REVISTA CHILENA DE DERECHO Y CIENCIA POLÍTICA
ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

El ciberespacio: Presupuestos para su ordenación jurídico-internacional

Cyberspace: Bases for a international regulation

MARGARITA ROBLES CARRILLO[1]
Universidad de Granada, España

RECEPCIÓN: 21/01/2016 • ACEPTACIÓN: 22/04/2016

RESUMEN El ciberespacio es un ámbito en el que el avance y el desarrollo tecnológicos, imparables en su velocidad y en su impacto, contrastan con una situación de relativo impasse desde el punto de vista jurídico. El derecho se ha ocupado de su regulación mediante una aproximación sectorial, coyuntural y fragmentaria que difícilmente puede cubrir sus necesidades de normación. El aumento de la criminalidad y de la conflictividad cibernética constituye una prueba evidente y constante de las carencias de esa regulación.

La ordenación jurídica del ciberespacio requiere un planteamiento global y coherente sobre la base de un análisis previo de esta realidad y de los condicionantes y presupuestos que impone y que la diferencian de otros espacios sujetos a regulación. La amenaza cibernética supone un cambio de paradigma porque es diferente, completamente deslocalizada, insuficientemente apreciada y de naturaleza estructural. La conflictividad ciberespacial se manifiesta, asimismo, de un modo singular en la cibercriminalidad, el ciberespionaje, el ciberterrorismo y la ciberguerra, diferenciándose de sus homólogas no virtuales y difuminándose los límites entre esas diversas categorías. El ciberespacio impone, también, la necesidad de abordar ciertos cambios en los modelos de organización interna e internacional.

[1] Abogada. Doctora en Derecho de la Universidad de Granada, España. Profesora titular de Derecho Internacional y Relaciones Internacionales de la Universidad de Granada, España. Correo: mrobles@ugr.es

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

PALABRAS CLAVE Ciberespacio - Derecho Internacional – Ciberamenazas - Conflictividad Cibernética - Ciberseguridad.

ABSTRACT Cyberspace is a field where technological progress and development, both for its speed and its impact, are in contrast with a situation of relative impasse from a legal point of view. The law has regulated cyberspace through a sectoral, conjunctural and fragmented approach. The increase in crime and cyber conflictivity is a clear and consistent proof of the shortcomings and limits of this regulatory action.

The international legal regulation of cyberspace requires a previous, comprehensive and coherent approach taking into account the uniqueness of cyberspace and based on the preliminary analysis of that reality and of the conditions and legal and non-legal features that prevails and that differentiate it from other areas subject to regulation. The cyber threat is a paradigm shift because it is different, completely delocalized, insufficiently appreciated and it is of structural nature. The cyber conflict is also manifested in a singular way in cybercrime, cyber espionage, cyber terrorism and cyber warfare, differing from their non-virtual counterparts and blurring the boundaries between these different categories. Cyberspace imposes also the need to address certain changes in the patterns of internal and international organization.

KEYWORDS Cyberspace - International Law – Cyberthreats - Cyber Conflict - Cybersecurity.

Introducción

Los avances científicos y tecnológicos de las últimas décadas han conducido a la generación del ciberespacio que, como el resto de los ámbitos de acción social, requiere una ordenación jurídica. No es una tarea fácil. El discurso político separa a quienes defienden la libertad y la accesibilidad del ciberespacio de quienes pretenden afirmar su soberanía y control sobre el mismo y enfrenta concepciones de fondo tan dispares que hace extremadamente difícil alcanzar un consenso a nivel internacional. A las divergencias políticas o ideológicas, que protagonizan China, Rusia y EEUU, se suman las diferencias de orden económico que, en este ámbito más que en otros, crean un contraste aparentemente insuperable entre los países tecnológicamente desarrollados y los que apenas se encuentran capacitados para acceder a las Tecnologías de la Información y la Comunicación (TICs). No se trata simplemente de una brecha digital porque, por su alcance y su naturaleza,

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

este fenómeno proyecta desigualdades de mayor calado en todos los ámbitos de la vida económica, cultural, política y social. Frente a esa situación, el debate jurídico se sitúa entre quienes propugnan una regulación específica atendiendo a la naturaleza singular del ciberespacio y quienes mantienen la aplicabilidad de la normativa creada para el mundo no virtual. El análisis académico y científico bascula también entre posiciones enfrentadas y, a veces, diametralmente opuestas en cuanto al modo de abordar la realidad cibernética, sin que sus aportaciones ofrezcan una solución finalmente aceptable y resolutiva.

En ese contexto se justifica este trabajo que tiene por objeto analizar los presupuestos jurídicos y no jurídicos que condicionan la ordenación jurídica del ciberespacio. El objetivo no es presentar la normativa en vigor, que es objeto de tratamiento en otros publicaciones, apuntadas en la bibliografía, sino incidir en los condicionantes que dificultan la traslación al ciberespacio de los esquemas tradicionales de regulación normativa y evitar cualquier aproximación formalista a este ámbito en el entendimiento de que, para ser eficaz, el derecho ha de responder a los imperativos y caracteres de la realidad social que está llamado a regular. En mi opinión, el conocimiento de los mismos en el ciberespacio es una condición previa necesaria para su ordenación jurídico-internacional. La realidad, sin embargo, muestra que la aproximación jurídica al ciberespacio se ha caracterizado justo por lo contrario.

