ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

101/2019 12 de noviembre de 2019

Margarita Robles Carrillo *

El régimen jurídico de las operaciones en el ciberespacio: estado del debate

El régimen jurídico de las operaciones en el ciberespacio: estado del debate

Resumen:

El régimen jurídico de las operaciones en el ciberespacio está siendo objeto de debate en el marco de Naciones Unidas desde finales de los años noventa. El análisis de ese proceso permite identificar dos etapas. La primera está caracterizada por la consecución de un cierto consenso entre los Estados sobre la aplicación de normas obligatorias, principios y reglas de comportamiento responsable y medidas de fomento de la confianza y capacitación. La segunda etapa ha supuesto la aparición de un preocupante disenso, principalmente, sobre el alcance de las normas obligatorias y el contenido de las reglas de comportamiento voluntario. Ello ha conducido al fracaso de las negociaciones, a la adopción de dos resoluciones diferentes y al establecimiento de dos grupos de trabajo para la reactivación de un diálogo que resulta cada más más difícil.

Palabras clave:

Derecho internacional, ciberespacio, operaciones.

* Este trabajo se realiza en el marco del Proyecto TIN2017-83494-R.

The legal regime of operations in the cyber-space: The status of the debate

Abstract:

The legal regime of operations in cyberspace has been under discussion at the United Nations since the late 1990s. There are two stages in this process. The first is characterized by the achievement of a certain consensus among States on the implementation of mandatory regulations, principles and rules of responsible behaviour and measures for confidence-building and training. The second stage has resulted in a worrying dissent, mainly on the scope of mandatory standards and the content of voluntary rules of behaviour. This has led to the failure of negotiations, the adoption of two different resolutions and the establishment of two working groups for the reactivation of dialogue that seems to be complicated.

Keywords:

International Law, cyberspace, operations.

Cómo citar este documento:

ROBLES CARILLO, Margarita. *El régimen jurídico de las operaciones en el ciberespacio: estado del debate*. Documento de Opinión IEEE 101/2019. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Introducción

El régimen jurídico de las operaciones en el ciberespacio constituye, desde hace tiempo, el objeto de un amplio y controvertido debate en el plano internacional y estatal. Mientras que el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) muestra un crecimiento exponencial constante, no parece haber avances en la regulación de las actividades y operaciones en el ciberespacio en el contexto y desde la perspectiva de la seguridad internacional.

El modelo de seguridad colectiva formalizado en 1945 en la Carta de Naciones Unidas establece el marco jurídico fundamental que ha permitido desde entonces garantizar la paz y la seguridad internacional. Junto con ello, el Derecho Internacional de los Conflictos Armados (DICA) ha servido para ordenar y humanizar, en la medida de lo posible, la conducta de las hostilidades. Con sus carencias y limitaciones, que no son pocas, esas normas conocidas como el *Ius ad Bellum* y el *Ius in Bello* han cumplido su función previniendo y evitando las situaciones de conflicto y ordenando su desarrollo, cuando finalmente se han producido, a pesar del amplio periodo de tiempo transcurrido desde su adopción y de los significativos cambios políticos y sociales acontecidos desde entonces.

La aparición y el desarrollo del ciberespacio y de las TIC suponen, sin embargo, un punto de inflexión en esa dinámica continuista y un desafío sin precedentes. Más allá de constituir un quinto dominio[1], alteran esencialmente los parámetros de organización y funcionamiento de ese modelo de seguridad, en particular, desde una triple perspectiva: la deslocalización y diversificación de las amenazas, la ruptura del paradigma de la asimetría entre los actores y una alteración substancial de los términos del conflicto[2]. Este cambio de circunstancias, que no es meramente coyuntural, obliga a plantearse la operatividad del marco jurídico en vigor.

En la doctrina, Moses identifica cuatro razones concretas que justifican la necesidad de cambios jurídicos como respuesta a los cambios tecnológicos: 1) La incertidumbre

[1] La idea de que el ciberespacio constituye el quinto dominio, que se suma a tierra, mar, aire y espacio exterior, es generalmente aceptada en la práctica estatal, institucional y doctrinal. Puede verse una opinión distinta, minoritaria, en DELEREU, Francois, "Reinterpretation or Contestation of International Law in Cyberespace", *Israel Law Review*, vol. 53, nº 3, 2019, 302-303.

[2] Sobre este cambio de paradigma puede verse ROBLES CARRILLO, Margarita, "Amenaza y uso de la fuerza a través del ciberespacio"," *Revista Latinoamericana de Derecho Internacional*, nº 4, 2016, 1-62.

jurídica sobre la manera de aplicar el derecho en vigor en esa situación; 2) El alcance incorrecto de la normativa porque fue creada con anterioridad, de manera que puede incluir o excluir inadecuadamente conductas o situaciones; 3) La obsolescencia jurídica porque, en ese contexto, la norma no es necesaria o no está justificada; y 4) La necesidad de crear nuevas normas específicas para regular, gestionar o prohibir determinadas técnicas o aplicaciones[3]. Todas y cada una de estas posibilidades se manifiestan en la articulación del régimen jurídico de las operaciones en el ciberespacio.

