1
Introducción

De todos es conocido el papel que desempeña en nuestras sociedades la cibernética, ciencia que estudia los flujos de comunicación y de información desde una perspectiva interdisciplinar, ocupándose de temas variados pero transcendentales para las sociedades actuales. Las tecnologías de la información y la comunicación (TICs) se han convertido en la piedra angular de nuestro crecimiento económico y constituyen un recurso crítico del que dependen todos los sectores económicos. Actualmente reposan en ellas los complejos sistemas que permiten funcionar a nuestras economías en sectores clave, tales como las finanzas, la sanidad, la energía y los transportes. Estas características forzosamente van a influir no solo, en efecto, en los aspectos civiles de las sociedades modernas, sino que también, como no podía ser de otra manera, en los aspectos de seguridad y defensa. Tanto es así que la cibernética ha hecho gala al origen griego del término "KuBEpvntnç" (Kybernètès), que significa la persona que maneja el timón y que dirige una embarcación. Es evidente que sin esta herramienta nuestras sociedades y, por ende, las relaciones internacionales serían algo muy distinto de lo que son en la actualidad. Pero al margen de todo esto, el mundo digital aporta grandes beneficios,

aunque también es vulnerable, por lo que la cibernética presenta unos retos para el sistema jurídico internacional que hace que se tengan que adoptar medidas para garantizar la seguridad de los Estados[1] y las libertades fundamentales de los ciudadanos, cuya garantía implica fomentar un control seguro y libre de internet como promoción de los derechos humanos[2].

Otro elemento a tomar en consideración es que, debido a lo novedoso de este sector, casi no existen normas sectoriales del Derecho internacional que se ocupen específicamente del ciberespacio, a pesar de la cantidad de comunicaciones que se llevan a cabo diariamente. Esto no es ninguna novedad en el ámbito del Dere-

1. A este respecto, para ver los retos que se presentan en materia de ciberseguridad, así como los riesgos, estrategias y fomento de las medidas de confianza, ver las conferencias presentadas que sobre esta materia tuvieron lugar en el Ministerio Federal Alemán de Asuntos Exteriores el 11 de diciembre de 2011, disponible en http://www.auswaertiges-amt.de/EN/Infoservice/Presse/Meldungen/2011/111212_Cybersicherheit.html¿?nn=382590 (consultado el 20 de marzo de 2020).

2. Este fue precisamente el objeto de la jornada que sobre Internet y Derechos Humanos tuvo lugar el 12 de septiembre de 2012. Disponible en: http://www.auswaertiges-amt.de/sid_D911C8E0F05824607EFD3F489C0E/EN/Aussenpolitik/Menschenrechte/Aktuell/120912-Konferenz-Internet-Menschenrechte.html. En esta ocasión el Ministro alemán de Asuntos Exteriores, Guido Westerwelle, haría hincapié en su discurso del 14 de septiembre de 2012 en que la libertad debe ser la máxima prioridad en los asuntos relacionados con internet, en donde debe asegurarse la libertad de expresión, la libertad de reunión, la libertad y el libre acceso a la información como pilares de la cibernética, indicando además que la libertad trae consigo la responsabilidad de todos los que recurren a esta herramienta como los individuos, las sociedades y los Gobiernos, que deben actuar con transparencia y espíritu de diálogo. A este respecto, cfr. Speech by Foreign Minister Guido Westerwelle at the conference "The Internet and Human Rights: Building a Free, Open and Secure Internet", 14 september 2012, disponible en: http://www.auswaertiges-amt.de/EN/Infoservice/Presse/Reden/2012/120914-BM_Internet_MR.html?nn=648756 (consultado el 20 de marzo de 2020).

cho internacional, pues problemas similares se dieron ya con las ondas de radio atravesando las fronteras, algo que más tarde sucedería con las comunicaciones vía satélite, etc., recurriendo siempre a las normas preexistentes del Derecho internacional. Desde esta perspectiva, no es extraño que en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional se haya reconocido que el Derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable y, además es esencial, al mantenimiento de la paz y de la estabilidad[3], al considerar que "the application of norms derived from existing International Law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability. Common understandings on how such norms shall apply to State behaviour and the use of ICTs by States requires farther Study…"[4].

Dicho esto, no hay que olvidar que el "ciberespacio", a pesar de que en muchas ocasiones se diga que es un espacio que no está localizado, esto es un grave error, pues esas comunicaciones necesitan "hardware" que debe estar en algún sitio, y las comunicaciones deben pasar por algún territorio o tener un vínculo en el ciberespacio como una especie de Derecho del Espacio en el que los Estados, como es sabido, no ejerce jurisdicción[5].