I. El problema científico: La aproximación jurídica al ciberespacio

1. La función del Derecho internacional en el ciberespacio

Desde sus inicios, la historia del Derecho Internacional es un proceso evolutivo en el que, estructuralmente, destacan la formación del Estado moderno y la articulación molecular de la sociedad internacional sobre la base del principio de igualdad soberana de los Estados. Ese modelo de organización territorial se ha construido mediante la delimitación de los espacios terrestre, marítimo, aéreo y exterior, de modo progresivo, a medida que era factible el acceso y el uso de los mismos. En ese contexto, el principio de soberanía territorial constituye el fundamento de un modelo global que, en las últimas décadas, ha evolucionado desde el imperio del derecho de apropiación hasta la configuración de una nueva categoría de espacios no susceptibles de apropiación estatal, sujetos a un régimen internacionalizado, bajo la cobertura de su definición como patrimonio común de la humanidad. La atribución de esa calificación jurídica significa algo más que excluir dichos espacios de los imperativos de la soberanía territorial, exclusiva y excluyente. Ello es debido a que con dicha categoría se traslada realmente la

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

existencia de bienes jurídicos merecedores de especial consideración y se articula la función de protección de intereses generales y comunes de la sociedad internacional en su conjunto como función del Derecho Internacional. La aparición del ciberespacio supone una ruptura en esa dinámica[2].

Hasta ahora, el Derecho Internacional no se ha ocupado realmente del ciberespacio como del resto de los espacios físicos[3], ni de su delimitación, ni de su régimen jurídico[4]. No lo ha hecho a pesar de que su función es la ordenación de las competencias y de que es un espacio genéticamente universal, que se adiciona y transversaliza a los anteriores porque también es estructural y funcionalmente global[5]. No es un simple problema de organización de las competencias, como en el resto de los dominios, sino que se trata de ordenar la coexistencia social en un espacio diferente de sus predecesores y con una extraordinaria capacidad de interacción y de afectación de los mismos.

Es también, y no en menor medida, un problema de seguridad internacional[6], al menos, desde una doble y coincidente perspectiva: por una parte, en términos prácticos y contrastados en la realidad, la amenaza, el ataque y el conflicto cibernético se están consolidando como alternativas a las modalidades tradicionales de uso de la fuerza y de conflicto armado[7]; y, por otra parte, en el

---

[2] HEVERLY (2011) explica de un modo sucinto y claro la evolución del ciberespacio desde una perspectiva jurídica.

[3] SHACKELFORD (2009) y RYAN *et al* (2010-2011) advierten sobre las diferencias con esos otros espacios.

[4] Sobre los condicionantes que dificultan la elaboración del consenso necesario a esos efectos, véase SATOLA y JUDY (2011) p. 1749 y ss.

[5] La necesidad de un acuerdo internacional es analizada desde esa perspectiva por SOFAER en SOFAER y GOODMAN (2001) p. 221 y por MOORE (2013) p. 223.

[6] En los últimos años, más de veinte países han anunciado su intención de poner en marcha o reforzar sus capacidades cibernéticas no sólo defensivas sino ofensivas, iniciando una carrera armamentista digital en el contexto de seguridad del ciberespacio. Véase, al respecto, la información en: <http://geographicalimaginations.com/2015/09/29/visualising-the-invisible/>. [Fecha de consulta: 20 de enero de 2016].

[7] Sobre el tema se recomienda el Informe: *Beyond the Build Delivering Outcomes through Cyberspace. The Commander's Vision and Guidance for US Cyber Command*, Department of Defense. United States Cyber Command. Disponible en: <http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf>. [Fecha de consulta: 20 de enero de 2016].

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

plano teórico, el ciberespacio no es un ámbito material más que se adiciona a los anteriores, como la seguridad económica, medioambiental o alimentaria, dentro del modelo de seguridad global. El ciberespacio introduce un nuevo paradigma de seguridad llamado, por su naturaleza, a sustituir a sus predecesores porque la ciberseguridad no es simplemente la seguridad del ciberespacio sino que constituye un nuevo modelo global de seguridad[8]. A pesar de ello, el ciberespacio no ha sido aún objeto de una ordenación global en el marco jurídico-internacional[9], que ha de ser el contexto natural y lógico para esa operación jurídica.

En el marco de la ONU, la cooperación internacional no responde a un planteamiento global, sino sectorial[10], en el que destacan la lucha contra la ciberdelincuencia transnacional[11], el impulso a la sociedad de la información[12] y la

[8] CRAIGEN *et al* (2014) recopilan los diversos significados del concepto de ciberseguridad.

[9] Hay numerosas normas universales y regionales que regulan distintos aspectos del ciberespacio pero no hay una aproximación global a su régimen jurídico. La dificultad de alcanzar un acuerdo global se muestra, sin ir más lejos, en el Convenio sobre la ciberdelincuencia de 2001 de Budapest que ha sido ratificado por importantes países no europeos, incluyendo EEUU, y constituye una referencia para la regulación de este materia en otros sistemas regionales porque resulta más fácil trasladar este modelo que consensuar uno propio o consensuarlo a nivel general. Sobre este convenio puede verse MIQUELON-WEISMANN (2005), p. 329.

[10] MAURER (2011) explica las distintas líneas de actuación de la ONU.

[11] Este objetivo ha sido objeto de numerosas resoluciones de la AGNU, se gestiona a través de la Oficina de la ONU para las drogas y el crimen (UNODC) y ha desembocado en la inclusión de la lucha contra la cibercriminalidad en sucesivos Congresos Mundiales sobre Prevención del Delito y Justicia Penal (https://www.unodc.org/). Desde 1990 la AGNU está adoptando resoluciones contra el ciberdelito y en 1994 se publica un Manual sobre la prevención y el control de los delitos informáticos. El 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal tuvo lugar en Doha, del 12 la 19 de abril de 2015, con una destacada atención a la ciberdelincuencia (https://www.unodc.org/documents/congress//Documentation/IN_SESSION/ACONF222_L6_s_V1502123.pdf). La Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus Protocolos son un instrumento valioso a esos efectos por su alcance universal.

