Revista Española de Derecho Internacional
Sección FORO
Vol. 69/2, julio-diciembre 2017, Madrid, pp. 291-299
http://dx.doi.org/10.17103/redi.69.2.2017.2.02

ISSN: 0034-9380; E-ISSN: 2387-1253

CIBERSEGURIDAD Y DERECHO INTERNACIONAL

Antonio Segura Serrano*

SUMARIO: 1. INTRODUCCIÓN.—2. EL CIBERESPACIO.—3. LA CIBERSEGURIDAD.—4. LA COOPERACIÓN INTERNACIONAL.—5. CONSIDERACIONES FINALES.

1. INTRODUCCIÓN

1. La aproximación más primigenia a la cuestión de la ciberseguridad por parte de la doctrina se ha producido desde el punto de vista de la seguridad colectiva. En este contexto, existe consenso sobre la aplicación, dificultosa en cualquier caso, de las reglas básicas relativas a la prohibición de la amenaza y el uso de la fuerza ya existentes en el ordenamiento internacional. No obstante, la ciberseguridad constituye una cuestión problemática que plantea diversos desafíos desde otras vertientes jurídico-internacionales. Tras unas precisiones jurídicas sobre el ciberespacio, el presente trabajo pretende analizar la ciberseguridad desde ese enfoque más holístico, incidiendo en los esfuerzos que se han desarrollado hasta el momento para una mayor cooperación en este sector.

2. EL CIBERESPACIO

2. Olvidadas ya las primeras reivindicaciones libertarias, sigue existiendo un cierto debate en cuanto a la naturaleza jurídica del ciberespacio. Por un lado están quienes lo consideran parte de los *global commons*, junto con un grupo variado de espacios internacionales[1]. No obstante, teniendo en cuenta que actualmente la infraestructura de Internet es tanto pública como

* El presente trabajo se ha realizado en el marco del Proyecto de Investigación «La estrategia de seguridad nacional de España: un enfoque geográfico» (REF. DER2014-57671-R), financiado por el Ministerio de Economía y Competitividad. Antonio Segura Serrano es profesor titular de Derecho internacional público y relaciones internacionales en la Universidad de Granada (*asegura@ugr.es*). Todas las páginas web de referencia han sido consultadas por última vez el 19 de mayo de 2017.

[1] US Department of Defense, *Strategy for Homeland Defense and Civil Support*, 2005, p. 12, accesible en *https://www.hsdl.org/?view&did=454976*; Government of Canada, *Canada's Cyber Security Strat-*

privada y que las normas que se le aplican son tanto nacionales como internacionales, algunos autores optan por el concepto de *commons* «imperfecto» o *pseudo-commons* [2]. Este tipo de caracterización apunta a que podría alcanzarse en un futuro un régimen jurídico claramente internacionalizado para los recursos básicos del ciberespacio, siguiendo los contornos del concepto de patrimonio común de la humanidad [3].

3. En cualquier caso, que un solo Estado no pueda someter globalmente a su jurisdicción la actividad que tiene lugar en el ciberespacio, de naturaleza transfronteriza en buena parte, no implica que no se esté ejerciendo jurisdicción estatal en el mismo a través de las tradicionales bases de competencia territorial y personal, e incluso de forma indirecta, lo que permite territorializar el ciberespacio [4]. Los Estados pueden ejercer su jurisdicción, y de hecho lo están haciendo, sobre la actividad cibernética que está orientada hacia un territorio determinado y tiene un efecto local, obviando el instrumento utilizado (Internet) [5]. De todos modos, el ejercicio de jurisdicción estatal puede facilitarse en el futuro si existe consenso internacional.