Desde la década de los noventa, la Asamblea General de Naciones Unidas (AGNU) centraliza el debate en el marco universal a través de la Comisión de Desarme y Seguridad Internacional. Los trabajos se desarrollan mediante dos procedimientos principales: la presentación de observaciones y propuestas individuales o conjuntas por parte de los Estados y los informes realizados en el marco de los Grupos de Expertos Gubernamentales (GEG). El análisis de ese proceso permite identificar dos etapas. En una primera se va construyendo progresivamente un consenso que se materializa en los informes de los GEG de 2013 y 2015. A pesar de las expectativas generadas por esos resultados, el disenso marca el desarrollo de los trabajos posteriores provocando en 2017 el fracaso de las conversaciones en el GEG constituido en 2016 y la adopción de dos resoluciones diferentes en 2018 que cambian los métodos de trabajo. El análisis del estado de debate pretende determinar dónde se encuentra el desacuerdo y las posibilidades de reactivación de un cierto consenso a nivel internacional sobre el régimen jurídico de las operaciones en el ciberespacio.

La construcción progresiva de un consenso

La AGNU viene trabajando sobre la relación entre las TIC y la seguridad internacional desde hace varias décadas, sobre varios aspectos y con diversos formatos. Desde 1998, el núcleo de este debate se desarrolla en el marco de los trabajos sobre los *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*[4]. En ese contexto se plantea la propuesta de crear los llamados GEG con la misión de examinar las amenazas existentes y potenciales en materia de seguridad

[3] MOSES, Lyria B., "Why Have a Theory of Law and Technological Change?" *Minnesota Journal of Law, Science & Technology,* vol. 8, 2007, 594-595.

[4] A/RES/53/70, de 4 de enero de 1999.

de la información, así como las posibles vías de colaboración para hacer frente a las mismas. En realidad, los GEG han desarrollado una función más extensa y compleja porque se han convertido en el foro institucional de alcance universal donde se analiza el conjunto de la normativa internacional aplicable en materia de seguridad internacional.

Como cabía esperar, el proceso no ha sido fácil. El primer GEG, en 2004, es también un primer fracaso. El segundo, en 2010, se limita a identificar algunos riesgos, amenazas y vulnerabilidades[5]. El tercero, en 2013, concluye con un escueto informe, pero afirma el principio de soberanía y la jurisdicción de los Estados sobre las infraestructuras TIC situadas en su territorio[6]. El informe del GEG de 2015 constituye la primera aportación consensuada de alcance global sobre el régimen aplicable a las actividades y operaciones en el ciberespacio. Este informe traduce un acuerdo incipiente, básico, sobre dicha regulación sobre la base de cuatro categorías jurídicas[7]: a) Normativa internacional obligatoria; b) Normas, reglas y principios de comportamiento responsable; c) Medidas de fomento de la confianza; y d) Medidas de cooperación y asistencia internacionales. Mientras las dos últimas tienen un contenido operativo, administrativo o meramente técnico, las dos primeras establecen los contenidos principales del régimen jurídico de las actividades y operaciones en el ciberespacio en los siguientes términos:

a) La normativa de derecho internacional «aplicable obligatoriamente» al uso de las TIC incluye los principios de igualdad soberana, solución pacífica de controversias, prohibición del uso y de la amenaza de la fuerza, no intervención en los asuntos internos de otros Estados y respeto de los derechos humanos, así como los principios de humanidad, necesidad, proporcionalidad y distinción, dentro del DICA.

El problema que se plantea en este punto es doble. Por una parte, prácticamente en su totalidad, esas disposiciones son aplicables obligatoriamente al ciberespacio porque se trata de normas de naturaleza imperativa, no dispositiva, que los Estados están obligados a respetar con independencia del medio, físico o virtual, en el que operen. Por otra parte, el informe se limita a confirmar la obligatoriedad de esas normas en el marco del ciberespacio, pero no aborda la problemática específica que plantea su aplicación concreta respecto de las actividades y operaciones realizadas en ese ámbito que es,

[5] A/65/201, de 30 de julio de 2010.
[6] A/68/98, de 24 de junio de 2013.
[7] A/70/174, de 22 de julio de 2015.