[12] El impulso a la sociedad de la información por parte de Naciones Unidas se ha traducido en las Cumbres Mundiales de la Sociedad de la Información (CMSI) (http://www.itu.int/net/wsis/index-es.html). La Cumbre de Ginebra de 2003

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

integración de las TIC en el desarrollo. Sin soslayar el valor de estas aportaciones, es indudable que la contribución esencial de la ONU en materia de ciberseguridad ha de ser impulsar la formación del consenso entre sus Estados miembros en relación con el mantenimiento de la paz y la seguridad internacional. Pero, por el momento, parece ser un objetivo difícilmente alcanzable. La Asamblea General de Naciones Unidas está canalizando los debates sobre la regulación internacional del ciberespacio desde varias perspectivas. Desde hace casi dos décadas se está trabajando en diversas líneas que van desde la presentaciones de observaciones individuales o conjuntas por parte de los Estados, hasta la elaboración de informes por Grupos de Expertos Gubernamentales[13]. El exiguo consenso alcanzado hasta ahora en esos trabajos se basa en dos postulados genéricos: la afirmación de la aplicación del Derecho internacional en vigor en el ciberespacio y la adopción progresiva de normas específicas que atiendan a su singularidad. Pero, precisamente, el problema reside en la dificultad de adoptar tales normas porque, como explica Sánchez de Rojas, coexisten tres cosmovisiones básicas y distintas de la ciberseguridad: la ciberliberal defensiva representada por la UE y los países europeos, la ciberliberal ofensiva abanderada por EEUU y la cibernacionalista-aislacionista de Rusia y China[14]. La idea misma de la soberanía cibernética, que está siendo acogida por un número creciente de Estados, pone de manifiesto que aún no se ha apreciado el cambio estructural que impone el ciberespacio a efectos de su ordenación jurídico-política.

---

adopta la "Declaración de Principios para Construir la Sociedad de la Información: un desafío global para el nuevo milenio" y el Plan de Acción de Ginebra. La Cumbre de Túnez en 2005 desemboca en el Compromiso de Túnez y en la Agenda de Túnez para la Sociedad de la Información. En Ginebra se adopta también la Agenda de Solidaridad Digital (https://www.itu.int/net/wsis/outcome/booklet/plan_action_D-es.html), que tiene por objeto fijar las condiciones necesarias para movilizar los recursos humanos, financieros y tecnológicos que permitan incluir a todos los individuos en la Sociedad de la Información mediante una estrecha cooperación nacional, regional e internacional entre todas las partes interesadas. El objetivo de superar la brecha digital exige utilizar con mayor eficiencia los enfoques y mecanismos existentes y, además, analizar otros nuevos para la financiación de infraestructuras y equipos y la creación de capacidades y contenidos que son indispensables para garantizar el acceso y la participación en la Sociedad de la Información.

[13] ROBLES (2016) explica esas diversas líneas de actuación y los resultados alcanzados, en particular, en los sucesivos Grupos de Expertos Gubernamentales.

[14] SÁNCHEZ DE ROJAS (2013) p. 262.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

El ciberespacio es, efectivamente, un espacio con una sustancia, una naturaleza y unos caracteres diferentes a los conocidos. Es artificial por ser el único creado por el hombre. Es virtual pero, también, físico porque depende del entramado material de sistemas y redes que le sirven de sustento y porque interacciona y se proyecta en el mundo no virtual. Es ilimitado, incluso infinito, en el sentido de no ser susceptible de delimitación espacial, material, funcional o temporal. Es universal, global, abierto, descentralizado y transnacional, transversal y esencialmente mutable. En una perversa paradoja, todo permanece de manera indefinida y todo cambia irremediablemente en el ciberespacio. Las coordenadas funcionales de tiempo y espacio, que han impuesto el ritmo y los límites en la evolución de la humanidad, operan de modo distinto en el ciberespacio[15]. La neutralidad, la popularidad y el anonimato son caracteres distintivos y definitorios del ciberespacio. Desde la perspectiva de la seguridad, es un escenario estratégico, táctico y operativo pero, a pesar de ser un campo de operaciones como la tierra, el mar o el aire[16], tiene algunas significativas particularidades que han llevado a su calificación como el quinto dominio[17]. Es un espacio capacitado para integrarse en esos otros espacios y condicionar su uso[18] y, además, evoluciona a una velocidad extraordinariamente mayor que los demás por su propia capacidad de expansión debida al desarrollo tecnológico y por su capilaridad en relación con el espacio físico[19].

Por todo ello, no es simplemente un espacio más[20], ni un *Global Commons* como los demás[21], sino que su verdadero signo distintivo radica en lo que se ha denominado su "esencia". Siguiendo a Gómez de Ágreda, esa esencia consiste en el modo en que altera las realidades de los otros dominios, su capacidad para interactuar con las otras realidades y modificar la percepción de las mismas y su

---

15 MIRÓ (2011) p. 6-7 realiza un extraordinario análisis de los cambios que impone el ciberespacio en ambas coordenadas.

16 SOFAER (2001) p. 239 identifica las similitudes entre el espacio aéreo y el cibernético y recurre a la OACI como modelo de referencia para la organización del ciberespacio.