4. En el ámbito de la responsabilidad internacional, actualmente existen algunas dificultades de tipo técnico y jurídico. Por un lado, está el problema de la trazabilidad de la actividad cibernética (que puede atravesar distintas jurisdicciones nacionales) y, por otro, la cuestión de la atribución de la conducta [6], que se complica por el anonimato existente en la red [7]. A falta de obligaciones primarias más específicas, se aplicaría en el ciberespacio el Derecho internacional general (el Proyecto de Artículos de la Comisión de Derecho Internacional sobre la responsabilidad internacional del Estado) [8] que, además, se ha interpretado restrictivamente, tanto por el informe del Grupo de Expertos Gubernamentales de la Organización de las Naciones Unidas (ONU) de 2015 [9],

---

egy: For a stronger and more prosperous Canada, 2010, p. 2, accesible en *https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf*.

[2] Nye, J. S., *Cyber Power*, Cambridge MA, Harvard Kennedy School, 2010, p. 15; Shackelford, S. J., «Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance», *American University Law Review*, vol. 62, 2013, pp. 1263-1364, esp. p. 1292.

[3] Segura-Serrano, A., «Internet Regulation and the Role of International Law», *Max Planck Yearbook of UN Law*, vol. 10, 2006, pp. 191-272, esp. p. 231.

[4] Tsagourias, N., «The legal status of cyberspace», en Tsagourias, N. y Buchan, R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar, 2015, pp. 13-29, esp. pp. 19-21.

[5] Treppoz, E., «Jurisdiction in the Cyberspace», *Swiss Review of International and European Law*, vol. 26, 2016, pp. 273-287, esp. p. 275.

[6] Zimmermann, A., «International Law and Cyber Space», *ESIL Reflection*, vol. 3, 2014, núm. 1, pp. 1-6, esp. p. 3.

[7] Antonopoulos, C., «State responsibility in cyberspace», en Tsagourias, N. y Buchan, R. (eds.), *op. cit.*, nota 4, pp. 55-71, esp. p. 62.

[8] Proyecto de artículos de la Comisión de Derecho internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, Documentos oficiales de la Asamblea General, 56.º periodo de sesiones, Suplemento núm. 10 (A/56/10), pp. 10-405.

[9] Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, Documentos oficiales de la Asamblea General, 70.º periodo de sesiones (A/70/174), pp. 2-20.

como por el Manual de Tallin[10]. Las actividades de los actores no estatales no podrían atribuirse a los Estados más que si se prueba la existencia de un control efectivo, lo que resulta muy restrictivo para el ciberespacio[11]. Esta situación solo podría superarse si, como se apunta desde la doctrina, se aplica el criterio de la diligencia debida en el marco de la obligación consuetudinaria de no permitir el uso del territorio de un Estado para causar daños en otro Estado (asunto de *Canal de Corfú*)[12], recogida en el mencionado informe de 2015[13] y en el Manual de Tallin[14]. De este modo, se obviaría la necesidad de identificar al autor de la actividad cibernética (la atribución técnica) y el requisito de atribución al Estado sería menos oneroso[15].

3. LA CIBERSEGURIDAD

5. El creador de Internet, Tim Berners-Lee, ya advertía que es difícil preservar la seguridad en la Red. En la etapa actual, el objetivo de la ciberseguridad contiene algunos elementos propios de un bien público[16]. Diversos autores han identificado las distintas amenazas para la seguridad nacional que emergen desde Internet, como son la ciberguerra, el ciberterrorismo, el cibercrimen y el ciberespionaje[17]. Desde el Derecho internacional no se han adoptado iniciativas normativas concretas dirigidas a afrontar cada una de estas amenazas, salvo en el caso de la Convención de Budapest de 2001[18]. La doctrina y la práctica estatal han optado por una aplicación extensiva o analógica de las normas convencionales o consuetudinarias en vigor, consideradas por muchos como suficientes para hacer frente a estos desafíos.