realmente, el asunto que hay que resolver. No se ocupa, por ejemplo, de analizar el principio de soberanía en el ciberespacio, a pesar de ser un concepto vinculado a la existencia de un poder político con una base territorial que no resulta igualmente gestionable en el contexto virtual. No aborda el problema de aplicar el principio de prohibición del uso o de la amenaza de la fuerza en el ciberespacio, ni siquiera qué se entiende por arma, ataque o fuerza cibernética. No avanza en la determinación de las modalidades de aplicación de los principios de distinción o proporcionalidad en un conflicto armado cuando un medio como el ciberespacio difícilmente se presta a criterios de esa naturaleza creados para el entorno físico. En definitiva, confirmar su obligatoriedad, cuando ya son obligatorias, no resuelve el verdadero problema que consiste en determinar sus modalidades de aplicación y garantizar su cumplimiento en el ciberespacio.

b) Las normas y principios de «comportamiento responsable» de los Estados son voluntarias y no vinculantes. Esta doble caracterización significa que los Estados se adhieren voluntariamente a estas normas, pero ello no implica que se conviertan en obligatorias para quienes se han adherido a las mismas. La precisión es importante porque, como es sabido, en derecho internacional, la regla básica es que una norma solo es obligatoria respecto de un Estado cuando este ha prestado el consentimiento para obligarse por la misma. En este caso, la aceptación de la norma no supone su conversión en obligatoria, esto es, no genera obligaciones y no resulta exigible jurídicamente su respeto por parte del Estado en cuestión. El consenso alcanzado sobre este conjunto de normas, reglas y principios de comportamiento responsable de los Estados debe ser valorado, en cuanto a su alcance y naturaleza, teniendo presente que no solo es voluntaria la aceptación de este, sino que dicha aceptación no genera obligaciones exigibles jurídicamente.

La naturaleza de este conjunto de disposiciones se confirma en el informe del GEG cuando identifica sus tres elementos distintivos: 1) No tratan de limitar ni prohibir acciones que, siempre según el informe, son compatibles con el derecho internacional; 2) Reflejan las expectativas de la comunidad internacional y establecen criterios para un comportamiento responsable de los países; y 3) Permiten a la comunidad internacional evaluar sus intenciones y actividades. El problema principal que se plantea en este punto radica en que, atendiendo al contenido de esas normas, no todas y cada una de ellas pueden considerarse voluntarias, a pesar de ser definidas como tales.

El informe del GEG relaciona en torno a una decena de normas y reglas sobre distintos aspectos del uso de las TIC, desde atender solicitudes de información o cooperar y prestarse asistencia mutua hasta alentar la divulgación responsable de vulnerabilidades relacionadas con las TIC. El caso es que algunas de esas disposiciones no pueden ser calificadas como voluntarias porque constituyen, por sí mismas, obligaciones jurídicas. El caso paradigmático se encuentra en la afirmación de que un Estado «no debería realizar ni apoyar de forma deliberada actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional». No es, ni puede ser, una regla voluntaria de comportamiento, como se califica en el informe del GEG de 2015. Cumplir las obligaciones internacionales es, por definición, en sí misma, una obligación, por lo que situarlo en el terreno de las normas y reglas voluntarias constituye algo más que un despropósito en términos jurídicos, incluso, un retroceso.

A pesar de sus aspectos jurídicamente cuestionables, este informe recibe el beneplácito de la AGNU[8] y la aceptación generalizada de sus países miembros[9], impulsando la convocatoria de un nuevo GEG en 2016. Pero, en este caso, el resultado de sus trabajos pone de manifiesto el disenso de fondo existente entre los Estados.

El alcance y contenido del disenso

El disenso entre los Estados sobre el régimen jurídico de las actividades y operaciones en el ciberespacio se manifiesta en los trabajos de la AGNU, pero también en la formulación de propuestas y políticas nacionales.

[8] A/RES/71/28, de 9 de diciembre de 2016.

[9] A/70/174, de 22 de julio de 2015.

Los trabajos en el marco de la AGNU

En 2017, los trabajos del GEG terminan sin acuerdo[10]. Un año después, en el Informe de la Comisión de Desarme y Seguridad Internacional de 19 de noviembre de 2018[11] se plantean dos propuestas: por una parte, el proyecto de resolución titulado *Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional*, presentado el 18 de octubre por el representante de EE. UU. con el apoyo de 36 países, incluidos todos los miembros de la UE, además de Australia, Canadá, Georgia, Israel, Japón, Malawi y Ucrania, al que se suman posteriormente 15 países más, que resulta aprobado con 139 votos a favor, 11 en contra y 18 abstenciones; y, por otra parte, el proyecto de resolución titulado *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, presentado el 8 de noviembre por la Federación de Rusia en nombre de 31 países, a los que se suman después otros 3, y que recibe 109 votos a favor, 45 en contra y 16 abstenciones.