3. A este respecto, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Doc. UN. A/68/98, 24 June 2013, 13 p. especialmente p. 8, en donde se recogen las recomendaciones sobre las normas y principios que deben respetar los Estados, párrafos 16-25. Ver también, BUCHAN, Russel: *Cyber Espionage and International Law*, Bloomsbury Academic, 2018, 248 p.

4. *Ibid*, p. 8, párrafo 16.

5. Para más detalles, cfr. ZEKOLL, Joachin: "Jurisdiction in Cyberspace", en HANDL, Günther / ZEKOLL, Joachin / ZUMBANSEN, Peer (Eds.): *Beyond Territoriality: Transnational Legal Authority in an Age of Globalisation*, Martinus Nijhoff Publishers, The Hague, 2012, pp. 341-369. Ver también KOHL, Uta: "Jurisdiction in Cyberspace", en TSAGOURIAS, Nicholas y BUCHAN,

Esto no quiere decir, sin embargo, que el ciberespacio, que es *de iure* sometido al Derecho internacional, y que puede caer bajo la jurisdicción de uno o más Estados, no presente serios retos a nivel internacional, ya que muchos Estados, así como los actores no estatales o las empresas transnacionales, que tienen un papel relevante en el ciberespacio, no desean regular de una manera estricta este ámbito, pues esto les impediría llevar a cabo sus actividades con la libertad que tienen ahora. Si a esto añadimos la enorme distancia tecnológica existente entre los Estados industrializados y las empresas multinacionales, por un lado, y los pequeños Estados, incluidos muchos en desarrollo, por otro, es evidente, y así se reconoce *de facto*, que estos últimos no están en condiciones de poder ejercer un mínimo de control sobre las actividades ciberespaciales que afectan a su territorio. Desde este prisma, la gran cantidad de información que circula a través de distintos territorios y de Estados trae consigo que no siempre los mecanismos existentes, sobre todo los de los pequeños Estados puedan detectar las peligrosas actividades que se ciernen sobre el ciberespacio, y esto al margen de que puedan proceder de actores no estatales o de ciertos Estados. Pero incluso al margen de esto, ya se sabe que no siempre es posible, o al menos encierra muchas dificultades, trazar el camino de las actividades cibernéticas, no solo cuando proceden de actores no estatales, sino también cuando se trata de actividades que puedan atribuirse a un determinado Estado aplicando las normas del Derecho internacional de la responsabilidad internacional, tal y como han sido codificadas por la Comisión de Derecho Internacional (CDI)[6].

Russell (Eds.). *Research Handbook on International Law and Cyberspace*, Edward Elgar, Cheltenham UK, 2015, pp. 14 y ss.

6. A este respecto, cfr. Resolución A/56/83, del 28 de enero de 2002, Anexo. Véase *per omnia*, GUTÍERREZ ESPADA, Cesáreo: *La responsabilidad: las*

En estas circunstancias no es extraño que la ciberseguridad se haya convertido en un elemento imprescindible de la sociedad internacional actual[7], al formar parte de ese dúo tan importante de las relaciones internacionales actuales como son la paz y la seguridad internacionales[8], concepto amplio que requiere, según algunos autores, la adopción de normas específicas primarias, normas basadas en los principios generales del derecho derivados de los principios comunes a los principales sistemas jurídicos del mundo o la adaptación por analogía de las normas existentes en la medida de lo posible al ámbito de la ciberseguridad[9]. Un principio general se podría elevar a la categoría de principio general del derecho

consecuencias del hecho ilícito, Diego Marín librero Editor, Murcia, 2005, 311 páginas, y la bibliografía allí destacada.

7. Cfr. LIBICKI, Martin: *Cyberspace in Peace and War*, Naval Institute Press, Annapolis, 2011, 496 p. Ver también, MILLÁN MORO, Lucia (Dir): *Ciberataques y ciberseguridad en la escena internacional*, Thomson-Aranzadi, Cizur Menor, 2020, 308 p.; SEGURA SERRANO, Antonio: "Ciberseguridad y Derecho internacional", *Revista Española de Derecho Internacional*, vol. 69/2, 2017, pp. 291-299.

