la guerra informativa; el terrorismo informativo; el crimen informativo; el uso de una posición de dominio en el espacio informativo para dañar la seguridad de otros países; la difusión de información que impacte negativamente en los sistemas político, socio-económicos y en los entornos espirituales, culturales y morales de otros países. cis-legislation.com/document.fwx?rgn=28340

140 *Declaration of the Heads of Members States of the Shanghai Cooperation Organization on International Information Security*. 2006. https://chinacopyrightandmedia.wordpress.com/2006/06/15/declaration-by-the-heads-of-state-of-the-shanghai-cooperation-organization-member-states-concerning-international-information-security/

141 LIS, J., "Was there Russian meddling in the Brexit referèndum? The Tories just didn't care", https://www.theguardian.com/commentisfree/2020/jul/21/russian-meddling-brexit-re-

En segundo lugar, el riesgo de obsolescencia jurídica es mayor que en otros ámbitos debido a la velocidad y el impacto de los cambios tecnológicos,[142] por ello en los procesos de regulación *se opta por las negociaciones políticas, más ágiles y flexibles, y por las normas no vinculantes frente a las negociaciones jurídicas conducentes a los tratados, más lentas y rígidas*. En el ciberespacio la lentitud de los procesos legislativos y reguladores tiene mayor repercusión que en otros ámbitos en los que las transformaciones se desarrollan a ritmos más pausados. Este es uno de los motivos que contribuyen a que se adopte el enfoque no formal del *soft law*, con instrumentos que no requieren ratificación y con negociaciones más breves. Así, hasta el momento el instrumento mayoritariamente preferido por los actores, tanto Estados como empresas, para avanzar en la regulación de la ciberseguridad han sido las normas, tal como han sido definidas en este trabajo, mientras que el Derecho internacional, como instrumento regulador del ciberespacio, ha sido relegado a un segundo plano y la idea de crear un nuevo régimen internacional específico para el cibespacio o un tratado internacional general sobre la materia ha sido prácticamente abandonada.[143] Toni Erskine y Madeleine Carr han acuñado el término de "casi normas" para referirse a las cibernormas que generan principios y códigos de conducta que no tienen la fuerza prescriptiva, la aceptación y la internalización de las normas.[144] Martha Finnemore afirma que el entusiasmo actual por las normas como instrumento de las políticas del ciberespacio proviene de las extendidas dudas sobre la eficacia de los tratados formales en este campo.[145] También influye, en nuestra opinión, el hecho de que las cibernormas son un instrumento menos intrusivo en la soberanía estatal que el Derecho internacional. Los Estados, principales creadores normativos, justifican su opción apelando a la mayor flexibilidad y agilidad de las normas pero en realidad están optando por ellas para mantener un mayor margen de maniobra en el ciberespacio y no renunciar, de manera vinculante, a determinados instrumentos y conductas. De todos modos, normas y derecho no son opciones excluyentes ni

---

ferendum-tories-russia-report-government; ALANDETE, D., "How the Russian meddling Machine won the online battle of the illegal referèndum", https://english.elpais.com/elpais/2017/11/12/inenglish/1510478803_472085.html

142 KURBALIJA, J., *La gobernanza de Internet,*Ginebra, DiploFondation, 2017, pp. 135 et ss.

143 FINNEMORE y HOLLIS, *op. cit.,* nota 63, p. 436.

144 Hay dos vías por las que los actores presentan las "casi normas" como normas: las aspiraciones normativas (los actores desean crear e imponer normas en el ciberespacio y presentan como tales a principios y códigos de conducta) y la importación de reglas y principios (los actores importan reglas y principios de otros ámbitos al ciberespacio). Un principio es reconocido como norma cuando los actores se sienten impelidos a justificar o a negar su violación. ERSKINE, T. y CARR, M., *op. cit.*, nota 61, p.100 y 105.

145 FINNEMORE, M., "Cybersecurity and the concept of Noms", Carnegie Endowment for International Peace, pp. 1-6, noviembre 2017, Disponibleenhttps://carnegieendowment.org/files/Finnemore_web_final.pdf

incompatibles, al contrario son realidades interrelacionadas: las leyes y tratados pueden servir de base a la formulación de normas y estas pueden ser codificadas jurídicamente o cristalizar como Derecho consuetudinario.[146] Las cibernormas se enfrentan a las "conductas de conformidad hipócrita", es decir al hecho de que los actores las aceptan discursivamente pero no las aplican en la práctica.[147] Tal es la conducta de las autoridades chinas que se han comprometido a renunciar al ciberespionaje para obtener ventajas comerciales pero siguen utilizándolo. A pesar de ello, la adhesión formal a una cibernorma no debe menospreciarse ya que puede convertirse en un instrumento a favor de quienes presionan en pro del cambio de conducta y en un factor socializador. Las cibernormas también son, a menudo, siguiendo la terminología de Cars Sunstein adaptada al ciberespacio por Marta Finnemore y Duncan Hollis, "normas teorizadas de forma incompleta", es decir, normas que crean una expectativa de conducta determinada sin que los miembros del grupo que las aceptan compartan los motivos de corrección de dicha conducta. Así, la aceptación por diferentes actores del compromiso a revelar las vulnerabilidades de los programas cuando se descubren, para evitar que sean utilizadas con objetivos ilícitos, puede obedecer a motivos muy dispares: motivos económicos, búsqueda de prestigio, sentimiento de responsabilidad social, proteger la seguridad nacional o protección de la privacidad.[148]

También en este campo se visualizan las diferencias entre las preferencias de las potencias occidentales y las no occidentales. China y Rusia, y sus socios de la Organización para la Cooperación de Shanghái, apuestan por la regulación a través de un tratado internacional que regule las "armas de información" mientras que Estados Unidos y sus aliados se oponen a él. Los países occidentales temen que un tal tratado pudiera ser utilizado por Rusia y China para limitar los flujos de información, incrementar el control sobre Internet en sus territorios y frenar la inestabilidad política y las protestas civiles.[149] Por lo tanto, queda en evidencia que lo que está en juego no es tanto el tipo de instrumento normativo como el contenido.

A pesar de ser partidarios de la regulación jurídica, China y Rusia no se han unido al Convenio de Budapest sobre ciberdelincuencia impulsado por Estados Unidos y el Reino Unido.[150] El motivo es que no regula lo que a ellos les interesaría regular y que estiman que atenta contra la soberanía digital que tanto defien-

---

146 FINNEMORE, M. y HOLLIS, D., *op. cit.,* nota 63, p. 442 y SCHMITT, M. y VIHUL, L., *op. cit.*, nota 132, p. 47.

147 FINNEMORE, M. y HOLLIS, D., *op. cit.,* nota 63, p. 443-444.

148 STEIN, C., "Incompletely Theorized Agreements in Constitutional Law", *Social Research,* vol. 74, núm. 1, pp. 1-24.

149 ROBERTS, A. *op. cit*. 139, p. 307.

150 El Convenio sobre la Ciberdelincuencia, liderado por el Consejo de Europa, firmado en 2001 y en vigor desde 2004, es el primer tratado internacional sobre la materia. https://

den.[151] Esta última razón también se podría aplicar para explicar la reticencia de la mayoría de Estados a la creación de un nuevo tratado internacional general sobre telecomunicaciones para regular el ciberespacio.

En tercer lugar, *la mayor parte de la regulación en materia de ciberseguridad proviene de los Estados[152] o de organizaciones intergubernamentales[153] y es deudora del el enfoque westfaliano por ellos preferido*. La ciberseguridad, al igual que la seguridad global, pero aún con más motivo por la singularidad del ciberespacio, bien podría ser considerada un Bien Público Global desde una perspectiva multilateralista, cosmopolita y *worldfaliana*. No obstante, los Estados se resisten a ello y prefieren considerarla como una cuestión más de seguridad nacional lo que conlleva la reticencia a compartir información, estrategias y recursos. Esto queda plasmado en el rápido desarrollo de las estrategias nacionales de ciberseguridad de muchos países[154], de las estrategias regionales, en el marco de las organizaciones intergubernamentales,[155] e incluso de los tratados bilaterales, lo que contrasta con el lento avance de las iniciativas multilaterales globales. A pesar de la

---

rm.coe.int/16802fa41c Véase punto 5.2.2. b). Rusia, miembro del Consejo de Europa, no lo ha firmado.

151 SCHREIBER, C., "El futuro de China y Rusia como aliados en el ciberespacio", *Análisis GESI,* 2/2019. Disponible en http://www.seguridadinternacional.es/?q=es/content/el-futuro-de-china-y-rusia-como-aliados-en-el-ciberespacio.

152 *Ibíd*.

153 Las organizaciones regionales han elaborado diferentes instrumentos normativos –estrategias, directivas, convenciones, códigos de conducta–, la mayoría de ellos no vinculantes: *African Union Convention onCybersecurity and Personal Data Proteccion*, 2014; *ARF Statemen on Cooperation in Ensuring Cyber Security*, 2012; *APEC Strategy to Ensure Secure and Sustenaible On Line Environment; Convention on Cybercrime*; *Directive on Fighting Cyber Crime Within ECOWAS*; *Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace*, 2013; *Estrategia integral para combatir las amenazas a la seguridad cibernética* de la OEA, 2014; *Medidas de la OSCE para el fomento de la confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de tecnologías de la información y la comunicación*, 2012; *International Code of Conduct for International Security*, elaborado por la Organización de Cooperación de Shanghái, presentado a la Asamblea General de Naciones Unidas, 2011, actualizado en 2015.

154 Aunque el desarrollo es muy desigual según las regiones, la tendencia es a la alza. Según datos de la Unión Internacional de Telecomunicaciones, en 2018 el 58% de los Estados (de un universo de 134) tenían una estrategia de ciberseguridad y el 42% no (se había producido un incremento del 8% respecto al año anterior). La región que menos tenía era África y la que más, Europa. ITU, *op. cit,,* nota 125, p. 9.