La denominación utilizada para designar cada propuesta no debe llevar a confusión. Este segundo proyecto se centra realmente en las reglas, normas y principios de comportamiento responsable. En cambio, aunque lleva ese título, el primer proyecto se dedica principalmente a apoyar el seguimiento y la aplicación de los informes de los GEG y la constitución de un nuevo GEG en 2019. En realidad, paradójicamente, la propuesta rusa sobre los avances en la esfera de las TIC se centra en las normas de comportamiento responsable, mientras que la propuesta estadounidense sobre comportamiento responsable mantiene la dinámica y los contenidos de las resoluciones previas sobre los avances en la esfera de las TIC. Más allá del desconcierto lógico que provoca este uso ambivalente de la terminología, el disenso interestatal se traduce finalmente en la aprobación de dos textos por parte de la AGNU.

Avances en la esfera de las TIC en el contexto de la seguridad internacional

La Resolución de la AGNU de 5 de diciembre de 2018 sobre *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional* reproduce el proyecto liderado por Rusia aprobado en la Comisión de Desarme y

[10] A/72/327, de 14 de agosto de 2017. Sobre los motivos del fracaso puede verse DELEREU, Francios., *opus citatum*, 305 y ss.

[11] A/73/505, de 19 de noviembre de 2018.

Seguridad Internacional[12]. Desde el punto de vista de sus contenidos, cabe destacar tres aspectos: el acervo normativo del preámbulo (A) y la parte dispositiva sobre comportamiento responsable de los Estados que agrupa contenidos diversos puesto que incluye algunas obligaciones jurídicas (B) junto con principios o reglas de comportamiento no vinculantes (C).

A) Asumiendo el acervo existente en la materia, la resolución confirma las conclusiones de los trabajos de los GEG en 2013 y 2015 en el sentido de que el derecho internacional y, en particular, la Carta de Naciones Unidas, son aplicables y fundamentales para garantizar la paz y la seguridad en el ciberespacio[13]. La soberanía y los principios que de ella derivan son objeto de una mención específica que justifica el ejercicio de la jurisdicción sobre las infraestructuras situadas en el territorio del Estado.

En ese mismo contexto, antes de entrar en la parte dispositiva, se reafirma el derecho y el deber de los Estados de combatir, en el marco de sus prerrogativas constitucionales, la difusión de noticias falsas o distorsionadas que puedan interpretarse como una injerencia en los asuntos internos o perjudicar la promoción de la paz o la cooperación internacional. Ese compromiso se completa con otro consistente en el deber de todo Estado de abstenerse de toda campaña de difamación, vilipendio o propaganda hostil que pueda dirigirse a o suponer una injerencia en los asuntos internos. El hecho de que estas normas no formen parte del contenido dispositivo de la resolución pone de manifiesto el desacuerdo existente en cuanto a la calificación y el marco normativo aplicable a las actividades de desinformación. Posiblemente, esta disposición se encuentra entre los motivos que explican el voto en contra por parte de un buen número de países entre los que se cuentan EE. UU. y los miembros de la UE.

[12] A/RES/73/27, de 11 de diciembre de 2018. La resolución es aprobada por 119 votos a favor, 14 abstenciones y 46 votos en contra que corresponden a Albania, Andorra, Australia, Austria, Bélgica, Bulgaria, Canadá, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Georgia, Alemania, Grecia, Hungría, Islandia, Irlanda, Israel, Italia, Japón, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Islas Marshall, Mónaco, Montenegro, Países Bajos, Nueva Zelandia, Noruega, Polonia, Portugal, Rumania, San Marino, Eslovaquia, Eslovenia, España, Suecia, ex República Yugoslava de Macedonia, Ucrania, Reino Unido de Gran Bretaña e Irlanda del Norte y Estados Unidos de América. Disponible en: https://undocs.org/es/A/73/PV.45

[13] La intervención del representante de la Federación Rusa para explicar el fracaso del GEE de 2017 no acaba de encajar con esta afirmación. Disponible en: http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288.

B) En la parte dispositiva de la resolución es posible identificar una serie de obligaciones que, injustificadamente, son calificadas como normas voluntarias o directamente reinterpretadas en su formulación. Entre ellas se encuentran las siguientes: a) Cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos; b) No permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando las TIC; y c) No realizar ni apoyar a sabiendas actividades en la esfera de las TIC contrarias a las obligaciones que les incumben en virtud del derecho internacional.

C) Los principios y reglas de conducta voluntaria incluyen la cooperación en distintos ámbitos entre los que destacan la formulación y aplicación de medidas para aumentar la estabilidad y seguridad en el uso de las TIC o el intercambio de información y la asistencia mutua. También se establecen reglas de conducta individual como la protección de las infraestructuras fundamentales o la adopción de medidas para garantizar la integridad de la cadena de suministro o para evitar la proliferación de técnicas o instrumentos maliciosos.