17 JOYANES (2010) p. 29.

18 HATHAWAY *et al* (2012) aportan un apreciable análisis sobre el posible impacto de un ciberataque en el régimen jurídico del resto de los espacios.

19 TEPLINSKY (2013) p. 227: "Cyberspace touches practically everything and everyone".

20 OPDERBECK (2012) p. 797: "Cyberspace is as vulnerable as it is vital".

21 GÓMEZ DE ÁGREDA (2010) p. 53 y GÓMEZ DE ÁGREDA (2011) p. 1321.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

naturaleza como aglutinante catalizador que provoca alteraciones en los demás entornos y en la comprensión de los mismos[22].

El ciberespacio es, ante todo, un bien público[23] y global[24]. Esta categorización tiene una doble virtualidad: permite expresar la singularidad genética, funcional y sistémica del ciberespacio; y es, asimismo, un argumento concluyente para la definición de una *public policy* como opción de técnica y de política legislativa para su organización y gestión[25].

La sociedad internacional y los Estados, como responsables de su ordenación jurídica, no han apreciado suficientemente su naturaleza, ni sus efectos sobre el resto de los espacios y sobre la comunidad global[26]. El Derecho internacional se encuentra, por ello, en una encrucijada porque sigue operando sobre coordenadas y parámetros que, si antes estaban bien asentados[27], ahora se están viendo superados por una realidad difícilmente aprehensible, imparable en su progresión y, además, en buena medida imprevisible en cuanto a sus potencialidades. El ciberespacio implica un modelo diferente de sociedad en el que se cuestionan desde los paradigmas clásicos sobre seguridad y defensa, hasta los mecanismos de defensa de los derechos y libertades fundamentales. Exige, además, una cooperación internacional porque ningún Estado puede hacer frente aislada o

[22] GÓMEZ DE ÁGREDA (2013b) p. 2.

[23] ASLLANI *et al* (2013) p. 9.

[24] MOLINA (2015) p. 7: "Tal vez el Derecho tenga ya asumido como bienes dignos de protección jurídica muchos de los elementos materiales e inmateriales que componen el Ciberespacio, como es el caso de la información, la tecnología o ciertas relaciones humanas, pero no lo hace con el conjunto como realidad autónoma a pesar de que, desde todas las perspectivas, es reconocido como un activo indiscutible para la humanidad que demanda ser protegido legalmente".

[25] ASLLANI *et al* (2013) p. 9: "Approaching cybersecurity as a public good represents a sensitive starting point toward creating an appropriate legal framework. It justifies the role of federal, state, and local governments to implement policies and initiatives that improve the cybersecurity of individuals and organisations".

[26] LÓPEZ DE TURISO (2012) p. 120: En menos de una generación, "la informática ha pasado de ser una mera herramienta administrativa… a constituir un recurso estratégico nacional". Actualmente, como hace Estados Unidos, "considerar el ciberespacio como el centro de gravedad de una nación significa reconocer que constituye el centro neurálgico de todos los poderes del país, el ente del que todo depende".

[27] GÓMEZ DE ÁGREDA (2012) p. 180.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

individualmente a esta desafiante realidad[28]. Esa cooperación no sólo es indispensable, sino ineludible. No es una opción, no es una necesidad, es un imperativo. La respuesta jurídica no ha estado, sin embargo, a la altura del desafío.

2. La necesidad de una ordenación jurídica del ciberespacio

Desde la creación de Internet, en 1989, la evolución del ciberespacio se ha caracterizado por un progreso constante y un avance tecnológico inimaginable hace unas décadas más allá de la ficción. No ha ocurrido igual, sin embargo, con su ordenación socio-política y jurídica en el ámbito interno o en el internacional. En ambos niveles se ha procedido en una doble y complementaria dirección con un enfoque legislativo cambiante[29]: por una parte, la adaptación de la normativa en vigor y de las competencias de las organizaciones y organismos preexistentes para gestionar determinados ámbitos sectoriales del ciberespacio[30]; y, por otra parte, la creación de nuevas normas, estructuras o instituciones con finalidades específicas dentro del ciberespacio[31].

Ese doble proceso de adaptación de lo anterior y de generación *ex novo* de normas y estructuras institucionales ha tenido dos efectos perversos de carácter

---

[28] HEVERLY (2011) p. 1083.

[29] GONZÁLEZ CUSSAC (2010) p. 92: Hasta fechas recientes, "la ciberseguridad respondía a la exigencia de tutelar la información (*Information Security*), lo que determinaba un enfoque legislativo destinado a sancionar los accesos, usos, revelaciones, o daños ilícitos no autorizados. Sin embargo, en la actualidad, la evolución conduce hacia la gestión de riesgos del ciberespacio (*Information Assurance*) en la que los riesgos para la seguridad se encuentran vinculados al uso, procesamiento, almacenamiento y transmisión de información o datos, y los sistemas y procesos utilizados".

[30] Es el caso de organizaciones como la ONU, la UIT, la OCDE, la OSCE, la OEA, la UA, la UE o el Consejo de Europa, entre otras. Pueden consultarse ENRÍQUEZ (2012) p. 66; SYMANTEC (2014); WEGENER (2014) p. 1; PETRATOS en CARAYANNIS *et al* (2014) p. 279; EFTHYMIOPOULOS en CARAYANNIS *et al* (2014) p. 303. Un caso paradigmático es el de la OTAN que ha evolucionado desde la Cumbre de Praga de 2002 y espoleada en 2008 por la crisis de Estonia hacia la configuración de una política de ciberdefensa que tiene como centro de referencia doctrinal el Centro de Excelencia de Tallin de donde ha salido el Manual de Tallin. Sobre este proceso, SCHMITT (2012a) p. 13; KESSLER y WERNER (2013), p. 793; RAMÍREZ (2014) p. 1.