155 ASEAN: https://asean.org/wp-content/uploads/2012/05/14-TELMIN-17-JMS_adopted.pdf; OEA: http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf; Unión Europea: https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en; Unión Africana: https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf.

naturaleza trasnacional y plural del ciberespacio y la ciberseguridad, los mayores avances regulatorios se generan en el espacio nacional y gubernamental.

En cuarto lugar, aunque los Estados han evitado generar nuevos tratados multilaterales sobre la materia, *se ha ido admitiendo progresivamente que el ciberespacio no es un espacio ajurídico sino que el Derecho internacional existente es aplicable* (véase apartado 5.2). La principal consecuencia de este hecho, victoria de los Estados occidentales potentes en TIC, es que la soberanía estatal, y por tanto la responsabilidad internacional, se aplica a las ciberhostilidadades.[156] Este grupo de Estados temía que un nuevo convenio internacional limitara sus capacidades y pudiera ser utilizado por China y Rusia para controlar la libertad de expresión y el acceso a la información de países terceros. Como hemos mencionado, estos dos países reclamaban insistentemente un tratado internacional, instrumento propio y exclusivo de Estados soberanos, para regular los delitos de información al tiempo que desarrollaban normativas internas muy restrictivas del uso de Internet a fin de controlar a su población, apelando a la soberanía digital y a la no injerencia en asuntos internos.[157] Aunque algunos autores afirman que un acuerdo global sería la mejor solución para regular la ciberseguridad, ya que sería específico y por ende más claro, los Estados se mueven entre la ambigüedad, o la hipocresía, de buscar soluciones a la ciberinseguridad y, a la vez, mantener intactas e ilimitadas sus cibercapacidades. Sus planteamientos no son monolíticos ya que tienen que ver con la posesión o no de cibercapacidades ofensivas. Aquellos Estados que ni las poseen ni tienen perspectivas de desarrollarlas son partidarios de una regulación global, mientras que quienes las poseen apelan a un comportamiento responsable, pero evitan cualquier regulación vinculante que las limite. Por otra parte, el acuerdo necesario para crear un nuevo tratado sería difícil de alcanzar

---

156 Las compañías de TIC querían evitar la responsabilidad internacional por las vulnerabilidades de sus sistemas. LÉTÉ, B. y CHASSE, P., *op. cit.,* nota 119.

157 En febrero de 2019, la Duma aprobó el *Proyecto de ley de soberanía digital* que, siguiendo el camino trazado por China, proponía la nacionalización de Runet, la red rusa, que permitiría a Russia aislarse de Internet, la red global. Bajo el argumento de aumentar la resiliencia ante los ciberataques se esconde el deseo de controlar la información que consumen sus ciudadanos. China tiene el mayor "cortafuegos digital" con el que restringe el acceso a los contenidos de Internet a su población, es decir al mayor número mundial de usuarios. VENABLES, A., "Establishing cyber Sovereignty- Russia Follows China's Example", International Center for Defence and Security, 20 marzo 2019. Disponible en: HTTPS://ICDS.EE/ESTABLISHING-CYBER-SOVEREIGNTY-RUSSIA-FOLLOWS-CHINAS-EXAMPLE/
CHINA Y RUSIA INSISTEN EN EL MODELO JURÍDICO MULTILATERAL (DESCONFÍAN DE LOS ACTORES NO ESTATALES) Y TAL COMO ESTABLECE EL CÓDIGO DE CONDUCTA PARA LA SEGURIDAD DE LA INFORMACIÓN (ORGANIZACIÓN PARA LA COOPERACIÓN DE SHANGHÁI) DEFIENDEN UNA GESTIÓN MULTILATERAL DE INTERNET. ROBERTS, A., *op. cit.* 139, p. 314.

en momentos de retorno a las rivalidades geopolíticas y geoeconómicas y, de alcanzarse, estaría perforado por las reservas con lo cual, en la práctica, se degradaría su efecto.[158] Otro problema más que generaría un nuevo tratado global, en opinión de Bruno Lété y Peter Chase, es que se correría el peligro de que entrara en contradicción y cuestionara el derecho existente.[159]

La aplicabilidad del Derecho internacional existente no resulta fácil y los principales escollos surgen a propósito de la aplicabilidad del uso de la fuerza y de las contramedidas a los ciberataques. Los tratados internacionales que regulan la guerra fueron redactados en momentos en que las ciberarmas ni siquiera formaban parte de la ciencia ficción.[160] Las definiciones de guerra, ataque armado y agresión son difíciles de traspasar al ciberespacio y a los ciberataques. Las analogías jurídicas no resuelven el tema. ¿Cuándo un ciberataque puede ser considerado acto de agresión o ataque armado?¿Cuándo se justifica el uso de la fuerza como legítima defensa individual o colectiva? Al igual que ya ocurrió en 2001 cuando los Estados Unidos fueron atacados por el terrorismo transnacional, las nuevas realidades ponen de manifiesto la inadecuación de los instrumentos jurídicos tradicionales y las opciones pueden ser crear nuevos instrumentos o interpretar los existentes de manera adaptativa. En esta dirección algunos autores han propuesto considerar determinados ciberataques como ataques armados no convencionales, basándose en sus consecuencias.[161] Las ciberoperaciones que causan daños similares a los producidos por las armas convencionales, químicas, biológicas o nucleares, es decir, que provocan lesiones o muerte a las personas o destruyen física o funcionalmente objetos e infraestructuras deberían ser consideradas, según este criterio, equivalentes a un ataque armado.[162] Otros incluso serían partidarios de una concepción más amplia ya que argumentan que algunos ciberataques pueden causar daños muy serios a la economía y a la vida política de un país sin que se produzca destrucción física.[163] Pero sigue sin haber un consen-

---

158 SCHMITT, M.N. y VITUL, L., *op. cit.*, nota 132, p.39.

159 LÉTÉ, B. y CHASE, P., *op. cit.,* nota 119.

160 El gusano informático Stuxnet (ver nota 122), creado con objetivos militares, es considerado la primera arma cibernética.

161 SKELEROV, M. J., "Solving the Dilemma of State Response to Cyberattacks: a Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent", *Military Law Review*, 2009, vol. 201, pp. 1-85. Estas cuestiones jurídicas fundamentales escapan al objeto central de este trabajo. Algunos trabajos que recogen las discusiones al respectos son: LÉTÉ, B. y CHASSE P., *op. cit.,* nota 119; MELZER, N., *op. cit.*, nota 114; SHACKELFORD, S., *op. cit.*, nota 116; SIMONET, L., *op. cit,* nota 113.

162 MELZER, N., *op. cit.*, nota 114, p. 7.

163 Se considera que el ciberataque a la central iraní de Natanz tuvo el mismo efecto destructivo que una ráfaga de misiles. KUSHNER, D., "The Real Story of Stuxnet", *IEEE Sprectrum,* 26 de febrero de 2013. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Igualmente, algunos autores estiman que el ataque sufrido por

so generalizado ni sobre esta ni sobre tantas otras cuestiones, más allá de que lo importante no son los instrumentos sino los efectos, y se sigue actuando sobre la base del caso por caso.

Estrechamente vinculada a la cuestión de la aplicabilidad del Derecho internacional, en quinto lugar, la regulación de la ciberseguridad se enfrenta al enorme *problema de la atribución de responsabilidad*.[164] Por una parte, determinar la responsabilidad de los ciberataques es extremadamente complejo ya que entre las habilidades de los autores se cuentan las de proteger su anonimato y las de derivar la responsabilidad hacia otros actores. Incluso en aquellos casos que parece clara la relación entre un actor y un ciberataque, como en el ya mencionado caso de los ciberataques sufridos por Estonia en 2007, y en los que todos los expertos y analistas atribuyen a Rusia la responsabilidad, ésta no se puede probar. A pesar de que los ataques fueron lanzados desde direcciones IP rusas y las instrucciones en línea estaban en ruso, no se ha podido demostrar que los atacantes siguieran órdenes del gobierno ruso. Por otra parte, el Derecho internacional regula las relaciones entre Estados y la noción de agresión remite a los Estados mientras que los ciberataques no son necesariamente ejecutados por las autoridades estatales. Las investigaciones son largas y costosas y los resultados no suelen ser concluyentes. Esto ha llevado a hablar de una "guerra asimétrica" porque los Estados se enfrentan a un atacante "invisible" o de difícil, si no imposible, identificación y ello merma su capacidad defensiva, cuestionando la estrategia militar moderna.[165]

5.2. Procesos e instrumentos normativos y deliberativos

En este apartado se analizan, sin ánimo exhaustivo, algunas de las principales iniciativas normativas, así como algunos procesos cooperativos y deliberativos representativos de los diferentes tipos de actores implicados en el proceso normativo del ciberespacio y la ciberseguridad. El objetivo es identificar los grandes temas discutidos, los acuerdos alcanzados y las cuestiones en que existen claros desacuerdos o en las que no ha sido posible alcanzar un acuerdo por falta del consenso necesario.

5.2.1. Procesos multilaterales universales

Las Naciones Unidas (NU) lideran la iniciativa reguladora de carácter multilateral más importante. A pesar de no generar acuerdos vinculantes, el proceso

---

Estonia en 2007, tuvo consecuencias equivalentes a las de un ataque armado. SIMONET, L., *op. cit,* nota 113, p. 125.

164 SIMONET, L., *op. cit,* nota 113, p.134.

165 *Ibíd.,* p. 136

negociador es lento y arduo porque los intereses de las partes son muy diferentes y porque las temáticas tratadas son muy amplias y políticamente complejas. NU han sido también el escenario de enfrentamiento de los dos grandes enfoques (occidental-no occidental) de la regulación del ciberespacio y la ciberseguridad. Por ello, llegar a los acuerdos que se han ido adoptando han sido costoso y, en consecuencia, estos son muy relevantes. Se ha conseguido perfilar el mínimo común denominador necesario para ser aceptados por todas las partes. Se han resuelto algunas cuestiones clave sobre las que no existía acuerdo previo y estos acuerdos se han convertido en normas que guían la conducta de los Estados, crean expectativas colectivas, y sirven de base para que se avance en otros ámbitos y en otros foros.