La lectura de esta resolución permite llegar a tres conclusiones principales : a) Algunos de sus contenidos trasladan obligaciones jurídicas que no pueden, ni deben, ser identificadas como reglas voluntarias de comportamiento responsable; b) La mayoría de esas reglas se explica en el texto de la resolución atribuyéndole un alcance y significado que no necesariamente se corresponde con el contenido natural y preciso de la regla en cuestión, como ocurre, en particular, cuando se precisan las modalidades de atribución de autoría o responsabilidad[14]; y c) La inclusión de la desinformación, en términos de injerencia en los asuntos internos y estableciendo deberes a cargo de los Estados, constituye un punto principal de desacuerdo capaz de justificar el rechazo a esta resolución por parte de un gran número de países.

Por otra parte, la principal aportación institucional de esta resolución es la decisión de crear un grupo de trabajo de composición abierta (Open Ended Working Group, OEWG) que actuará por consenso y en el que se contempla la posibilidad de participación de partes interesadas distintas de los Estados.

[14] Resulta interesante, a este respecto, la lectura de la explicación dada por el experto estadounidense a propósito del fracaso de 2017. Disponible en: https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/.

Promoción del comportamiento responsable de los Estados en el ciberespacio

Mucho más breve y expeditiva en su formulación, la Resolución de la AGNU de 22 de diciembre de 2018 sobre *Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional*—que responde a la propuesta encabezada por EE. UU.— exhorta a los Estados miembros a guiarse por los informes de los GEG y solicita la convocatoria de un nuevo GEG organizado sobre la base de una distribución geográfica equitativa[15].

Esta resolución, como la anterior, incluye en sus considerandos referencias a la normativa de derecho internacional aplicable obligatoriamente en el ciberespacio, en particular, la Carta de Naciones Unidas. Pero, a diferencia de la resolución promovida por la Federación Rusa, no menciona expresamente la soberanía de los Estados y los principios y normas que de ella se derivan. Tampoco se avanza en la definición de las modalidades de aplicación de esas normas obligatorias al ciberespacio. No hay mención alguna al problema de la desinformación como modalidad de injerencia política.

En definitiva, en el marco de la AGNU, el desacuerdo se ha materializado, normativamente, en la adopción de dos resoluciones distintas y, funcionalmente, en la creación de un GEG y un OEWG, trasladando dos concepciones diferentes del régimen jurídico de las actividades en el ciberespacio. Esa situación ha propiciado la presentación de propuestas de distinto signo, colectivas e individuales, por parte de los Estados.

Las propuestas estatales

Mientras se desarrolla el debate en el marco de la AGNU, con sus avances y retrocesos, las posiciones de los Estados se han ido manifestando mediante propuestas conjuntas o acciones individuales en foros institucionales o no gubernamentales. Hay algunas aportaciones especialmente destacables.

En 2011, un grupo de países liderado por Rusia y China presentaba una propuesta de código internacional de conducta para la seguridad de la información con el propósito de determinar los derechos y responsabilidades de los Estados en el marco del

[15] A/RES/73/266, de 2 de enero de 2019. La resolución es aprobada por 138 votos a favor, 16 abstenciones y 12 en contra que corresponde a Bolivia, China, Comoras, Cuba, República Popular Democrática de Corea, Egipto, Irán, Nicaragua, Federación de Rusia, República Árabe Siria, Venezuela y Zimbabue. Disponible en: https://undocs.org/es/A/73/PV.65

ciberespacio[16]. En 2015, proponían un código revisado, abierto a la adhesión de todos los Estados y de carácter voluntario[17]. En el marco de la Organización de Cooperación de Shangai (OCS), de la que forman parte los países promotores de esas iniciativas, se concluye, en 2009, el Convenio sobre Cooperación en el ámbito de la Seguridad Internacional de la Información que entró en vigor en 2011[18]. En la Declaración de Xiamen, de 5 de septiembre de 2017, se hace un reconocimiento expreso de los principios de derecho internacional incluidos en la Carta de Naciones Unidas, pero mencionando la soberanía, la independencia política, la integridad territorial, la no injerencia en los asuntos internos y el respeto de los derechos y libertades fundamentales[19]. No hay referencia a la prohibición del uso o amenaza de la fuerza o al arreglo pacífico de las controversias, que son los temas prioritarios para el grupo de países que apoya la resolución propuesta por EE. UU. En la Declaración de Bishkek del Consejo de jefes de Estado de la OCS, de 14 de junio de 2019, se afirma que los Estados miembros lucharán contra el uso de las TIC para socavar la seguridad política, económica y pública en los países de la OCS. Como cabía esperar, solo se menciona la Resolución de la AGNU de 5 de diciembre de 2018 y se avanzan dos líneas de cooperación. Por un lado, promover la elaboración de reglas, principios y normas universales de comportamiento responsable; y, por otro, cooperar activamente para garantizar la seguridad de la información en el espacio de la OCS[20].