[31] Sobre la normativa universal, regional y nacional, UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2009); CONSEJO DE EUROPA (2013); OCDE (2012).

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

general: en primer lugar, una proliferación normativa inusual, innecesaria y escasamente útil, porque a las normas adaptadas se suman las nuevas, sin que las unas ni las otras cubran el vacío normativo de fondo que caracteriza el ciberespacio; y en segundo lugar, una multiplicación orgánica y estructural donde coexisten organizaciones, organismos, instituciones, agencias y foros[32], entre otros, con atribuciones concurrentes en el ciberespacio[33].

Más allá de la problemática estrictamente jurídica que genera esa situación, en términos de inseguridad, falta de transparencia o, incluso, de coherencia normativa, las consecuencias prácticas se están dejando sentir, quizás no de modo alarmante, pero sí inquietante: el crecimiento de la criminalidad cibernética y de la conflictividad socio-política en el ciberespacio constituye un auténtico problema que ha hecho de la ciberseguridad una de las preocupaciones esenciales tanto de los Estados y organizaciones internacionales, como de gestores de los sectores público y privado, incluyendo la sociedad civil. Ese fenómeno, bien conocido y documentado con multitud de estadísticas coincidentes en cuanto al aumento y la diversificación de las amenazas cibernéticas[34], incluida la mutación de las precibernéticas[35], se debe obviamente a las potencialidades de acceso y uso que ofrece el avance y el desarrollo tecnológico en el ámbito cibernético, pero también trae causa -y esto no se puede obviar- de la ausencia de un régimen normativo

[32] CANDAU (2010) p. 259 y PASTOR *et al* (2009) p. 1 tratan sobre los mecanismos creados en el marco nacional.

[33] GANUZA (2010) p. 167.

[34] Resulta ilustrativo, en ese sentido, el *European 2015 Cyber Risk Survey Report* (2015).

[35] La propia amenaza nuclear se manifiesta de un modo distinto porque ahora un ciberataque de origen imprevisible puede provocar una catástrofe de esa naturaleza. De hecho, la Organización Internacional de la Energía Atómica (OIEA) organizó del 1 al 5 de junio de 2015 una conferencia en colaboración con la Organización Internacional de Policía Criminal (INTERPOL), la Unión Internacional de Telecomunicaciones (UIT), el Instituto de Investigaciones de las Naciones Unidas para la Delincuencia y la Justicia (UNICRI) y la Comisión Electrotécnica Internacional (IEC), con más de 650 expertos de 92 países miembros y 17 organizaciones internacionales y regionales. El objetivo de la conferencia era ofrecer un espacio de diálogo para compartir información y fortalecer la cooperación en el marco de los esfuerzos globales para proteger las instalaciones y los materiales nucleares contra ataques cibernéticos.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

capacitado para la ordenación del ciberespacio[36]. El gran dinamismo de las TICS y la ausencia de reacción socio-política y jurídica son el caldo de cultivo para el crecimiento anómalo y desordenado del ciberespacio.

La dinámica normativa adaptación/creación *ex novo* que ha caracterizado la regulación del ciberespacio, tanto en el plano nacional como a nivel internacional, y curiosamente coincidente a pesar de las diferencias estructurales y funcionales entre esos ordenamientos jurídicos, es en parte responsable de los problemas de ciberseguridad donde confluyen desde la necesaria protección de datos personales, la propiedad intelectual o la protección de las infraestructuras críticas, hasta la lucha contra todas las variables de la criminalidad cibernética internacional.

Sin negar, ni infravalorar, la complejidad de esa tarea, especialmente en Derecho internacional donde se precisa el consenso de los Estados, en términos de política y de técnica jurídica se ha incurrido en tres carencias principales. Una primera ha sido combinar la técnica de adaptar las instituciones y normas preexistentes y de crear paralelamente normas y estructuras nuevas porque se podría haber optado por la primera o la segunda, que se justificaba además por la singularidad característica del ciberespacio, y porque, puestos a utilizar ambas, por la fuerza de los hechos o por necesidades de normación, el recurso por una u otra no ha respondido a un planteamiento previo coherente que justifique la elección de la adaptación o de la generación de nuevos marcos y estructuras jurídicas[37]. Una segunda deficiencia radica en que la regulación resultante de esa doble dinámica es sectorial, parcelada o fragmentada atendiendo a los ámbitos competenciales y a los sectores materiales presentes en el ciberespacio, que se ha realizado sin haber apreciado que no es simplemente un espacio más que se suma a los precedentes sino que, en realidad y sobre todo, es un espacio esencialmente diferente que interactúa y transversaliza a los anteriores, afectando a su

[36] Entre las múltiples disfunciones que se aprecian en la ordenación jurídica del ciberespacio se encuentran las derivadas de una errónea o inadecuada evaluación de las decisiones normativas antes de su adopción. Prueba de ello son las consecuencias de la decisión de expandir el número de dominios de nivel superior (gTLD), más allá de los genéricos y de los asignados a países, que ha provocado la proliferación de nuevos dominios compuestos de sitios utilizados para el spam, las estafas, la distribución de malware o los ataques cibercriminales. Véase, al respect, el informe BLUE COAT (2015).

[37] SHACKELFORD (2009) p 211: "before an international legal regime can be developed to deal with cyberattacks, the theoretical justifications for regulating cyberspace need to be considered".