La Organización se ocupa de la seguridad en el ciberespacio desde que 1998 Rusia presentara un proyecto de resolución a la Primera Comisión de la Asamblea General (AG). Al presentarla ante la Comisión de Desarme y Seguridad, Rusia pretendía marcar el carácter político-militar de la cuestión (ciberguerra), frente a la opción estadounidense de redefinirla de manera más estrecha, centrándose solo en los aspectos económicos (cibercrimen).[166] La resolución, breve y de carácter general, instaba a los Estados miembros a examinar multilateralmente el tema de los peligros en materia de seguridad informática y a transmitir sus opiniones al Secretario General (SG), quien debería redactar un informe. Se pedía el seguimiento del tema por la AG. Hacía una triple llamada normativa a los Estados: debían esforzarse en conseguir la óptima explotación de las TIC para el desarrollo a través de la cooperación internacional; respaldar la estabilidad estratégica y la seguridad estatal; y prevenir el uso criminal o terrorista de las tecnologías.[167] Desde entonces, anualmente, el SG ha redactado informes en base a los informes nacionales que, voluntariamente, le hacen llegar los Estados. Igualmente se publican los informes nacionales completos.[168]

---

166 Por su parte, Estados Unidos en 2001 presentó una resolución –Lucha contra la utilización de la tecnología de la información con fines delictivos– (AG Res. 55/63) a la tercera Comisión (Asuntos –sociales, humanitarios y culturales) y en 2003 otra –Creación de una cultura mundial de seguridad cibernética. AG Res 57/239- a la Segunda (Asuntos económicos y financieros)

167 Resolución 53/70. Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional (https://undocs.org/es/A/RES/53/70). Fue aprobada por consenso, después de que Estados Unidos consiguiera eliminar algunos elementos claves de la misma: las referencias al uso de la tecnología de la información con objetivos militares, las definiciones concretas de "armas informativas" y de "guerra informativa" y el equiparamiento entre estas y las armas de destrucción masiva. AUSTIN, G. "International Legal Norms in Cyberspace: Evolution of China's National Security Motivations", en OSULA, A-M. y RÕIGAS, H., *op. cit*., nota 61, pp.171-201, p. 181.

168 https://www.un.org/disarmament/ict-security

En 2004, las NU crearon un primer grupo de trabajo, el *Grupo de Expertos Gubernamentales en el campo de la Información y las Telecomunicaciones en el contexto de la Seguridad Internacional* (en adelante GEG). Hasta el momento se han creado seis grupos. En cuanto a su composición, los grupos están integrados por los cinco miembros permanentes del Consejo de Seguridad (CdS) además de por otros Estados (entre 10 y 20) elegidos atendiendo a criterios de representación geográfica, equilibrio político e interés en la materia.[169] La Oficina del Alto Representante para el Desarme es quien propone la composición del grupo al SG. En 2018 se creó, en paralelo al GEG, otro Grupo de Trabajo de Composición Abierta (GTCA) que permite la participación de todos los Estados que lo deseen. Es interesante destacar que se ha operado un cambio en el perfil de los representantes seleccionados por cada Estado. Al principio, respondiendo a la visión tecnicista de la problemática, eran diplomáticos y expertos técnicos. Progresivamente, a medida que los Estados han reconocido el carácter eminentemente político de las negociaciones, han ido designando representantes con perfiles políticos. Hoy en día los expertos técnicos en TIC ocupan un lugar secundario, mientras que quienes negocian son expertos en diplomacia, control de armas y no proliferación.[170] No se admiten observadores de ningún tipo, ni gubernamentales ni privados. En varias ocasiones, dada su proximidad con la temàtica, ha sido sugerida, y rechazada, la participación de la Unión Internacional de Telecomunicaciones (UIT). La negativa demuestra la férrea voluntad de la AG de mantener los trabajos del GEG en el ámbito de la seguridad y el desarme y separarlos netamente de las cuestionas técnicas asociadas a las TIC. Esta decisión es lógica e inevitable a la luz de los controvertidos temas que se tratan en el GEG: la responsabilidad de los Estados vis-a-vis los actos de actores no estatales operando desde su territorio contra la infraestructura de otros Estados; la operacionalización de la norma de no atacar las infraestructuras críticas en tiempo de paz; la consideración o no de éstas como bienes públicos globales; la opción por el desarme o la desmilitarización del ciberespacio o por la precisión de la aplicación del derecho de los conflictos armados en el ciberespacio; la implicación de los países en desarrollo en el GEG; la atribución de la responsabilidad de los ciberataques, un reto tridimensional (técnico, jurídico y político); o el control del uso dual de la cibertecnología. A nivel procedimental, el grupo opera con un formato cerrado para favorecer las discusiones y las decisiones se toman por consenso.

No todos los GEG han conseguido alcanzar acuerdos para avanzar en la regulación del ciberespacio. Pero, en conjunto, el GEG, como proceso, ha conseguido

169 Para una información detallada sobre la composición de cada grupo y su funcionamiento, consúltese: https://www.un.org/disarmament/ict-security y https://dig.watch/processes/un-gge.

170 https://dig.watch/processes/un-gge

tres grandes logros: mantener de manera permanente la ciberseguridad global en la agenda de Naciones Unidas, definir el contenido de la agenda de ciberseguridad global e introducir el principio de la aplicabilidad del Derecho internacional al ciberespacio (Informe de 2013). Este último logro se considera un hito en el avance de la ciberregulación. Los resultados son importantes, pero el proceso en sí también lo es. En este sentido, todos los GEG han hecho aportaciones importantes a la regulación normativa por el solo hecho de poner sobre la mesa negociadora temas de profundo calado sobre los que los Estados han tenido que pronunciarse.

El primer GEG (2004-2005) se centró en el examen del impacto de los desarrollos de las TIC sobre la seguridad nacional y los asuntos militares. El debate giró en torno a dos cuestiones problemáticas: cómo caracterizar la amenaza planteada por la explotación estatal de las TIC con fines militares y si las discusiones debían focalizarse en el contenido de la información o en la infraestructura. No fue posible el consenso.[171]

El segundo grupo (2009-2010), primero en emitir un informe final, instó a abrir el diálogo entre los Estados sobre el uso delas TIC a fin de proteger las infraestructuras críticas; a crear medias de confianza y de reducción de riesgos; a intercambiar información sobre legislaciones nacionales y estrategias de ciberseguridad; y a ayudar al desarrollo de medidas de confianza en los países en desarrollo.[172]

El tercer grupo (2012-2013) es el que ha producido el informe más determinante hasta el momento.[173] Partía de la premisa de que el fomento de la cooperación era fundamental para el establecimiento de un entorno pacífico, seguro, resistente y abierto para las TIC. Sus conclusiones pusieron punto final al debate sobre si el ciberespacio era un espacio sin normas o no.[174] Estableció que la aplicación de las medidas del Derecho internacional vigente pertinentes para el uso de las TIC era una medida fundamental para alcanzar la paz, la seguridad y la estabilidad internacionales (art. 16). Al afirmar que el Derecho internacional y, especialmente la Carta de NU, aplican al ciberespacio (art. 19), el GEG dio protagonismo a los Estados en la gestión de la ciberseguridad y reforzó su soberanía. El ciberespacio dejaba de ser

---

171 RES. A/60/202, Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, https://undocs.org/es/A/60/202.

172 RES. A/65/201. Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional https://undocs.org/es/A/65/201

173 RES. A/68/98* Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. https://undocs.org/es/A/68/98´-

174 Ver apartado III. Recomendaciones sobre normas, reglas y principios de conducta estatal responsable. Artículos 16 a 25, A/68/98*, pp 7 a 9. https://undocs.org/es/A/68/98.

un espacio global, trasnacional y ajurídico y se convertía en un espacio territorial diferente al resto de espacios territoriales, pero sobre el que los Estados podían ejercer su jurisdicción. El informe llamaba a los Estados a respetar los Derechos Humanos y las libertades en todas sus actividades para conseguir la ciberseguridad (art. 21). Establecía la obligación de cooperar en la lucha contra el ciberterrorismo y el ciberdelito (art. 22). Establecía la responsabilidad de los Estados y les instaba a asumir sus obligaciones respecto a los hechos internacionalmente ilícitos que se les puedan atribuir, a no valerse de agentes para cometer actos ilícitos y a no hacer un uso ilícito de las TIC (art. 23). Instaba a los Estados a alentar al sector privado y la sociedad civil a contribuir a la mejora de la seguridad de las TIC (arts. 24 y 25). El informe incluía recomendaciones sobre la adopción de medidas voluntarias para incrementar la confianza y la transparencia (apartado IV) y sobre la cooperación internacional para crear capacidades en la esfera de la seguridad de las TIC, especialmente en los países en desarrollo (apartado V).

Este informe, al reconocer la aplicabilidad del Derecho internacional existente –extremo que China y Rusia negaban para justificar la necesidad de un nuevo tratado sobre el ciberespacio– fue una victoria del campo occidental pero, parcialmente, también de estos dos países, al reconocerse el principio de soberanía estatal y de las normas y principios de ella derivadas, incluido el reconocimiento de la jurisdicción estatal sobre las infraestructuras de las TIC situadas en su territorio.[175]

El cuarto grupo (2014-2015) avanzó en la detección de las normas, reglas y principios de Derecho internacional aplicables a los Estados en el ciberespacio (entre otros el del principio de soberanía, el de arreglo pacífico de controversias y el de no injerencia en los asuntos internos) a la vez que insistía en algunas de las conclusiones ya alcanzadas por el anterior grupo (respeto de los Derechos Humanos, abstención estatal de contratar a agentes interpuestos para cometer ciberdelitos o ciberataques y control estatal del territorio para evitar que sea usado por ciberactores no estatales para cometer delitos). Finalmente, en una apuesta clara por el multilateralismo tradicional, establecía el rol líder de las NU en la promoción del ciberdiálogo y en el desarrollo de consensos sobre la aplicación del Derecho internacional.[176]

Finalmente el quinto y último grupo que había terminado su mandato (2016-2017) en el momento de redactar este trabajo, siguió los trabajos de los grupos

175 ROBERTS, A., *op. cit.*, nota 139, p. 311. Rusia y China también consiguieron frenar la inclusión de una mención a la aplicabilidad del Derecho internacional humanitario a pesar del consenso existente entre los países occidentales y la comunidad académica. El Manual de Tallín lo admitiría sin ambages. SCHMITT, M.N. y VIHUL, L., *op. cit.,* nota 132, pp. 34 et ss.