El problema de esta cooperación regional es doble. Por una parte, jurídicamente, debe situarse dentro de los límites que impone el sistema de Naciones Unidas. Aunque se admite la actuación de organismos regionales, la responsabilidad principal en materia de paz y seguridad internacional corresponde a la ONU. Garantizar la seguridad de la información en el espacio OCS, cuando el concepto mismo de «seguridad de la información» resulta polémico[21], no es un propósito fácil y automáticamente subsumible dentro del modelo de seguridad colectiva de la Carta. No parece que el Consejo de Seguridad, máximo responsable en materia de seguridad internacional, pueda llegar a

[16] A/ 66/359, de 14 de septiembre de 2011.

[17] A/ 69/723, de 13 de enero de 2015.

[18] Disponible en: http://cis-legislation.com/document.fwx?rgn=28340

[19] Disponible en: http://www.bricschn.org/English/2017-09/05/c_136583711_2.htm

[20] Disponible en: http://eng.sectsco.org/documents/

[21] El Reino Unido insiste en el uso del término «ciberseguridad» (A/72/315, de 11 de agosto de 2017, p. 25), mientras que los países de la OCS se refieren siempre a “seguridad de la información”.

acuerdos sobre este tema cuando las posiciones de China y Rusia y el resto de los miembros permanentes con derecho a veto son tan opuestas. Por otra parte, políticamente, la situación es también complicada. La OCS se ha convertido en la organización en la que encuentran apoyo institucional las políticas desarrolladas por la Federación Rusa y China. Al vincular y fortalecer la posición de ambos países, la actividad de la OCS puede limitar las posibilidades de cooperación dentro de la OSCE, que estaba llamada a ser la estructura de generación de confianza sobre el régimen jurídico del ciberespacio entre la Federación Rusa y el resto de sus países miembros. La combinación ruso-china, institucionalizada y fortalecida en la OCS, no solo debilita las posibilidades de alcanzar un acuerdo dentro de la OSCE, sino que sacraliza la presencia de dos bloques opuestos en el Consejo de Seguridad sobre las actividades en el ciberespacio desde la perspectiva de la seguridad internacional.

EE. UU., Australia, Canadá y los Estados miembros de la UE, entre los que se encuentran Francia y Gran Bretaña, miembros permanentes del Consejo de Seguridad, mantienen una concepción distinta a la ruso-china que se ha manifestado en distintos ámbitos y organizaciones. El G-7 ha sido un foro especialmente activo. En la reunión de Ise-Shima de 26 y 27 de mayo de 2016, adopta los denominados G7 Principles and Actions on Cyber[22]. Entre ellos hay que destacar tres elementos: 1) La afirmación de que el derecho internacional, incluida la Carta de Naciones Unidas, es aplicable en el ciberespacio; 2) La defensa de un marco jurídico basado en el tríptico formado por la aplicabilidad del derecho en vigor, la promoción de normas voluntarias de comportamiento y el desarrollo de medidas de confianza; y 3) El reconocimiento de que, en determinadas circunstancias, las actividades cibernéticas pueden constituir un uso de la fuerza o un ataque armado en el sentido de la Carta de Naciones Unidas y del derecho consuetudinario. En caso de ataque armado, podría invocarse el derecho a la legítima defensa de conformidad con el art. 51 de la Carta y la normativa internacional, incluido el derecho internacional humanitario. No se hace referencia, en cambio, a la respuesta en caso de uso de la fuerza.

La Declaración del G7 sobre el comportamiento responsable de los Estados en el ciberespacio, adoptada en Lucca, el 11 de abril de 2017, reitera los compromisos adoptados con anterioridad y apoya los trabajos de los GEG. En este caso, se dedica

[22] Disponible en: https://www.mofa.go.jp/files/000160279.pdf

una atención especial al asunto de la responsabilidad por hechos ilícitos en el ciberespacio desde una doble perspectiva. Por una parte, se reconoce que el marco jurídico internacional de la responsabilidad permitiría la adopción de contramedidas frente al Estado responsable de hechos ilícitos con objeto de restablecer la legalidad garantizando el cumplimiento de sus obligaciones. Por otra parte, respecto del delicado asunto de la atribución, se afirma que «the customary international law of State responsibility supplies the standards for attributing acts to States, which can be applicable to activities in cyberspace». Ello implica reconocer que un Estado «is free to make its own determination in accordance with international law with respect to attribution of a cyber-act to another State»[23].