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

naturaleza, estructura y funcionamiento como nunca antes había acontecido con los otros espacios sometidos a reglamentación jurídica. La tercera carencia de política y de técnica legislativa consiste precisamente en que esa aproximación sectorial o fragmentaria implica desconocer la realidad del desafío que plantea el ciberespacio que consiste precisamente en que impone un cambio estructural, inapreciable aún en cuanto a su alcance o consecuencias, pero evidente en cuanto a su naturaleza y a sus dimensiones estructurales.

Es cierto que ni la entidad ni la velocidad del avance tecnológico eran fácilmente previsibles y es incuestionable, asimismo, que el derecho como producto de la realidad social sigue una dinámica y unos procesos diferentes y generalmente posteriores al fenómeno que ha de regular. Pero también es verdad que no se está operando la diligencia requerida, ni se advierte la suficiente preocupación por sus carencias de orden jurídico.

La función primera del derecho como instrumento de racionalización de la vida en sociedad es garantizar la coexistencia y, a esos efectos, el desafío que impone el ciberespacio es fácilmente apreciable atendiendo a la naturaleza y el alcance de la llamada amenaza cibernética, si se entiende por tal el conjunto de acciones y situaciones que pueden suponer un riesgo o un peligro para la seguridad. En realidad, el concepto y la tipología de la amenaza se alteran en el ciberespacio hasta el extremo de que no cabe ya operar con categorías clásicas como la amenaza interna, exterior o de carácter internacional, la seguridad nacional o la seguridad ciudadana, el conflicto interestatal, asimétrico o híbrido o, incluso, la garantía última del pacto interestatal para garantizar la paz y la seguridad internacional.

La función principal del Derecho Internacional, tal y como se ha organizado desde el final de la II Guerra Mundial, sobre la base de la Carta de Naciones Unidas, se centra precisamente en garantizar el mantenimiento de la paz y la seguridad internacional. Ese modelo, creado por y para gestionar la seguridad entre Estados en un escenario protagonizado por ellos, resulta difícilmente extrapolable, tanto en términos operativos como de efectividad, a un contexto diferente y caracterizado porque los Estados no son los únicos actores[38], ni siquiera los más temibles, cuando se trata sobre las amenazas a la mera coexistencia y a la propia seguridad en el plano cibernético. Hay que preguntarse hasta qué punto el modelo interestatal de seguridad pactado en la Carta y que, con todas sus carencias, permanece estructuralmente inalterado desde entonces, puede servir en el ciberespacio cuando la amenaza a la seguridad es esencialmente distinta.

[38] NIKITAKOS y MAVROPOULOS en CARAYANNIS *et al* (2014) p. 259: "Cyberespace as a State's Element of Power".

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

II. La idiosincrasia de la amenaza cibernética

1. Un nuevo paradigma: La deslocalización de la amenaza

Desde mediados del siglo XX, el modelo tradicional de seguridad vinculado a la existencia, independencia e integridad territorial del Estado ha coexistido con otros paradigmas de seguridad que se han adicionado a aquel primero con objeto de dotarlo de un contenido material más amplio –seguridad económica, seguridad ideológica, seguridad alimentaria o seguridad medioambiental, entre otras- o que, directamente, han aspirado a sustituirlo como ocurre con el concepto de "seguridad humana". El ciberespacio impone un nuevo paradigma de seguridad que encaja directamente en el propósito y el efecto de sustitución, característico de la fórmula "seguridad humana", más que en el modelo de ampliación material del objeto y los contenidos de la seguridad. Pero, con una apreciable y significativa diferencia: la ciberseguridad se está imponiendo, más que como una opción, por la fuerza de los hechos o por un principio de efectividad, mientras que la seguridad humana se ha movido, más y generalmente, en el plano de los ideales que en el de las realidades. Es un prototipo de seguridad que está llamado a sustituir a su predecesor y debe ser capacitado a esos efectos en la medida en que ya lo está transversalizando, modificando sus parámetros funcionales y afectando a los estructurales hasta el punto de que no cabe hablar de un modelo de seguridad sin ciberseguridad porque ésta constituye, como el propio ciberespacio, un fenómeno multidimensional en lo económico, lo social y lo jurídico[39].

El ciberespacio impone un paradigma diferente porque cambia el concepto, la autoría, la motivación, los medios, la naturaleza, los objetivos y la exteriorización de la amenaza. La amenaza no es sólo física, ni cuantificable o cualificable por cantidad o entidad, ni uniforme, ni desde luego previsible porque se ha universalizado, multiplicado y diversificado hasta el punto de que resulta extremadamente difícil encajarla en categorías concretas que permitan articular los mecanismos adecuados para neutralizarla o eliminarla. Ni los Estados tienen la misma capacidad de mostrar su potencial con ánimo y efectos disuasorios o como argumento para la distensión[40], ni mantienen el monopolio de la violencia[41], ni

[39] ROBLES (2015a) p. 6.

[40] TAIPALE (2010) ofrece un estudio sobre la distensión en el ciberespacio.

[41] GÓMEZ DE ÁGREDA (2013a) p. 8: "El ciberespacio rompe, de alguna manera, el monopolio estatal sobre la violencia. Digo de alguna manera, porque la sociedad –así, en abstracto– sí se va acomodando al significado de la globalización, por mucho

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

tampoco los individuos se encuentran, como hasta ahora, fuera del paradigma interestatal de organización de la seguridad internacional que, mejor o peor, ha sido el indiscutiblemente imperante a lo largo de la historia del Estado moderno. Si la evolución de la conflictividad internacional ha obligado a reformular la idea de amenaza y a incorporar conceptos como las guerras híbridas o asimétricas, el desarrollo del ciberespacio conduce a la deslocalización última de la amenaza, que es el primer y principal obstáculo para garantizar la seguridad[42]. Ese fenómeno se manifiesta en el plano subjetivo, instrumental, funcional, material, espacial y teleológico.