176 RES A/70/74, Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, https://undocs.org/es/A/70/74.

anteriores –análisis de las amenazas existentes y emergentes, construcción de capacidades, medidas de confianza, aplicación del Derecho internacional a las TIC y aplicación de normas, reglas y principios para la conducta responsable de los Estados– pero concluyó sin alcanzar un informe de consenso.[177] Se atribuye el fracaso a la posición cubana que, en línea con los intereses de Rusia y China, frenó el acuerdo sobre la aplicación de contramedidas y del Derecho internacional humanitario en el ciberespacio.[178] La falta de consenso ha sido calificada de "callejón sin salida del GEG" debido a que las diferencias ideológicas que lo motivaron parecen insalvables y, además, se les suman divergencias derivadas de la posesión o no de cibercapacidades.[179]

Sin embargo el proceso sigue. Los dos grupos de trabajo que actualmente están desarrollando su mandato deben concluir en 2021. Como novedades, se puede destacar que el sexto GEG tiene el mandato de ampliar los debates y consultas a las organizaciones regionales.[180] Respecto al GTCA, además de su composición universal, la gran novedad que acompaña su creación es que podrá llevar a cabo consultas informales con la industria del sector de las TIC.[181]

Sin duda el proceso del GEG es un proceso largo y con resultados intermitentes y desiguales pero que ha conseguido ciertas clarificaciones relevantes. El nuevo formato del GTCA puede introducir cambios significativos –ampliar las voces de los países del Sur global– o puede acabar sin consenso porque a mayor número de actores, mayor dificultad de acuerdo. No obstante hay que concederle tiempo y ver qué pueden dar de sí los diferentes formatos de reunión, a la vez que se experimentan las posibilidades de otras plataformas multilaterales.[182] Hasta el momento, además de los consensos alcanzados, se le puede reconocer el mérito de catalizar el interés internacional sobre la ciberseguridad.[183]

---

177 RES A/72/327, Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, https://undocs.org/A/72/327.

178 LÉTÉ; B. y CHASE, P., *op. cit.,* nota 119.

179 HENRIKSEN, A., *op. cit.*, nota 137, p. 5. Las revelaciones de Snowden pusieron de manifiesto las diferencias de opinión sobre la privacidad y la seguridad entre Estados ideológicamente afines (a favor de la libertad en Internet). A raíz del caso Wikileaks los Estados liberales menos ciberpoderosos vieron claro que sus intereses en la gobernanza del ciberespacio diferían enormemente de los de los Estados Unidos.

180 RES A/73/266, Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, https://undocs.org/es/A/RES/73/266.

181 RES A/73/27/, Informe de la Conferencia de Desarme. Período de sesiones de 2018, https://undocs.org/es/A/73/27

182 LÉTÉ, B. y CHASSE, P., *op. cit.,* nota 119.

183 LEWIS, J. (con el apoyo de VIGNARD, K.), op. cit., nota 117, p. 20

5.2.2. Procesos e instrumentos impulsados por organizaciones regionales

La tendencia a la regionalización impera en el ámbito de la ciberseguridad. La fragmentación de la ciberregulación refleja la coincidencia de intereses y enfoques entre Estados y actores afines. La afinidad les permite avanzar a mayor velocidad que los procesos multilaterales. En este recogemos algunos ejemplos significativos de esta tendencia.[184]

a) Manuales de Tallín

El Manual de Tallín sobre el Derecho internacional aplicable a la ciberguerra[185] y el Manual de Tallín sobre el Derecho internacional aplicable a las ciberoperaciones[186] son dos documentos elaborados por el Grupo Internacional de Expertos subvencionado por el Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN, en 2013 y 2017 respectivamente. A pesar de haber sido impulsados por la OTAN no son textos ni acuerdos oficiales de la OTAN. Se trata de textos académicos, no vinculantes, que expresan la opinión de sus autores. En palabras del director de ambos proyectos: "El Manual de Tallin consiste en 'normas' adoptadas unánimemente por el Grupo Internacional de Expertos que reflejan el Derecho internacional consuetudinario, acompañadas por 'comentarios' que perfilan sus bases legales y subrayan las diferencias de opinión entre los expertos así cómo su interpretación en el cibercontexto."[187] Esto no impide que los países miembros de la OTAN adopten este "corpus normativo"como guía.[188]

El primero es el resultado de un proyecto de investigación llevado a cabo entre 2009 y 2012 por una veintena de académicos y profesionales, apoyados por ex-

---

184 Algunos ejemplos no desarrollados en este capítulo son, entre otros, la Convención de la Unión Africana sobre seguridad y protección de datos personales (2014, a fecha de junio 2019 no había alcanzado las 15 ratificaciones necesarias para entrar en vigor); el Acuerdo de la organización para la Cooperación de Shanghái sobre la cooperación en el campo de la seguridad de la información internacional (2009); la Declaración de Brazaville (2016, Recomendaciones del secretariado de la Comunidad Económica de Estados de África Central sobre ciberseguridad); o la Directiva de la UE sobre redes y sistemas informativos (2016). Para un listado completo de los diferentes instrumentos véase, VAN HORENBEECK, M. (ed.), *Cybersecutity Agreements . Background Paper to the IGF Best practicves Forum on Cybersecurity,* IGF, 2019

185 SCHMITT, M.N., *op. cit* nota 109.

186 SCHMITT, M.N., (gral. ed.) y VIHUL, L. (man., ed). *Tallinn Manual on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017.

187 SCHMITT, M.N, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", *Harvard International Law Review,* vol. 54, núm. 2, 2012, pp.13-37 (15)

188 FONSECA, C.E. et al., "El Manual de Tallín y la Aplicabilidad del Derecho Internacional a la Ciberguerra", *Revista de la ESG,* núm. 588, 2014, pp. 126-146 (136).

pertos técnicos,[189] y analiza la aplicabilidad del Derecho internacional Humanitario a la ciberguerra. En el proceso participaron observadores del Mando Aliado de Transformación de la OTAN, del Cibercomando de los Estados Unidos y de la Cruz Roja. Una vez redactado el texto, a fin de dotarlo de legitimidad científica, fue sometido a un proceso de revisión por pares en el que participaron otra treintena de académicos. También se recibieron los comentarios oficiales y no oficiales de los Estados que quisieron hacerlos.[190]

El Manual de Tallín es el documento que analiza con mayor profundidad todas las cuestiones relativas al Derecho internacional en el ciberespacio. Por cuestiones de espacio y pertinencia, recogeremos aquí tan solo a sus principales conclusiones, obviando algunos de los importantes debates interpretativos que suscitaron y que quedan recogidos en los comentarios del Manual.[191] La cuestión más destacable es la ya mencionada conclusión de que el Derecho internacional puede aplicarse, sin ninguna duda, a las ciberactividades ya que son desarrolladas por individuos que usan objetos tangibles en dominios físicos que forman parte de la arquitectura normativa del Derecho internacional. Así, el ciberespacio no es una zona libre de Derecho en el que cualquiera pueda llevar a cabo conductas hostiles sin reglas ni límites Esta afirmación no es incompatible con el reconocimiento de la dificultad interpretativa que surge de la naturaleza única de las ciberactividades derivada del hecho de que pueden provocar efectos devastadores sin causar daño físico ni matar. El Director del proyecto se sorprendía del tiempo que había tomado y lo dificultoso que había resultado que los Estados aceptaran lo obvio. Por ello insistía en subrayar la importancia de haber empezado"el viaje".[192]

El Manual establece además de manera clara y contundente que, en el contexto de un conflicto armado, el Derecho de la Guerra aplica para regular el uso de ciberinstrumentos en las hostilidades. Los principios de necesidad y proporcionalidad limitan el uso de la fuerza en caso de legítima defensa y deben establecer qué se considera una respuesta adecuada bajo cada circunstancia. En el contexto de los ciberconflictos, de la misma manera que los principios de la Carta de UN relativos a la prohibición del uso de la fuerza y la legítima defensa aplican a cualquier uso de la fuerza independientemente de las armas utilizadas,[193] el uso de ciberinstrumentos o ciberarmas, en lugar de armas convencionales, no afecta a la calificación de

---

189 Aunque numerosos miembros del grupo ocupaban altos cargos en sus países, participaban en el proyecto a título individual. SCHMITT, M.N. *op. cit,* nota 109*,* p. 14.

190 *Ibíd*.

191 Si no indicamos lo contrario, seguiremos el análisis realizado por el editor general, Michael Schmitt en SCHMITT, M.N., *op. cit.,* nota 109.

192 *Ibíd*., pp. 36-37.

193 Los expertos aplicaron la lógica de la Opinión consultiva de la Corte Internacional de Justicia sobre la legalidad o el empleo de armas nucleares. A/51/ 218, https://www.icj-cij.org/files/advisory-opinions/advisory-opinions-1996-es.pdf

una operación como uso de la fuerza. Las ciberactividades pueden ser consideradas uso de la fuerza, en el sentido del artículo 2 (4) de la Carta de UN y del Derecho internacional consuetudinario, cuando sus efectos son comparables a los de otras operaciones tradicionales en las que se hiere o se mata a personas o se provocan daños o destruyen bienes materiales e infraestructuras. El Manual también considera aplicable a las ciberoperaciones la cláusula Martens: no porque un acto no esté explícitamente prohibido puede ser considerado legal o autorizado. Cuando no haya Derecho internacional aplicable, los civiles y combatientes quedarán bajo la protección y la autoridad de los principios de Derecho internacional consuetudinario, de los principios de humanidad y de los dictados de la conciencia política.