6. La ciberguerra es quizá una de las cuestiones que han sido objeto de mayor tratamiento por la doctrina, en particular, por parte de los autores de Estados Unidos vinculados al ejército. El problema se suscita, en primer lugar, con la posible calificación de los ciberataques como uso de la fuerza. Existe consenso en la literatura académica a la hora de interpretar que un ciberataque con consecuencias similares al uso de la fuerza armada vulnera

---

[10] Schmitt, M. N. (ed.), *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013.

[11] Mačak, K., «Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors», *Journal of Conflict & Security Law*, vol. 21, 2016, pp. 405-428, esp. p. 427.

[12] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania),* Sentencia de la Corte Internacional de Justicia, sobre el fondo, de 9 de abril de 1949 (ICJ Reports 1949), p. 22.

[13] Véase Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, *op. cit.*, nota 9, p. 10.

[14] Véase Schmitt, M. N. (ed.), *op. cit.*, nota 10, p. 26.

[15] Tsagourias, N., «Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm», *Journal of Conflict and Security Law*, vol. 21, 2016, pp. 429-453, esp. p. 431.

[16] Rosenzweig, P., *Cybersecurity and Public Goods: The Public/Private «Partnership»*, Stanford University, Hoover Institution, 2011.

[17] Nye, J. S., *op. cit.*, nota 2, p. 16.

[18] Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, *BOE* núm. 226, de 17 de septiembre de 2010. En vigor desde el 1 de julio de 2004.

el art. 2.4 de la Carta de la ONU. En concreto, se trata de los ataques que causen lesiones o pérdida de vidas humanas, destrucción de la propiedad y, también, daños a infraestructuras críticas que provoquen un quebranto significativo en la prestación de servicios esenciales[19]. Igualmente, con relación a si un ciberataque puede ser interpretado como un ataque armado conforme al art. 51 de la Carta de la ONU que justifique el recurso a la legítima defensa, la mayoría de autores se decanta por aceptar esta posibilidad, siempre y cuando el ataque previo tenga una «escala y efectos» (asunto *Nicaragua*)[20] cualitativamente análogos a los de un ataque armado (Regla 13 del Manual de Tallin). Sin embargo, estos supuestos no se han constatado nunca, ni siquiera en los episodios de Estonia en 2007[21] o el virus *Stuxnet* en 2010[22].

7. Por lo que respecta al ciberterrorismo, por un lado existe la posibilidad de aplicar las Convenciones sectoriales de la ONU que desde la década de los años sesenta se han ido celebrando para combatir diversos fenómenos relacionados con el terrorismo, como el secuestro, la toma de rehenes, la seguridad de la navegación o la aviación, etc.[23]. Algunos actos de ciberterrorismo podrían quedar encuadrados en estos convenios pero, por el enfoque funcional de los mismos, la mayoría se situarían fuera de su ámbito de aplicación[24]. Por otro lado, el proyecto de Convenio global contra el terrorismo internacional[25] incorpora en su art. 2 una definición que, por su enfoque general, podría abarcar la mayoría de actos ciberterroristas, incluidos los ataques a las infraestructuras críticas públicas, pero también a la propiedad privada, si bien habría que aplicar el sentido común con el objeto de dejar fuera de su ámbito de aplicación ciertos casos-límite[26]. Aunque todos los grupos terroristas se encuentran presentes en la Red, un ciberterrorismo auténtico es hasta ahora una posibilidad, más que una realidad cotidiana.

8. Con relación al ciberespionaje, existe una preocupación creciente en la comunidad internacional por el aumento de esta práctica, aunque el caso *Snowden* ha puesto de manifiesto que esta actividad también se realiza por parte de los gobiernos occidentales, especialmente el de Estados Unidos. Como es sabido, no existe ningún tratado internacional que regule o prohíba el espionaje y tampoco el ciberespionaje. No obstante, una corriente crecien-

---

[19] Roscini, M., *Cyber Operations and the Use of Force*, Oxford, OUP, 2014, pp. 44-67.