8. Cfr. ZIOLKOWSKI, Katharina (Ed.): *Peacetime Regime for State Activiti's in Cyberspace: International Law,* International Relations and Diplomacy, NATO CCD COE Publications, 2013, 746 p. En esta obra participan 24 autores del mundo académico y militar, abordando lo esencial de los problemas que plantea la ciberseguridad en el campo del Derecho internacional, las Relaciones Internacionales y de la Diplomacia, con una amplia bibliografía, pp. 691-738.

9. A este respecto, cfr. los estudios siguientes publicados en el *German Yearbook of International Law*, Vol. 58, 2015: WALTER, Christian: "Obligations of State Before, During and After a Cyber Security Incident", pp. 67-86; DÖRR, Oliver: "Obligations of the State of Origin of a Cyber Security Incident", pp. 87-99; KOLB, Robert: "Reflections on Due Diligence Duties and Cyberspace", pp. 112-128; BRUNNEE, Jutta / MESHEL, Tamar: "Teaching and Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance: Due Diligence Obligations and Institutional Models for Enhanced Inter-State Cooperation", pp. 169-185.

que forma parte del Derecho internacional, si la comunidad de naciones en general considera que dicho principio es justo o que refleja su conciencia colectiva, o un principio inherente a cualquier sistema jurídico[10]. Esto ha sido lo que ha ocurrido *grosso modo* con el Derecho internacional del medio ambiente, por ejemplo, y se puede decir que el resultado ha sido exitoso. Un poco más claro, sin embargo, se ven las actividades del ciberespacio en relación con el *jus ad bellum* y con el *jus in bello*, al partir de la premisa de que es posible que ataques cibernéticos puedan pasar el umbral previsto en la prohibición del uso de la fuerza tal y como está recogida en el artículo 2.4 de la Carta de las Naciones Unidas, y constituir ataques armados que den lugar al derecho de legítima defensa tanto consuetudinario como convencional, de conformidad con el artículo 51 de la Carta de las Naciones Unidas, siempre que el ataque reúna los requisitos previstos para poder ejercer ese dere-

10. WEIL, Prosper: "Le droit international en quête de son identité: cours général de droit international public", *Recueil des Cours de l'Academie de Droit International de La Haye*, vol. 237, 1992, pp. 146 y 147. En esta misma línea, años más tarde, la Sala de Primera Instancia en la causa *Kunarac* argumentaba con detalle que "el valor de esas fuentes [nacionales] es que pueden revelar "conceptos generales e instituciones jurídicas" que, si son comunes a un amplio espectro de sistemas jurídicos nacionales, ponen de manifiesto un enfoque internacional acerca de una cuestión jurídica que podría considerarse un indicador apropiado del derecho internacional en la materia. Al examinar esos sistemas jurídicos nacionales, la Sala de Primera Instancia no lleva a cabo un estudio de los principales sistemas jurídicos del mundo para identificar una disposición jurídica específica adoptada por la mayoría de los sistemas jurídicos, sino para considerar, a partir de un examen de los sistemas nacionales en general, si es posible identificar ciertos principios básicos o, según las palabras empleadas en el fallo de la causa *Furundžija*, "denominadores comunes", en esos sistemas jurídicos que encarnen los *principios* que deben adoptarse en el contexto internacional". Cfr., *Prosecutor v. Dragoljub Kunarac, Radmir Kunac and Zoran Vukovic*, causa nº. IT-96-23-T & IT-96-23/1-T, fallo, 22 de febrero de 2001, Tribunal Penal Internacional para la ex-Yugoslavia, párrafo 349.

cho. Estos aspectos son los que queremos abordar en las siguientes páginas, siendo conscientes de que tanto en el ámbito del *jus ad bellum* como en el del *jus in bello,* la cibernética presenta grandes retos al Derecho internacional[11], cuya respuesta es tarea onerosa, pero no imposible. Para que el Derecho pueda adoptar medidas al respecto hay que definir claramente el problema y los desafíos que han de ser abordados basándose en el conjunto de normas y principios generales aplicables y que regulan esos ámbitos, clásicos en sí mismos, pero abiertos al dinamismo de la evolución de la sociedad internacional y la potencialidad de las nuevas tecnologías aplicables tanto en tiempos de paz como en tiempos de guerra.

11. Cfr. MARTÍN, Ney / ZIMMERMAMN, Andreas: "Cyber-Security Beyond the Military Perspective: International Law 'Cyberspace' and the Concept of Due Diligence", *German Yearbook of International Law*, vol. 58, 2015, pp. 51-66.