Al ocuparse del derecho a la legítima defensa, reconocida por el art. 51 de la Carta de UN, el Manual admite que un Estado puede responder a un ciberataque ejerciendo ese derecho cuando sea equivalente a un ataque armado o a una amenaza inminente.Los expertos establecieron que no todos actos de uso de la fuerza son ataquesarmados y, siguiendo las recomendaciones de la Corte Internacional de Justicia, distinguieron entre las formas más graves de uso de la fuerza que constituyen un ataque armado, de otras formas menos graves, que no.[194] En el caso de la legítima defensa anticipada frente a un ciberataque, el Manual aplica la misma lógica que a cualquier tipo de ataque: el Estado puede actuar anticipadamente si hay indicios claros de que va a ser atacado y si el hecho de no actuar le supondría perder la capacidad de defenderse.[195] El Manual también considera un ataque armado toda ciberacción realizada por un actor no estatal, cuando se trata de un grupo organizado (no de individuos aislados) y justifica el uso de la fuerza contra él en base a la escala y los efectos de la acción. En lo que concierne al DIH, el Manual reconoce el principio de distinción entre civiles y combatientes, aunque recoge que su aplicación reviste una gran complejidad ya que los ciberataques contra ordenadores de civiles no provocan necesariamente daños físicos. De nuevo se impone la lógica de la calificación de los actos en virtud de sus consecuencias, remitiendo al análisis caso a caso.[196] En materia de soberanía, el Manual establece que ningún Estado puede reclamar la soberanía

194 Aun con todo los expertos no se pusieron de acuerdo en cómo se traslada esto al ciberespacio ya que algunos defendían que un ciberataque contra la economía de un país que produzca un impacto de gran magnitud debería justificar la calificación de ataque armado, aunque no cause daño ni destrucción física, y otros lo rechazaban.

195 Por el contrario se rechazó la idea de la defensa preventiva (emprender acciones defensivas cuando el atacante aún no tiene los medios o, sí los tiene, no hay evidencias de que se disponga a atacar).

196 La adopción del principio de distinción no zanjó todas las cuestiones ya que, en el ámbito del ciberespacio, la línea entre civil-militar no siempre es nítida. La interconectividad hace que, por ejemplo, un ataque a instalaciones militares pueda generar un grave impacto en sistemas civiles. Otro caso que generaba dudas fue el de la cada vez más frecuente utilización de plataformas civiles, como las redes sociales, en los conflictos

sobre el ciberespacio. No obstante, los Estados pueden ejercer sus prerrogativas soberanas sobre las ciberinfraestrucucturas ubicadas en sus territorios –sean públicas o privadas–, sobre las personas implicadas en ciberactividades que se desarrollen en su territorio y extraterritorialmente, de acuerdo con el Derecho internacional (un Estado tiene jurisdicción sobre una actividad iniciada en su territorio independientemente de donde se produzcan los efectos). La soberanía también genera obligaciones: un Estado no debe permitir ciberactividades ilícitas contra otros Estados iniciadas desde su territorio o utilizando sus infraestructuras tecnológicas. Respecto a la responsabilidad, el Manual determina que los Estados son responsables de las ciberoperaciones que les sean atribuibles y que constituyan violaciones de obligaciones internacionales, ya sea por acción o por omisión. Igualmente, un Estado es responsable de las acciones de actores no estatales a los que haya dado instrucciones específicas o que haya controlado directamente. Sin embargo, no es suficiente que un ciberataque sea lanzado desde el territorio de un Estado para determinar su responsabilidad. Se requieren evidencias que permitan asociarle a dicha acción. Y, lamentablemente, no fue posible el desarrollo normativo de criterios de atribución de responsabilidades ni de los estándares de evidencia necesarios para la atribución de responsabilidades.

Marco Roscini, autor de una de las más exhaustivas obras sobre las ciberoperaciones y el uso de la fuerza en el Derecho internacional, apunta otras deficiencias importantes del Manual de Tallín: el no haber tratado, o haberlo hecho superficialmente, algunas cuestiones tales como la aplicación del principio de no intervención al ciberespacio; el no ser concluyente en la definición del umbral a partir del cual una ciberoperación es considerada uso de la fuerza; y la poca discusión sobre las ciberoperaciones de espionaje y su consideración como actos hostiles. A pesar de ello, lo considera un hito en la ciberregulación, en tanto que primer intento de demostrar que el Derecho internacional es lo suficientemente flexible como para ser aplicado al ciberespacio y punto de partida de un proceso de interpretación normativa a largo plazo.[197]

El proceso que condujo a la elaboración del Manual de Tallín 2.0 fue similar al del primero con algunas variaciones menores. Por ejemplo, se amplió el origen geográfico del grupo de expertos para responder a las críticas recibidas acerca de la procedencia eminentemente occidental de los miembros del primer grupo.[198]

---

armados. Los expertos concluyeron que cuando son utilizadas con fines militares se convierten en objetivos militares.

197 ROSCINI, M., *op. cit,* nota 128, p. 32.

198 JENSEN, T. E., "The Tallinn Manual 2.0: Highlights and Insights", *Georgetown Journal of International Law,* vol. 48, 2017, pp. 735-778 (738) y ROSCINI, M., *op. cit*., nota 127, p. 31. Marco Roscini precisa que 9 de los 23 expertos del primer grupo eran de origen estadounidense y que no se incluyó a ninguno de origen ruso o chino a pesar de que Rusia y China son dos de los principales Estados implicados en ciberoperaciones. *Ibíd*.

En relación al contenido, la novedad fundamental es que en él se amplía el foco de atención y se analizan los ciberincidentes más comunes, los que no alcanzan el umbral del uso de la fuerza ni se dan en situaciones de conflicto armado. Tallín 2.0 examina en detalle la aplicabilidad de numerosos regímenes internacionales (Derechos Humanos, Derecho del Mar, Derecho del Espacio, Derecho diplomático y consular) a las ciberoperaciones.[199] En general, reafirma la mayoría de principios admitidos por el primer Manual y sigue profundizando en las cuestiones de difícil interpretación más allá de estos principios. Pero como señala Eric Jensen Talbot, tras Tallín 2.0 todavía falta claridad normativa y hay muchas áreas de desacuerdo, incluso entre los expertos que redactaron ambos Manuales. Además, hay muchas situaciones respecto a las que los Estados no se han pronunciado. Con todo, mientras los Estados no clarifiquen sus posiciones, Tallín 2.0 es el punto de partida para que el Derecho avance en el campo de las ciberoperaciones.[200]

b) Convenio sobre la Ciberdelincuencia

El Convenio de Budapest, auspiciado por el Consejo de Europa (CdE), es el acuerdo internacional más relevante sobre un tema concreto relacionado con la ciberseguridad, la ciberdelincuencia. Desde los años 80, el CdE se ocupaba del tema con un enfoque penalista, pero no fue hasta inicios del nuevo siglo que se pudo concluir un tratado internacional. El Convenio fue aprobado en 2001 y entró en vigor desde 2004. La idea de un tratado internacional surgió de la cada vez más apremiante realidad de los ciberdelitos y del convencimiento de los Estados de la necesidad y urgencia de cooperar entre ellos y con el sector privado para luchar contra la ciberdelincuencia y proteger sus intereses en la utilización y desarrollo de las TIC. Desde su aprobación, las adhesiones se han ido ampliando progresivamente y, más importante, ha aumentado la calidad de la aplicación y el nivel de cooperación entre las partes.[201] Esta evolución exitosa es deudora de la fórmula que Alexander Seger denomina "el triángulo dinámico": el convenio se complementa con un mecanismo de seguimiento y con programas de

---

199 El Manual 2.0 también recoge los comentarios a las normas consensuadas así como las opiniones minoritarias. Para un análisis en profundidad, véase JENSEN, T.E., *op. cit.,* nota 198. El autor trabajó como experto en ambos grupos.

200 *Ibíd*., p. 778.

201 64 Estados ya son Parte (26 de ellos no miembros del Consejo de Europa); 3 han firmado y no ratificado; hay 35 reservas; otros 70 Estados lo han usado como guía para la elaboración de la legislación nacional, con lo cual se podría pensar que se está empezando a convertir en Derecho consuetudinario (SCHMITT, M.N. y VIHUL, L., *op. cit*., nota 132, p. 40); y unos 160 han colaborado con el Consejo de Europa en actividades de construcción de capacidades. SEGER, A., "Enhanced cooperación on cybercrime: a case for a protocol to the Budapest Convention", 16 de julio de 2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

construcción de capacidades.[202] El convenio clarifica los tipos elementos que las partes pueden utilitzar para luchar eficazmente contra la ciberdelincuencia: las ciberconductas que han sido criminalizadas (capítulo I. Terminología); los poderes procesales con los que las autoridades de la justicia criminal pueden garantizar la evidencia electrónica en relación con cada crimen (capítulo II. Medidas a adoptar a nivel nacional); y los instrumentos de cooperación internacional en la persecución del cibercrimen y la búsqueda de las evidencias electrónicas (capítulo III. Cooperación internacional).[203] En 2006 se aprobó el Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.

c) Decisiones sobre medidas para fomentar la confianza

Algunas organizaciones regionales (Organización para la Seguridad y Cooperación en Europa –OSCE–, ASEAN Regional Forum, Organización de Estados Americanos), NU, e incluso Estados a través de acuerdos bilaterales están desarrollando medidas de fomento de la confianza (MFC) en el ámbito del ciberespacio como un complemento a las cibernormas y como una ayuda a la construcción de cibercapacidades para crear un ciberespacio estable y seguro. En algunas ocasiones las MFC sirven para garantizar la aplicación efectiva de ciertas normas. En otras impulsan la construcción de capacidades. Y, en otras, las MFC son impulsadas para evitar los riesgos derivados de la producción de bienes y servicios que acompañan el desarrollo de las cibercapacidades.[204] Sin espacio para analizarlas todas nos referiremos a las de la OSCE ya que tradicionalmente ha sido la gran impulsora de MFC para aumentar la seguridad internacional. Desde 2012 ha introducido la ciberseguridad en su agenda y ha adoptado varias decisiones para fomentar las medidas de confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de las TIC.[205] En el ciberespacio como en cualquier otro ámbi-

---

202 SEGER, A., "The Budapest Convention on Cybercrime: a framework for capacity building", *Global Forum on Cyber Expertise,* 7 de diciembre de 2016, https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime

203 SEGER, A., *Ibid*.

204 PAWLAK, P., "Confidence-Building Measures in Cyberspace: Current Debates and Trends", en OSULA, A-M. y RÕIGAS, H., *op. cit.*, nota 61, pp. 129-153.