La Declaración Política de Punta Cana, adoptada en la V Cumbre de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC), el 25 de enero de 2017, insiste en la necesidad de garantizar el uso pacífico de las TIC y de evitar y abstenerse de realizar actos unilaterales que no sean compatibles con la Carta de las Naciones Unidas, la Declaración Universal de los Derechos Humanos y el Derecho Internacional, tales como aquellas que tienen como objetivo subvertir sociedades o crear situaciones con el potencial de fomentar conflictos entre Estados[24].

En noviembre de 2018, durante la reunión del Foro sobre la Gobernanza de Internet, se publica el llamado *Appel de Paris pour la confiance et la sécurité dans le cyberespace* donde se afirma nuevamente la aplicación a las TIC del derecho internacional, convencional y consuetudinario en su integridad porque este ordenamiento constituye, junto con las normas de comportamiento responsable de los Estados y las medidas de confianza y de desarrollo de capacidades elaboradas en el marco de Naciones Unidas, el fundamento de la paz y la seguridad internacional en el ciberespacio[25]. Las propuestas concretas, sin embargo, no suponen un avance significativo respecto de los trabajos de Naciones Unidas porque se centran, en lugar de en la aplicación de aquel régimen jurídico, en aspectos menores de carácter técnico.

[23] Disponible en: https://www.mofa.go.jp/files/000246367.pdf

[24] Disponible en: http://www.sela.org/es/prensa/notas-de-prensa/2017/01/declaracion-política-de-punta-cana-v-cumbre-celac/

[25] Disponible en: https://www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf

A finales de septiembre de 2019 se ha hecho público el *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, promovido por EE. UU. y avalado originalmente por 26 de los países que impulsaron la resolución presentada con esa denominación en la AGNU. En esta declaración se afirma, como en los demás casos, que el marco jurídico de las operaciones en el ciberespacio está formado por las normas obligatorias de derecho internacional, la adhesión a normas voluntarias de comportamiento responsable en tiempos de paz y el desarrollo y aplicación de medidas de fomento de la confianza para reducir el riesgo de conflictos provocados por ciberincidentes. Se reconoce, asimismo, el compromiso con los trabajos del GEG y el OEWG. La defensa de un ciberespacio libre, abierto y seguro se acompaña de una advertencia: en caso de necesidad, «we will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law. There must be consequences for bad behavior in cyberspace. We call on all states to support the evolving framework and to join with us to ensure greater accountability and stability in cyberspace»[26].

Muchos Estados se están pronunciando sobre el asunto, en particular, en las observaciones presentadas a la AGNU a través de los informes del SGNU. Analizando los últimos informes del SGNU, existe un grupo de países que merece especial atención porque, con unos u otros argumentos, defienden la necesidad de centrarse en las modalidades concretas de aplicación de la normativa internacional al ciberespacio. Es el caso de Australia[27], Alemania[28], Colombia[29], Estonia[30], India[31], Japón[32], Noruega[33], Singapur[34] y España[35]. Hay otro grupo de Estados para los que la guerra de la información es el problema principal, entre los que se encuentran, además de China y

[26] Disponible en: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

[27] A/71/172, de 19 de julio de 2016, p. 5.

[28] A/72/315, de 11 de agosto de 2017, p. 5.

[29] A/71/172, de 19 de julio de 2016, p. 8.

[30] A/72/315, de 11 de agosto de 2017, p. 13.

[31] A/71/172, de 19 de julio de 2016, p. 13.

[32] A/72/315, de 11 de agosto de 2017, p. 16 y A/71/172, de 19 de julio de 2016, p. 14.

[33] A/72/315, de 11 de agosto de 2017, p. 27.

[34] A/72/315, de 11 de agosto de 2017, p. 27.

[35] A/71/172, de 19 de julio de 2016, p. 11.

Rusia, Armenia[36], Bielorrusia[37], Cuba[38] y Líbano[39]. Hay casos en los que se reconoce directamente el desarrollo de capacidades militares en el ámbito cibernético como hacen Canadá[40], Grecia[41] y Jordania[42]. Recientemente, en Francia, el Ministère des Armées ha publicado el informe *Droit international appliqué aux operations dans le cyberspace* que tiene como objetivo explicar la posición de Francia sobre la aplicación del derecho internacional a las operaciones en el ciberespacio[43]. Esa diversidad de políticas nacionales no parece facilitar la formación del necesario consenso internacional.

Conclusiones

El análisis de los trabajos sobre el régimen jurídico de las operaciones en el ciberespacio permite llegar a algunas conclusiones:

1) Existe acuerdo sobre la aplicación del derecho Internacional y, en particular, la Carta de Naciones Unidas al ciberespacio. Aunque no podría ser de otra manera, porque se trata de disposiciones obligatorias y algunas incluso imperativas, la apreciación de esas normas no es uniforme. Mientras que hay Estados que se están centrando en los aspectos relativos a la prohibición del uso o de la amenaza de la fuerza, en sus diversos aspectos, los países de la OCS rechazan ese debate priorizando la defensa del principio de no injerencia en los asuntos internos.