[20] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Sentencia de la Corte Internacional de Justicia de 27 de junio de 1986 (ICJ Reports 1986), párr. 195.

[21] Davis, J., «Hackers Take Down the Most Wired Country in Europe», *The Wired*, 21 de agosto de 2007, accesible en *https://www.wired.com/2007/08/ff-estonia/*.

[22] Zetter, K., «An Unprecedented Look at Stuxnet, the World's First Digital Weapon», *The Wired*, 3 de noviembre de 2014, accesible en *https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/*.

[23] Pueden consultarse estas Convenciones en el siguiente enlace: *http://www.un.org/en/counterterrorism/legal-instruments.shtml.*

[24] Saul, B. y Heath, K., «Cyber terrorism», en Tsagourias, N. y Buchan, R. (eds.), *op. cit*., nota 4, pp. 147-167, esp. pp. 152-153.

[25] Proyecto de convenio general contra el terrorismo internacional, Documentos oficiales de la Asamblea General, 59.º periodo de sesiones (A/59/894), pp. 8-20, esp. p. 10.

[26] Saul, B. y Heath, K., «Cyber terrorism», *op. cit.*, nota 24, pp. 155-159.

te de la doctrina anglosajona tiende hoy día a conceptuar el ciberespionaje, bien como una vulneración de la prohibición del uso de la fuerza[27], bien como una vulneración del principio de igualdad soberana de los Estados, cuyo corolario es el principio de no intervención, de modo que esta práctica se puede considerar como una amenaza a la paz y seguridad internacionales[28]. El cambio en el *status quo* político que Internet está introduciendo respecto de las tradicionales ventajas estratégicas disfrutadas por las grandes potencias está detrás de estas desmesuradas caracterizaciones jurídicas. En efecto, los Estados más poderosos desde el punto de vista político y económico son los que pueden perder más frente al ciberespionaje, sobre todo el económico[29]. No obstante, parece más aceptable la postura que interpreta que solo existe una vulneración del principio de igualdad soberana cuando una actividad de ciberespionaje conlleva el ejercicio de jurisdicción por parte de una autoridad extranjera[30].

9. Finalmente, el cibercrimen constituye la cuestión problemática más acuciante de todas. Por esa razón, la cooperación internacional se ha concretado muy pronto en Derecho convencional a través del Convenio de Budapest del Consejo de Europa de 2001, del que también forman parte países como Estados Unidos, Japón, Canadá, Australia o Méjico. Este convenio persigue incrementar la armonización material de los delitos relacionados con Internet y la cooperación transnacional en la persecución de los mismos, sobre la base de la aplicación del principio de territorialidad en sentido amplio (doctrina de los efectos) y del principio de la nacionalidad. Estos dos principios resultan suficientes para atribuir jurisdicción en la persecución de los delitos cibernéticos y los posibles conflictos de jurisdicción que surjan se pueden resolver a través de las consultas entre Estados de forma *ad hoc*[31]. No obstante, se achaca que el bajo nivel en la implementación del Convenio por parte de los Estados no está permitiendo obtener todos los beneficios que se derivarían del mismo.

4. LA COOPERACIÓN INTERNACIONAL

10. La cooperación internacional en materia de ciberseguridad se está produciendo en torno a algunas organizaciones internacionales como la

---

[27] Joyner, C. y Lotrionte, C., «Information Warfare as International Coercion: Elements of a Legal Framework», *European Journal of International Law*, vol. 12, 2001, pp. 825-865, esp. p. 855.

[28] Buchan, R., «Cyber espionage and international law», en Tsagourias, N. y Buchan, R. (eds.), *op. cit.*, nota 4, pp. 168-189, esp. p. 177.

[29] Ziolkowski, K., «Peacetime Cyber Espionage - New Tendencies in Public International Law», en Ziolkowski, K. (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, pp. 425-464, esp. p. 460.