La *deslocalización subjetiva* de la amenaza se produce por un doble motivo: porque cualquiera individualmente puede llegar a tener la capacidad de poner en riesgo la seguridad internacional[43] y porque, también, cualquiera, incluidos los Estados, pueden ser autores de acciones cibernéticas de naturaleza delictiva o criminal. El imperio del anonimato, el potencial igualador del ciberespacio[44], la problemática trazabilidad y la difícil operación de atribución de responsabilidad a los Estados se conjuran para convertir a los individuos en potenciales autores de actos contrarios a la legalidad internacional y a los Estados en potenciales autores de actos contrarios a la normativa de derecho interno, además de la internacional. En el plano cibernético, el Estado puede operar como un delincuente o un criminal, del mismo modo que el individuo puede actuar como un adversario bélico. Las probabilidades de ascenso del individuo al escenario de juego de la seguridad internacional se suman a las posibilidades de descenso del Estado al escenario de

---

que los Estados no lo hagan. Y la sociedad ya ha incorporado formas de violencia asimétrica que generan un impacto mucho más relevante del que corresponde a su potencia".

[42] ROBLES en OLARTE (2015b) p. 423.

[43] GÓMEZ DE ÁGREDA (2012) p. 180: el ciberespacio "vive en un *estado permanente de agresión* en el que todos los usuarios, sea cual sea su nivel, son susceptibles de recibir ataques con relativa independencia de su grado de protección". En su opinión, el efecto igualador que ejerce el ciberespacio sobre sus usuarios "amplía hasta el infinito el número de agresores potenciales mientras que las dificultades en la trazabilidad en tiempo real (o, al menos, útil) de dichos ataques hace que sus autores sean *relativamente invulnerables a medidas disuasorias*". En el mismo sentido, PADMANABHAN (2013) p. 288 y BOOTHBY (2013) p. 387.

[44] GÓMEZ DE ÁGREDA (2012) p. 176: el ciberespacio es "un elemento igualador de capacidades y reductor de asimetrías".

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

la pura y simple delincuencia o criminalidad[45]. Es un panorama distinto, adverso y desalentador en términos de seguridad interna e internacional.

La *deslocalización instrumental* viene dada porque no existe la opción de identificar todos los medios o instrumentos susceptibles de generar una amenaza[46] ni, tampoco, en consecuencia, de actuar normativamente respecto de ellos arbitrando normas y mecanismos para controlar su acceso y uso[47]. En las últimas décadas, el desarme y el control de armamentos se han materializado como un componente principal del modelo de seguridad de la ONU mediante numerosos procesos, negociaciones y acuerdos celebrados en un contexto alternativo de disuasión o distensión[48]. Sumándose a la deslocalización subjetiva, el avance tecnológico amplía constantemente los medios a disposición del cibernauta, consigue dotarlos de un efecto muy superior con consecuencias menos previsibles, obstaculiza su identificación porque pueden tener un uso polivalente, civil o militar, y, con todo ello, dificulta y limita extraordinariamente las posibilidades de control y regulación[49]. El "arma" cibernética no admite un modelo de gestión similar al que se ha articulado en materia de desarme y control de armamentos desde el final de la Segunda Guerra Mundial respecto del armamento utilizado en el mundo no virtual[50]. Ni siquiera está claro que ese componente seguritario pueda estar incluido dentro del modelo de seguridad del ciberespacio.

---

[45] En esa categoría podrían entrar los ciberataques destinados al espionaje comercial o industrial o al robo de datos personales con fines ilícitos detrás de los cuales se identifica con frecuencia a ciertos Estados.

[46] TIKK *et al* (2010) realizan un estudio muy completo de la diversidad de ciberataques.

[47] BOOTHBY (2013) p. 389: "a cyberweapon would comprise any computer equipment or computer device that is designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects".

[48] DÍAZ DEL RÍO (2010) p. 219: "la superioridad militar tradicional no constituye un factor de disuasión eficaz ni garantiza más seguridad automáticamente. Tampoco asegura una prevención efectiva… ni evita el riesgo de proliferación".

[49] Este fenómeno se advierte por dos motivos: uno, no existe la opción de precisar medios concretos susceptibles de generar una amenaza; y, dos, el avance tecnológico amplía los medios a disposición del agresor superando la dialéctica cívico/militar por disponer de ese doble uso y, además, consigue dotarlos de un efecto muy superior con consecuencias menos previsibles. Sobre este problema, JENSEN (2013) p. 198.

[50] ARIMATSU (2012) p. 91 analiza la posibilidad de un tratado al respecto.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

La *deslocalización funcional* resulta implícita porque, en ese contexto y con esas coordenadas, prácticamente cualquier actor y cualquier instrumento puede utilizar y ser utilizado, de modo respectivo, con una función indistinta o variable, lícita o ilícita, delictiva, criminal o bélica[51]. Una misma acción cibernética puede cumplir funciones diversas en función del autor, la intención, el destinatario y los efectos. La función asignada a la acción cibernética no conoce los límites que impone el mundo no virtual. En esa línea, desde la perspectiva de la seguridad, la *deslocalización material* se manifiesta por la dificultad para calificar esos actos cibernéticos como se ha hecho en el mundo físico con las categorías tradicionales operando con las distinciones entre la esfera civil y la militar o la seguridad interna y la defensa exterior, cuando, por ejemplo, un ciberataque a una infraestructura crítica puede ser un acto criminal, de espionaje, terrorista o directamente bélico[52].