205 PC.DEC/1039 de 26 de abril de 2012. Elaboración de medidas de fomento de la confianza para reducir los riesgos de conflictos dimanantes del uso de tecnologías de la información y las comunicaciones; PC.DEC/1106 de 3 de diciembre de 2013. Conjunto inicial de medidas de la OSCE para el fomento de la confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de tecnologías de la información y la comunicación; y PC.DEC/1202 de 10 de marzo de 2016. Medidas de la OSCE para el fomento de la confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de tecnologías de la información y la comunicación.

to de la seguridad el objetivo de las MFC es restringir el uso de la violencia a través del aumento de la transparencia y el intercambio de información. Al igual que cualquier decisión de la OSCE, éstas no son vinculantes y su aplicación depende de la voluntad de los Estados. Es remarcable la insistencia, explicita en todos y cada uno de los artículos, en que los Estados llevarán a cabo las actividades propuestas de manera voluntaria y en el nivel que estimen oportuno.

La primera decisión, adoptada en 2012, encargaba a la Presidencia de la OSCE, la creación de un grupo oficioso de composición abierta en el marco del Comité de Seguridad, responsable de elaborar un conjunto de MFC con el fin de mejorar la cooperación, transparencia, previsibilidad y estabilidad internacionales y reducir los riesgos de conflicto derivados de uso de las TIC. La segunda decisión, adoptada en 2013, precisaba el contenido de las MFC: la presentación de las posturas nacionales sobre el tema; el fomento de la cooperación entre organismos nacionales, la realización de consultas a fin de reducir los riesgos derivados de percepciones erróneas; el intercambio de información sobre las medidas adoptadas por los diferentes Estados; la oferta de la OSCE como plataforma de diálogo e intercambio de buenas prácticas; la elaboración de normativas nacionales modernas y eficaces; y la reunión tres veces al año del grupo de trabajo. La tercera decisión, adoptada en 2016, señalaba la complementariedad de las MFC con las iniciativas de UN y su conformidad con el Derecho internacional y con el Acta final de Helsinki. La novedad más destacable era la ampliación de los actores implicados en la creación de MFC: se instaba a los Estados a invitar a los actores del sector privado, del mundo académico, de los centros de excelencia y de la sociedad civil y se sugería el fomento de asociaciones público-privadas, así como la colaboración regional y subregional. También se llamaba a informar sobre las vulnerabilidades que afectan a las TIC. Todo ello, recordemos, siempre de manera voluntaria y en el nivel que los Estados consideren oportuno.

d) Recomendación sobre la gestión de riesgos de seguridad digital

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) elaboró en 2015 una Recomendación del Consejo sobre la gestión de riesgos de seguridad digital para la prosperidad económica y social.[206]Dada la naturaleza de la organización, su trabajo en el ámbito de la gestión del ciberespacio se ha orientado a resaltar los efectos de carácter económico de la ciberinseguridad. Deudora de este enfoque, la Recomendación transmitía dos mensajes claros: primero, enfatizaba el

206 OEDC, *Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document,* OECD, París, 2015. El documento acompañante es de carácter explicativo y no forma parte de la recomendación. Profundiza en los conceptos utilizados, los principios y su aplicabilidad.

carácter económico –que no tecnológico– de los efectos de los riesgos de la ciberinseguridad y apelaba a la gestión política, no tecnológica, de la misma, una gestión que tenga en cuenta los objetivos económicos y sociales de las organizaciones públicas y privadas; segundo, desde una visión próxima al sector privado de las TIC que defiende la libertad en el ciberespacio, advertía que la ciberseguridad completa es imposible si se quiere aprovechar el potencial que brindan las TIC, pero aseguraba que los riesgos pueden ser reducidos a un nivel acceptable si se gestionan eficientemente. La Recomendación llamaba a la cooperación de los sectores público y privado, bajo el liderazgo del primero. El instrumento, como recomendación que es, no tiene carácter vinculante sino que es una mera guía de conducta para aquellos Estados y organizaciones privadas que la suscriban. El espíritu que la inspira es el de aprovechar al máximo los beneficios económicos y sociales de las TIC, intentando mantener el máximo margen de libertad en el ciberespacio y gestionando los riesgos inherentes a su naturaleza. Los principios en los que se basa son: el deber de todas las partes a informarse y ser conscientes de los riesgos, la responsabilidad de todos los actores en su gestión, la protección de los Derechos Humanos y valores fundamentales, y la cooperación. Como principios operativos se señalan: la necesidad de una evaluación continuada de los riesgos, la necesidad de adoptar medidas de seguridad para contrarrestarlos, la obligación de seguir innovando, y la necesidad de dar continuidad a los planes de reducción de riesgos digitales. Sobre estas bases los Estados deberían desarrollar sus estrategias nacionales.

5.2.3. Procesos liderados por actores privados

a) Cibertriángulo de Weimar.

Esta es una iniciativa minilateralista o mini-multilateralista[207] liderada por el German Mashall Fund de Estados Unidos (GMF)[208] que entre 2017 y 2019 organizó

---

207 Los grupos minilateralistas o mini-multilateralistas responden a la idea de ofrecer una aproximación más pragmática e inteligente a los problemas de gobernanza global consistente en reunir en torno a la mesa de negociaciones al menor número de actores possibles, pero a los necesarios para obtener el mayor impacto en la solución de un problema determinado. NAIM, M., "Minilateralism. The Magic Number Get Real International Action", *Foreing Policy*, núm. 173, julio-agosto 2009, pp.135-136. https://foreignpolicy.com/2009/06/21/minilateralism/. Sobre la importanciacrecientedel mini-multilateralismo, véase: PATRICK, S., "Multilatéralisme à la carte. The New World of Global Governance", *Valdai Discussion Papers,* núm. 22, 2015; WRIGHT, T., "Toward Effective Multilateralism: Why Bigger Numbers May Not Be Better", *The Washington Quarterly,* vol. 3, 2009 núm. 3, pp. 163-180.

208 El nombre deriva de Triángulo de Weimar (TW), un grupo informal de Estados creado en 1991 por Francia, Alemania y Polonia para asistir a este último en su proceso de transición política. Actualmente es un instrumento para fomentar la cooperación trila-

una serie de tres mesas redondas en Varsovia, París y Berlín sobre las respuestas posibles a los ciberataques. El Cibertriángulo reunió a políticos, representantes de los ministerios de Asuntos Exteriores y de Defensa, directores de las unidades de ciberdefensa nacionales, asesores jurídicos, profesionales y especialistas académicos en Derecho internacional, representantes de las industrias TIC y de otras y miembros de la sociedad civil. Sus conclusiones se alinearon con los informes del GEG y con el Manual de Tallín. Asumían que los ciberataques son una realidad creciente; que la "democratización" del acceso a las ciberarmas constituye una grave amenaza a la seguridad; y que el peligro mayor proviene de los Estados y no del cibercrimen. Los representantes de los tres Estados afirmaron su alineamiento con la idea de que el Derecho internacional es aplicable a la conducta estatal en el ciberespacio y manifestaron su reticencia a una nueva Convención de Ginebra Digital que, en su opinión, debilitaría la aplicación del Derecho internacional y podría ser utilizada por Rusia y China para ejercer el control interno sobre sus ciudadanos y el acceso a la información de terceros países. En su opinión, las ambigüedades respecto a la aplicación del Derecho internacional, sobre todo en lo concerniente al uso de la fuerza, se dan porque su formulación proviene de una época en que no existían las tecnologías actuales, pero no las consideran paralizantes.[209]

b) Iniciativa a favor de un Convenio de Ginebra Digital

Las industrias del sector son protagonistas de los procesos normativos ya que a través de sus productos y servicios de mercado crean normas informales. La tecnología determina la evolución normativa.[210] Pero, además también llevan a cabo iniciativas que buscan implicar a otros actores dado que la iniciativa privada, aunque aparentemente se centra más en los aspectos técnicos, busca en todo momento limitar las políticas gubernamentales que puedan atentar contra la integridad del sector privado y, a la vez, conseguir compromisos vinculantes de los Estados. En esta dirección se sitúa la campaña a favor de la creación de un tratado internacional en materia digital liderada por la empresa Microsoft. Desde la pers-

---

teral y ayudar en la gestión de crisis. En su dimensión parlamentaria el TW, también se ha ocupado del tema de la ciberseguridad. Los senados francés y polaco y el Bundesrat alemán han organizado, en 2017, 2018 y 2019, tres conferencias parlamentarias sobre la ciberseguridad, la protección de datos y la inteligencia artificial.
El GMF es una organización privada que se define como no lucrativa y no partidista que fue fundada en 1972 con fondos alemanes en reconocimiento a la ayuda recibida por el Plan Marshall. Tiene su sede en Washington y siete oficinas en Europa. http://www.gmfus.org.