[30] *Ibid.*, p. 459; von Heinegg, W. H., «Territorial Sovereignty and Neutrality in Cyberspace», *International Law Studies*, vol. 89, 2013, pp. 123-156, p. 128.

[31] UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Nueva York, 2013, pp. 195-196, accesible en *https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*.

Unión Europea (UE), la Organización del Tratado del Atlántico Norte (OTAN) o la ONU, entre otras. Con relación a la UE, aunque la Comisión comenzó ya en el año 2001 a preocuparse por este ámbito, ha sido en 2013 cuando se ha adoptado la primera Estrategia de Ciberseguridad que identifica las prioridades que deben guiar la política de ciberseguridad en la UE y en el plano internacional[32]. Estas prioridades consisten en conseguir la ciberresiliencia, reducir de forma drástica el cibercrimen (en donde se ha adoptado la Directiva 2013/40/EU)[33], desarrollar una política y capacidades de ciberdefensa, desarrollar recursos industriales y tecnológicos y, finalmente, establecer una política internacional del ciberespacio coherente[34]. La concreción más importante que ha tenido esta Estrategia ha sido la Directiva 2016/1148/UE sobre seguridad de las redes y sistemas de información (conocida como Directiva NIS)[35]. Esta Directiva ha impuesto obligaciones tanto para los Estados miembros (resiliencia) como para los operadores de infraestructuras críticas y suministradores de servicios de la sociedad de la información (incluyendo redes sociales, servicios en la nube y motores de búsqueda). De este modo, la UE deja atrás el enfoque voluntario y opta por otro prescriptivo que impone a los operadores privados la obligación de adoptar medidas de seguridad, así como la obligación de compartir información con las autoridades sobre incidentes producidos. Este enfoque prescriptivo resulta novedoso y puede marcar el tono de las estrategias nacionales en materia de ciberseguridad en el plano global[36].

11. Respecto de la OTAN, esta ha sido la primera organización internacional en reaccionar ante este tipo de amenazas, ya desde 2002. Tras los ciberataques a Estonia en 2007 se ha dotado de una Política sobre Ciberdefensa, revisada y mejorada después, y ha incorporado esta preocupación al Concepto Estratégico desarrollado en Lisboa en 2010[37]. Los principios que guían esta Política son la prevención de los ciberataques y la resiliencia de las redes, que son fundamentalmente responsabilidad de los Estados miembros, aunque la OTAN suministra asistencia a los miembros que la requieran. Asimismo, aunque el Concepto Estratégico de 2010 ha incorporado expresamente la posibilidad de activar el art. 5 del Tratado de Washington sobre defensa colectiva, y la Cumbre de Varsovia de 2016 ha declarado el ciberespacio como el cuarto ám-

---

[32] Comisión Europea, «Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro», *JOIN (2013) 1 final*, de 7 de febrero de 2013.

[33] Directiva (UE) núm. 2013/40, del Parlamento Europeo y del Consejo, de 12 de agosto, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, *DO* L núm. 218, de 14 de agosto de 2013.

[34] Comisión Europea, *op. cit.*, nota 32, p. 5.

[35] Directiva (UE) núm. 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, *DO* L núm. 194, de 19 de julio de 2016.

[36] Segura-Serrano, A., «Cybersecurity: Towards a Global Standard in the Protection of Critical Information Infrastructures», *European Journal of Law and Technology*, vol. 6, 2015, pp. 1-15, esp. p. 12.

[37] Fidler, D. P., Pregent, R. y Vandurme, A., «NATO, Cyber Defense, and International Law», *St. John's Journal of International & Comparative Law*, vol. 4, 2013, núm. 1, pp. 1-25, esp. pp. 4-7.

bito de operaciones, junto con la tierra, el aire y el mar[38], la OTAN va a ser prudente en este terreno, como demuestra el episodio de Estonia. En este sentido, se plantea como escenario más común el de la acción frente al cibercrimen[39].