2) No existe consenso, ni se aprecian avances significativos en cuanto a la definición de las modalidades de aplicación de las normas obligatorias de derecho internacional a las actividades y operaciones en el ciberespacio. Aunque son muchos los países que están defendiendo la necesidad de abordar los aspectos concretos de la aplicación normativa, el desacuerdo sobre los principios está bloqueando este necesario desarrollo jurídico específico para las actividades y operaciones cibernéticas.

[36] A/72/315, de 11 de agosto de 2017, pp. 5-6.
[37] A/72/315, de 11 de agosto de 2017, pp. 7-8.
[38] A/72/315, de 11 de agosto de 2017, p. 11.
[39] A/71/172, de 19 de julio de 2016, p. 18.
[40] A/72/315, de 11 de agosto de 2017, p. 9.
[41] A/72/315, de 11 de agosto de 2017, pp. 14-16.
[42] A/72/315, de 11 de agosto de 2017, pp. 17-18.
[43] Ministère des Armées, *Droit international appliqué aux opérations dans le cyberspace*, Paris, 2019.

3) Existe acuerdo sobre la articulación de un régimen jurídico de las operaciones en el ciberespacio sobre la base del tríptico formado por normas obligatorias, normas de comportamiento responsable y medidas de fomento de confianza y de capacitación. El problema estriba en que la calificación dentro de cada una de esas categorías no es siempre correcta. Las llamadas reglas, normas o principios de comportamiento responsable son, en parte, una adulteración de las obligaciones asumidas con carácter general por los Estados en el marco del ordenamiento jurídico internacional y, en parte, un conjunto de compromisos de cooperación técnica o administrativa sin mayor trascendencia desde el punto de vista jurídico.

4) El disenso en el marco de la AGNU se manifiesta, normativamente, en la adopción de dos resoluciones distintas en 2018 y, funcional y orgánicamente, en la creación de dos estructuras y procedimientos de trabajo: un GEG y un OEWG. El acuerdo que suponía encauzar los debates a través de los GEG se ha quebrado porque, junto con el nuevo GEG, funcionará el OEWG. La eventual relación entre ellos y el alcance y naturaleza de sus propuestas son, por el momento, una incógnita. De acuerdo con la escasa información suministrada, ambos trabajan desde 2019 con vistas a presentar sus informes a la AGNU en 2020, en el caso del OEWG, y en 2022, el GEG, que está compuesto por 25 miembros siguiendo una distribución geográfica equitativa[44]. En una Resolución del 21 de octubre de 2019, la AGNU se limita a indicar que «los dos grupos son importantes mecanismos independientes de negociación bajo los auspicios de las Naciones Unidas, que deberían llevar a cabo su labor respectiva de manera constructiva y pragmática, sumando sus esfuerzos a los del otro»[45].

El desafío principal que plantea el régimen jurídico de las operaciones en el ciberespacio consiste en determinar cómo se aplican las normas obligatorias, cuáles han de ser las normas, reglas y principios voluntarios de comportamiento responsable de los Estados y cómo evitar que esta segunda categoría se utilice para desnaturalizar o desvirtuar el alcance de las normas contenidas en la primera condicionando, limitando o restringiendo el alcance de las obligaciones establecidas obligatoriamente en el ordenamiento jurídico internacional. La inclusión de un marco normativo voluntario en el diseño del régimen jurídico de las operaciones en el ciberespacio ha de tener la finalidad lógica y natural de

[44] Disponible en: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+and+GGE+processes+-+2.pdf

[45] A/C.1/74/L.50, de 21 de octubre de 2019.

posibilitar una adaptación progresiva y voluntaria a las normas nuevas o especiales que requiere la regulación de este espacio singular cuando no sean efectivas o suficientes las normas en vigor. No puede servir para excluir, eludir o reinterpretar las normas de naturaleza obligatoria.

El disenso existente entre los Estados es un problema no solo porque impide la adopción de acuerdos sobre el régimen jurídico de las actividades y operaciones en el ciberespacio sino, también, y no en menor medida, porque propicia la activación de políticas nacionales como reacción frente a la parálisis internacional. A su vez, el desarrollo de políticas nacionales, sobre la base de las concepciones propias de cada Estado y al margen de influencias externas, puede condicionar y obstaculizar en mayor grado la formación del necesario consenso internacional.

*Margarita Robles Carrillo**
Profesora titular de Derecho Internacional Público y Relaciones Internacionales
Grupo NESG-TIC233
Universidad de Granada