209 LÉTÉ, B. y CHASE, P., *op. cit.,* nota 119, pp. 7-8.

210 CHANTZOS, I. y ALAM, S., "Thecnological Integrity and the Role of Industry in EMerging Cyber Norms", en OSULA, A-M. y RÕIGAS, H., *op. cit*., nota 61, pp.203-220, p. 204.

pectiva empresarial es absolutamente necesario limitar la conducta de las ciberpotencias y hacerlo de forma vinculante. Su preocupación declarada es proteger a los ciudadanos de los ciberataques estatales y mantener el ciberespacio como un espacio de libertad y desarrollo. Su agenda oculta es proteger su negocio de la intrusión estatal. La empresa defiende que el reconocimiento de que el Derecho internacional aplica al ciberespacio es importante pero no es suficiente, y reclama regular de forma vinculante el comportamiento estatal en el ciberespacio de manera que no se pueda actuar contra los intereses empresariales en nombre de la seguridad. Desde el mundo empresarial se reconoce que será difícil, al requerirse la voluntad política y el compromiso de los Estados, pero se estima que si se ha conseguido en otras áreas geopolíticas tan complejas como la proliferación, bien puede conseguirse en esta.

La propuesta de convenio de Microsoft establece una serie de prohibiciones y de prescripciones. Prohíbe: atacar infraestructuras críticas con impacto sobre la seguridad de los ciudadanos; atacar sistemas cuya destrucción impacte negativamente en la economía global; hackear datos privados de periodistas y ciudadanos implicados en procesos electorales; usar las TIC para robar la propiedad intelectual corporativa o secretos comerciales e industriales con fines competitivos; e instar a la instalación de puertas traseras en la tecnología comercial. Exhorta a los Estados a: trabajar para alcanzar un acuerdo sobre la cooperación en materia de detección y comunicación de vulnerabilidades en los productos y servicios de masas; limitar la construcción de ciberarmas, controlar las existentes, y limitar su comercio y distribución; avanzar en acuerdos de no proliferación; utilizar todas las medidas a su alcance para sancionar a los Estados infractores; limitar su implicación en ciberoperaciones ofensivas; y ayudar al sector privado a detectar, contener y responder a los ciberataques.[211]

5.2.4. Iniciativas de participación múltiple

a) Comisión Global sobre la Estabilidad en el Ciberespacio (CGEC)

Es una comisión de participación multiple (*múltiple stakeholder*)[212] puesta en marcha, en 2017, por dos think tanks independientes, The Hague Centre for

---

211 Microsoft, "A Digital Convention to protect cyberspace", *Microsoft PolicyPapers*https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH; SMITH, B., "The need for a Digital Geneva Convention", 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/; "Creating a Digital Geneva Convention. Policy Recommendation, Trusted Cloud", https://news.microsoft.com/cloudforgood/policy/briefing-papers/trusted-cloud/creating-digital-geneva-convention.html

212 Son socios el gobierno de Holanda, Microsoft Corporation, la Agencia de Ciberseguridad de Singapur, el Ministerio de Asuntos Exteriores de Francia, la Internet Society y Afilias;

Strategic Studies y el EastWest Institute, con el objetivo de promover el conocimiento mutuo y el entendimiento entre los diferentes actores del ciberespacio para avanzar en la ciberseguridad. A través de la promoción del diálogo sobre la seguridad internacional entre las comunidades creadas por el ciberespacio, pretende contribuir a la coherencia de las políticas públicas y las normas relacionadas con la seguridad yla estabilidad en el ciberespacio. Los 26 Comisarios que la componen provienen de diferentes países y de distintos sectores profesionales –gubernamental, industrial, técnico y de la sociedad civil. La CGEC está vinculada a otras iniciativas existentes como la Comisión Global para la Gobernanza de Internet[213] o el Proceso de Londres (ver subapartado siguiente).

En 2018, la CGEC elaboró el Paquete normativo de Singapur consistente en seis nuevas normas para promover el uso pacífico del ciberespacio. Las normas van dirigidas tanto al sector público como al privado: 1) norma contra las falsificaciones; 2) norma contra la conversión de los dispositivos TIC en *botnets*; 3) norma para que los Estados creen un proceso para compartir el conocimiento de las vulnerabilidades; 4) norma para reducir y mitigar las vulnerabilidades; 5) norma sobre la ciberhigiene como base de la defensa;y 6) norma contras las ciberacciones ofensivas de los actores no estatales.[214]

b) Conferencia Global sobre el Ciberespacio (CGC)

La CGS, que también se conoce con el nombre de Proceso de Londres, son una serie de conferencias iniciadas en 2011, a partir de la Conferencia de Seguridad de Múnich (ver nota 10). Al principio su periodicidad era anual, pero desde la tercera pasaron a ser bienales. Reúnen a participantes de sectores y ámbitos diversos: representantes de gobiernos, de organizaciones internacionales, de empresas del sector privado y de asociaciones de empresas, del mundo académico y de la sociedad civil. Su objetivo es doble: promover la coope-

---

Son espónsores: el Ministerio japonés de Asuntos Internos y Comunicaciones, el Ministerio de Asuntos Exteriores de Estonia, GLOBSEC y el Departamento federal de Asuntos Exteriores de Suiza. Son simpatizantes: Packet Clearing House, UNIDIR, Black Hat USA, la Universidad de Tel Aviv, la Delegación de la UE en NU en Ginebra y DEF CON. Véase: https://cyberstability.org/

213 Esta es también una iniciativa de multipartenariado pero limitada a Internet. Fue creada en 2014 con un mandato de dos años por el Centre for International Governance de Canadá y la Chatham House del Reino Unido. La Comisión estuvo constituida por 25 miembros de diferentes orígenes geográficos y profesionales y en 2016 presentó su informe final: GCIG, *One Internet*, CIGI/Chatham House, Waterloo/Londres, 2016. https://www.cigionline.org/publications/one-internet

214 CGSC, SingaporeNormPackage, CGCS, La haya/Nueva York, 2018, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf

ración en el ciberespacio para mejorar las cibercapacidades, y discutir y crear normas para una conducta responsable. Desde su creación hasta la actualidad la asistencia a las conferencias ha ido aumentando exponencialmente así como también se han diversificado los países de origen de los asistentes.[215]La primera conferencia tuvo lugar en Londres y estableció 7 principios: 1) proporcionalidad: los gobiernos deben actuar en el cibercespacio en base al principio de proporcionalidad y de acuerdo al Derecho interno e internacional; 2) acceso al ciberespacio: cualquiera debe tener la posibilidad –en términos de habilidades, tecnología, confianza y oportunidad– de acceder al ciberespacio; 3) tolerancia y el respeto a la diversidad lingüística, cultural e ideológica; 4) mantenimiento de Internet como un espacio abierto a la innovación, a la libre circulación de ideas e información y a la libertad de expresión; 5) respeto a los derechos individuales de privacidad y de protección de la propiedad intelectual; 6) cooperación colectiva para hacer frente a las amenazas de los cibercriminales; 7) promoción de un entorno competitivo que garantice un retorno justo de las inversiones, servicios y contenidos vertidos en la red.[216] La segunda conferencia tuvo lugar en Budapest en 2012 y se centró en la relación entre derechos y seguridad en Internet. La tercera edición tuvo lugar en 2013, en Seúl y el tema de reflexión fue cómo conseguir un ciberespacio a la vez seguro y abierto. Los participantes coincidieron en que solo la cooperación de gobiernos e industrias podría asegurar a los ciudadanos el disfrute de los beneficios del ciberespacio, al tiempo que reconocían las diferentes responsabilidades y tareas de cada uno: mientras que los gobiernos son responsables de la adopción de políticas, estrategias y de la regulación para el desarrollo de la ciberseguridad, la industria es la fuente de la tecnología puntera, experiencia técnica, experiencia en despliegue y operativa y, en muchos países, propietaria de los componentes fundamentales de la infraestructura técnica.[217] La cuarta conferencia se celebró en 2015 en la Haya y en ella se decidió la creación de un mecanismo institucional, el Global Forum on Cyber Expertise, para ayudar a la construcción de capacidades. La quinta tuvo lugar en Delhi en 2017 bajo el lema de un Ciberespacio inclusivo y focalizó los debates sobre las políticas públicas que permitan que el ciberespacio sea un espacio de inclusión, sostenibilidad, desarrollo, seguridad y libertad.[218]

---

215 Se ha pasado de 700 participantes de 60 países a 1800 de más de 100 países. https://www.internetsociety.org/events/gccs-2017/

216 London Conference on Cyberspace: Chair' statement. https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement

217 "Moving Forward Together: Recommended Industry and Government Approaches for the Continued Growth and Security of Cyberspace " https://www.itic.org/dotAsset/9/d/9ded1e6-0281-4c19-84c5-00b8209b7bea.pdf.

218 https://www.internetsociety.org/events/gccs-2017/

c) Foro Internacional de Equipos de Respuesta a Incidentes de Seguridad

Creada en 1990, es una organización de equipos de respuesta a incidentes informáticos[219] que reúnen a gobiernos, empresas y representantes del sector académico. En la actualidad son miembros 483 equipos.[220] Su misión, de carácter técnico, es compartir las respuestas más efectivas a los incidentes de ciberseguridad y favorecer la confianza y la comunicación entre sus miembros. A través de FIRST los miembros pueden acceder al conocimiento de las mejores prácticas e instrumentos para responder a los diferentes tipos de incidentes que se producen en el ciberespacio.

6. REFLEXIONES FINALES.

El análisis realizado nos permite concluir que, teniendo que enfrentarse a la existencia de sistemas de valores contrapuestos, a la diversidad de actores y a la novedad, rapidez y fluidez de los cambios, el ciberespacio es un entorno de desarrollo normativo efervescente y multidireccional. En ese entorno múltiple y complejo, no obstante, las cibernormas consolidadas hasta el momento tienden a proteger más los intereses nacionales que los intereses generales de la comunidad internacional. La consideración del ciberespacio como un quinto espacio territorial y su vinculación a la soberanía estatal, en lugar de ser considerado un Bien Público Global o un Recurso Común Global, confirmaría esta apreciación. El control de las TIC se convierte en ciberpoder y las TIC se pueden convertir en ciberarmas. Las hostilidades y los conflictos armados se transforman y adquieren nuevas formas. Las transformaciones de la mano de las TIC acontecen a una velocidad vertiginosa. La regulación intenta adaptarse y responder a estas transformaciones pero el proceso es necesariamente mucho más lento. No obstante, hay que entenderlo como parte de la solución.