12. La actividad de la ONU ha sido muy prolífica en cuanto a la ciberseguridad. En el marco de la Primera Comisión de la Asamblea General (AG), ya Rusia comenzó en 1998[40] su práctica de proponer anualmente una Resolución sobre la seguridad internacional en el ámbito de las telecomunicaciones y la información[41]. Los países occidentales han sospechado siempre de esta iniciativa, al vincularla con un intento de restringir la libertad de información[42], hasta que Estados Unidos cambia de actitud en 2010 y comienza a co-patrocinar estas Resoluciones, eso sí, rebajando su lenguaje normativo[43]. En el marco de la Segunda Comisión, han sido Estados Unidos y los países occidentales los que han promovido diversas Resoluciones[44] que fomentan la creación de capacidades y una cultura de ciberseguridad por los Estados miembros. La Tercera Comisión se ha centrado en el combate del cibercrimen[45] y, tras el caso *Snowden*, en el derecho a la privacidad[46]. No obstante, son los cuatro Grupos de Expertos Gubernamentales establecidos en el marco de la Primera Comisión los que más atención han atraído. Si el primer Grupo de 2004 no pudo llegar a elaborar un informe final por falta de consenso[47] (Rusia quería avan-

---

[38] Paganini, P., «NATO officially recognizes cyberspace a warfare domain», *Security Affairs*, 18 de junio de 2016, accesible en *http://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html*.

[39] Ziolkowski, K., «NATO and cyber defence», en Tsagourias, N. y Buchan, R. (eds.), *op. cit.*, nota 4, pp. 426-445, esp. p. 433.

[40] Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional, Documentos oficiales de la Asamblea General, 53.º periodo de sesiones (A/RES/53/70).

[41] Maurer, T., *Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security*, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2011, p. 20, accesible en *http://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf*.

[42] Henderson, C., «The United Nations and the regulation of cyber-security», en Tsagourias, N. y Buchan, R. (eds.), *op. cit.*, nota 4, pp. 465-490, esp. p. 468.

[43] Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, Documentos oficiales de la Asamblea General, 65.º periodo de sesiones (A/RES/65/41).

[44] Creación de una cultura mundial de seguridad cibernética, Documentos oficiales de la Asamblea General, 57.º periodo de sesiones (A/RES/57/239); Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales, Documentos oficiales de la Asamblea General, 58.º periodo de sesiones (A/RES/58/199); y Creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales, Documentos oficiales de la Asamblea General, 64.º periodo de sesiones (A/RES/64/211).

[45] Lucha contra la utilización de la tecnología de la información con fines delictivos, Documentos oficiales de la Asamblea General, 55.º periodo de sesiones (A/RES/55/63) y, con el mismo título, A/RES/56/121. Véase Fortalecimiento del Programa de las Naciones Unidas en materia de prevención del delito y justicia penal, en particular de su capacidad de cooperación técnica, Documentos oficiales de la Asamblea General, 63.º periodo de sesiones (A/RES/63/195) y, con el mismo título, A/RES/64/179, A/RES/65/232, A/RES/66/181, A/RES/67/189 y A/RES/68/193.

[46] El derecho a la privacidad en la era digital, Documentos oficiales de la Asamblea General, 68.º periodo de sesiones (A/RES/68/167).

[47] Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, Documentos oficiales de la Asamblea General, 60.º periodo de sesiones (A/RES/60/202), p. 2.

zar en la fijación de nuevas reglas y Estados Unidos se oponía por entender que las vigentes resultan suficientes), el segundo Grupo sí alcanzó en 2010 el consenso necesario para establecer áreas de cooperación en materia de comportamiento estatal responsable, así como medidas de creación de capacidad y confianza (reiteradas en informes posteriores)[48]. Antes del informe adoptado por el tercer Grupo en 2013, Rusia, China y otros Estados introdujeron en 2011 en la AG un Código de Conducta Internacional para la Seguridad de la Información que proponía un tratado para regular Internet (al que se opuso Estados Unidos por las razones ya mencionadas), luego revisado en 2015[49]. La novedad consiste en que el Informe de 2013 sí pudo avanzar en su tarea al reconocer la aplicabilidad del Derecho internacional (y la Carta de la ONU) al ámbito de las tecnologías de la información y la comunicación (TIC), además de las normas sobre derechos humanos y responsabilidad internacional de los Estados[50]. El Informe del cuarto Grupo de 2015 ha matizado aún más sobre la aplicabilidad de las reglas del Derecho internacional, en concreto, respecto del principio de la diligencia debida, así como respecto de los principios propios del Derecho internacional humanitario[51].

5. CONSIDERACIONES FINALES

13. Superada la reticencia inicial de una parte de la doctrina, el ciberespacio se configura hoy como un ámbito sujeto al Derecho internacional. No obstante, es cierto que no se ha avanzado mucho en la adopción de normas convencionales y, desde luego, no se ha celebrado ningún tratado general sobre Internet. Pero el problema no es jurídico, sino político. Estados Unidos (y sus gigantes tecnológicos) se niega a avanzar en la regulación internacional de Internet por interés puramente estratégico[52]. Sin embargo, se han dado pasos importantes con el reconocimiento de la aplicabilidad de las normas generales de Derecho internacional al ciberespacio. Precisamente, y por el mismo beneficio estratégico, es también Estados Unidos el más interesado en apoyar esa aplicación analógica de las normas existentes.

---

[48] Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, Documentos oficiales de la Asamblea General, 65.º periodo de sesiones (A/RES/65/201), pp. 2-9.

[49] Carta de fecha 12 de septiembre de 2011 dirigida al secretario general por los representantes permanentes de China, la Federación de Rusia, Tayikistán y Uzbekistán ante las Naciones Unidas, Documentos oficiales de la Asamblea General, 69.º periodo de sesiones (A/66/359); y Carta de fecha 9 de enero de 2015 dirigida al secretario general por los representantes permanentes de China, la Federación de Rusia, Kazajstán, Kirguistán, Tayikistán y Uzbekistán ante las Naciones Unidas, Documentos oficiales de la Asamblea General, 69.º periodo de sesiones (A/69/723).

[50] Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, Documentos oficiales de la Asamblea General, 68.º periodo de sesiones (A/RES/68/98), pp. 2-12.

[51] Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, *op. cit.*, nota 9, pp. 9-20.

[52] Goldsmith, J., *Cybersecurity Treaties, A Skeptical View*, Stanford University, Hoover Institution, 2011.

14. La ciberseguridad será, con toda probabilidad, la cuestión problemática que seguirá impulsando la cooperación internacional en este campo. La seguridad colectiva es una preocupación de primer orden que ya está resuelta en el Derecho internacional, aunque la práctica demuestre que los ciberataques de carácter militar no constituyen una amenaza cotidiana. El verdadero problema está, sin embargo, en el cibercrimen y, en menor medida, en el ciberespionaje. Frente a estas ciberamenazas, las organizaciones internacionales analizadas, y otras, como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Unión Internacional de Telecomunicaciones (UIT), están fomentando un tipo de cooperación fundamentalmente de carácter asistencial. Es decir, se confía más en la creación de capacidades por parte de los Estados para avanzar en la resiliencia que en la cooperación de tipo jurídico (con la excepción de la Convención de Budapest, escasamente aplicada). Por otra parte, las revelaciones del caso *Snowden* no ayudan en nada a esa cooperación jurídica internacional, por lo que cabe esperar que el *status quo* actual se mantenga durante algún tiempo.

Palabras clave: seguridad nacional, ciberseguridad, ciberterrorismo, cibercrimen, ciberataque.

Keywords: national security, cybersecurity, cyberterrorism, cybercrime, cyberattack.