El cosmopolitismo blando, *Wordfalia*, no se ha impuesto a *Westphalia*. La tensión cosmopolita se ha resuelto, de momento a favor de este último modelo. Los intentos de crear una cultura mundial del ciberespacio no han funcionado. Hemos identificado diferentes actores con diferentes intereses y diferentes capacidades en el ámbito del ciberespacio y la ciberseguridad. Aquellos que defienden medidas de carácter cosmopolita son menos poderosos que aquellos que defienden objetivos de seguridad.

Aunque el ciberespacio es un espacio plural y los actores privados participen cada vez más activamente en los procesos regulatorios, estos están controlados

219 Es más conocida por sus siglas en inglés: FIRST.
220 Véase: https://www.first.org/ /

por las autoridades estatales ya sean en su formato de regulación nacional, bilateral, regional o multilateral. La concepción de la seguridad en clave tradicional, nacional y no global, es el argumento que lo justifica. La regulación fragmentada, traducida en acuerdos bilaterales y regionales, se ha impuesto de momento a la regulación global.

Los instrumentos regulatorios más utilizados son las normas, instrumentos de *soft law,* con sus ventajas (flexibilidad, adaptabilidad, fácil adopción) y sus inconvenientes (no se traducen en obligaciones jurídicas vinculantes, no llevan contramedidas asociadas, sus disposiciones son poco precisas y su cumplimiento depende de la voluntad política).

El intenso debate normativo que se desarrolla tiene un significado en sí mismo y puede interpretarse como una oportunidad para poner de relieve la existencia de una dimensión pública del Derecho internacional y avanzar en su defensa y consolidación. Sin embargo, la resistencia estatal sigue siendo férrea en un contexto en el que a pesar de que los retos son globales, nadie lo duda, las transformaciones en la estructura del poder internacional llevan a los Estados a adoptar posiciones defensivas y poco cooperativas. El llamado retorno a la geopolítica no ayuda a avanzar en la creación de normas globales. El ciberespacio y la ciberseguridad demuestran la necesidad y a la vez imposibilidad de gobernanza global en un mundo en el multilateralismo está en crisis y los nacionalismos están en auge.

A pesar del triunfo de *Westfalia,* el cosmopolitismo –en su versión blanda o suave– está presente **e**n la definición y desarrollo de los procesos de construcción de normas globales. El espíritu *wordfaliano* es la base, al menos discursiva, de los procesos normativos actuales sobre ciberseguridad. Los procesos normativos globales existentes son plurales (participan múltiples actores de categorías diferentes) y abiertos (son procesos en curso cuya importancia es el mecanismo negociador y cooperativo en sí mismo), multidireccionales (se trabajan diferentes aspectos que se solapan) e híbridos (se combinan simultáneamente instrumentos normativos diferentes). El reto está en conseguir que no solo los intereses de los Estados ciberpoderosos influyan en la regulación del ciberespacio sino en que sean escuchados las voces e intereses de otros Estados y de los actores de la sociedad civil y que el ciberespacio pueda ser un espacio de libertad y una plataforma de desarrollo.

El camino será largo. Los procesos normativos en el ámbito de la ciberseguridad no son sencillos y sea cual sea el camino elegido para la creación de cibernormas, siempre será difícil.[221] Lo importante es que no se interrumpa y para que no se interrumpa son aconsejables algunas estrategias. Marta Finnemore y Duncan

---

221 FINNEMORE, M. y HOLLIS, D., *op. cit.,* nota 63, p. 469.

Hollis[222] destacan la importancia de elegir el encuadre normativo adecuado, es decir, de seleccionar bien los problemas en los que debe centrarse la atención del regulador. Dado que en la gestión del ciberespacio y la ciberseguridad existen múltiples problemas solapados o interrelacionados, es clave optar por un contexto de entre los múltiples existentes: el más urgente o el que tiene mayores posibilidades de ser regulado. Esta misma aproximación es compartida por Stewart Patrick y Joseph Nye.[223] El primero defiende la pertinencia de la "gobernanza global en partes" consistente en descomponer los problemas complejos en sus elementos integrantes y abordarlos separadamente. Josep Nye, tras analizar el panorama de las ciberactividades, concluye que la aproximación que mejor ha funcionado hasta el momento en el ciberespacio es la que ha tratado aisladamente cada tipo de actividad: el cibercrimen, la protección de datos, los estándares técnicos en Internet, etc. Marta Finnemore y Duncan Hollis también señalan la relevancia, de cara al éxito regulador, de vincular la ciberseguridad a temas más amplios. Es más sencillo obtener mayor atención y apoyo a la regulación cuando se relaciona con temas más evidentes y más sensibles para diversos grupos de actores. Por ejemplo, si se vincula el cibercrimen a sus efectos económicos se consiguen mejores respuestas que si se trata como un tema de seguridad o como un problema meramente penal. Otra estrategia para avanzar en la ciberegulación es tomar en consideración y utilizar a su favor la cuestión de la identidad. En lugar de perseguir la universalidad, intentar la cooperación normativa en una región, o en un sector, en los que los actores sean afines. Está demostrado que en la gobernanza de los problemas globales se impone cada vez más el multilateralismo *ligth*, propio del siglo XXI, basado en la existencia de grupos minilateralistas o mini-multilateralistasque pueden jugar un rol de creadores normativos determinante. Los resultados obtenidos, una vez consolidados, pueden extenderse a otros grupos de actores o a otro sector. Regular bilateralmente o regionalmente es más fácil y genera menores costes de transacción. Así, en el ámbito económico global, el formato G2 (Estados Unidos-China) se impone en ocasiones al G20 y el G20 a las instituciones financieras multilaterales tradicionales. En el ámbito del ciberespacio, el bilateralismo China-Estados Unidos ha funcionado en la prohibición del ciberespionaje con fines lucrativos industriales y comerciales. En la misma dirección China y Rusia han firmado un acuerdo bilateral en el ámbito de la seguridad internacional de la información.[224] Estas "islas de normatividad" en un futuro

222 *Ibíd.,* pp. 465-476.

223 PATRICK, S., *op. cit* nota 207; NYE, J., "The Regime Complex for Managing Cyber Activities", *Global Comission on Internet Governances Paper Series,* núm. 1, 2014.

224 En 2015 Barak Obama y Xi Jinping alcanzaron un acuerdo bilateral, aunque posteriormente ambos países se han acusado mutuamente de violarlo. ROLLINS, J.W., "U.S.-China Cyber Agreement", *Congressional Research Service Insight*, 16 octubre 2015 (IN10376),https://www.hsdl.org/?abstract&did=788047. También en 2015, Xi Jinping y WladimirPutin firmaron lo que se puede considerar un pacto de no agresión en el ciberespacio. KORZAK, E.,

pueden producir el efecto de cascada normativa y extenderse a otros actores. Igualmente, es clave la selección de los elementos normativos. Aunque un tratado internacional multilateral o un régimen internacional específico del ciberespacio puede ser la opción teóricamente más deseable, también es la más difícil. Por lo mismo, puede ser aconsejable decantarse por opciones menos ambiciosas pero más realistas como seguir avanzando, por una parte, en la interpretación del Derecho internacional existente a fin de poder aplicarlo al ciberespacio y a la ciberseguridad; y, por otra en la creación de cibernormas voluntarias y no vinculantes pero que crean expectativas de conducta y que, en general, son respetadas por los actores que comparten una identidad. En esta dirección, las cibernormas basadas en las afinidades culturales grupales (especialmente las de sectores profesionales) son más sencillas de aplicar que las que se basan en otros criterios de corrección como la conformidad al Derecho internacional o interno, los compromisos políticos, o la costumbre. Cada ámbito tiene sus ventajas e inconvenientes: el jurídico internacional ofrece normas vinculantes pero que requieren de largos procesos negociadores y de procesos internos de ratificación; el jurídico interno tiene un límite geográfico; el político permite mayor flexibilidad y rapidez a cambio de un nivel menor de compromiso y de expectativas de cumplimiento menos intensas; la costumbre no exige negociaciones ni acuerdos a cambio de una mayor indeterminación; y las normas basadas en las culturas se dan por sentadas, pero se limitan a los grupos identificados con ellas. El desafío consiste en sacar provecho de las ventajas y minimizar las desventajas de cada modalidad. En relación al tipo de instrumentos normativos, también influye el grado de flexibilidad o rigidez con el que son descritas las conductas prohibidas o prescritas. Hasta el momento se han demostrado más efectivas las cibernormas flexibles ya que los ciberactores más importantes, los Estados, son muy reacios a ver limitada de forma rígida su soberanía. Un alto nivel de vinculación puede tener efectos contraproducentes. De la misma manera que los expertos afirman que en un mundo global deberemos acostumbrarnos a vivir con niveles de inseguridad hasta hace poco inaceptables, también en el ámbito normativo deberemos asumir la utilización, cada vez más importante, de instrumentos no jurídicos o de instrumentos de *soft law* menos garantistas. Otra estrategia a considerar es insertar el contexto institucional en el que se generan las normas y, por tanto, se prescriben las conductas, en contextos normativos más amplios (regímenes internacionales) ya que, por una parte, actuar dentro de contextos normativos existentes es más sencillo que crear un nuevo entorno normativo y, por otra, da mayor visibilidad a las nuevas normas. La articulación de contextos nuevos (un régimen especial para el ciberespacio) permitiría mayor funcionalidad pero las dificultades y costes serían mucho mayores. Finalmente, en cuanto a la generación de expectativas

---

"The Next Level for Russia-China Cyberspace Cooperation?, Council on Foreign Relations, https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation.

colectivas de conducta los emprendedores normativos en el ciberespacio buscan la completa internalización, aunque no siempre es realizable. Cuando no lo es, las normas teorizadas incompletamente pueden ser un buen compromiso en las situaciones en las que no existe consenso. Siempre son una mejor alternativa que la no existencia de normas. La selección de los instrumentos normativos debe ser, en definitiva, un compromiso entre incentivos, persuasión y socialización.