La *deslocalización espacial* deriva del hecho de que la conflictividad social o política, interna, internacionalizada o internacional, deja de tener una adscripción clara en términos territoriales[53]. A efectos de su prevención, neutralización, investigación, persecución o sanción, la localización misma del ciberataque, su autoría, su itinerario, su destinatario y sus efectos siguen parámetros distintos a los de las acciones del mundo físico. En general, el problema de la trazabilidad es una constante en el mundo cibernético al que se suma el problema de la atribución de responsabilidad, en particular, a los sujetos de Derecho internacional[54]. No hay límites ni fronteras, no hay categorías claras como la delincuencia interna o transnacional, no hay un criterio delimitador de las competencias en materia de legislación o de ejercicio de la jurisdicción, no hay tampoco un escenario de guerra o una zona civil o neutral, no es siquiera fácil calificar un conflicto como interno o internacional[55].

---

[51] O'MALLEY (2013) p. 137 y JENSEN (2013) p. 199 explican la dificultad de apreciar la licitud o ilicitud de determinados actos ciberespaciales.

[52] FELIU (2012) p. 529: "El principal problema es definir e identificar en su caso si es ciberguerra, ciberespionaje o ciberterrorismo cuando se produce una ciberagresión. Es muy difícil identificar al agresor y decidir si se trata de una acción de guerra (*casus belli*), de un acto de terrorismo o de una acción criminal".

[53] LÓPEZ DE TURISO (2012) p. 139: "el ciberespacio extiende la zona de combate hasta el mismo corazón de la nación al ser capaz de entrar en cada una de las casas de los ciudadanos y de cortarle los suministros básicos que necesita para su supervivencia".

[54] SHACKERFORD y ANDRÉS (2011) p. 971.

[55] SCHMITT (2013) p. 233.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

Con todo esto se llega a la *deslocalización teleológica* que expresa la dificultad o, incluso, la imposibilidad de una identificación inmediata y clara de los objetivos de una acción ciberespacial. Un ciberataque puede tener como objetivo a quienes ofrecen el servicio o a sus destinatarios, a las instituciones y organismos responsables, incluso a los propios servidores, y puede realizarse con una finalidad simplemente activista o una intención destructiva[56].

La deslocalización de la amenaza desde la perspectiva subjetiva, instrumental, funcional, material, espacial y teleológica es un argumento definitivo para proceder a una ordenación jurídica global del ciberespacio, en sentido genérico y en términos de seguridad, como un imperativo para garantizar la coexistencia en la sociedad internacional. Ese proceso requiere un consenso político y un consenso social de base. El problema estriba en que se carece tanto del primero como del segundo, en gran medida, por una errónea y generalizada percepción del ciberespacio que impide reconocer el alcance y la entidad de la amenaza y de los riesgos de naturaleza cibernética.

2. Una percepción sesgada del ciberespacio

La evolución tecnológica encierra una curiosa paradoja antropológica y sociológica resultante del hecho de que, por una parte, con carácter general, el ser humano y la sociedad en su conjunto se han ido incorporando con cierta naturalidad y relativa rapidez a ese proceso, apreciando y aprovechando sus beneficios y asumiendo sus desventajas; pero, por otra parte, no se advierte una percepción o una consciencia clara de la realidad del ciberespacio y de sus consecuencias sobre el mundo no virtual. Hay dos fenómenos que muestran y, al tiempo, retroalimentan esa situación: la calificación del ciberespacio como el espacio virtual por oposición al espacio real, es decir, *materialmente opuestos*, y la concepción del ciberespacio como un mundo paralelo al mundo físico o real, esto es, *funcionalmente paralelos*.

La idea del ciberespacio como *realidad virtual* diferente de la realidad material del mundo precibernético, aunque encuentra su razón de ser en la naturaleza singular del ciberespacio, es errónea por tres motivos: en primer lugar, porque desconoce la realidad del espacio virtual que es real[57], aunque sea una realidad diferente de sus predecesoras y a pesar de que su singularidad genética y su artificialidad, por tratarse de un espacio creado por el hombre, aderezadas con

[56] Sobre esas distintas variables de un mismo acto, PÉREZ (2012) p. 265; URUEÑA (2015), p. 2; SÁNCHEZ (2012), p. 239; HATHAWAY *et al* (2012) p. 817.
[57] GÓMEZ DE ÁGREDA (2012) p. 172; COLLIER *et al* (2013) p. 469.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

la especulación imaginativa que suscita, parezcan apuntar en otra dirección[58]; en segundo lugar, porque desconoce el alcance y las consecuencias de la interacción que se produce entre el espacio cibernético y el resto de los dominios como consecuencia de la capilaridad característica del primero y de su capacidad para transversalizar a estos últimos; y, en tercer lugar, en un orden diferente de cuestiones, porque su existencia se sustenta por el momento en estructuras, aparatos y mecanismos físicos que son los que permiten el acceso y el uso del ciberespacio. Es, en definitiva, una realidad diferente y una realidad que altera estructural y funcionalmente al resto de las realidades.

La idea del ciberespacio como un *mundo paralelo* puede ser práctica, en términos de comprensión de ese dominio desde una perspectiva funcional, pero es igualmente errónea. Hay, en efecto, una inconsciente y generalizada percepción del ciberespacio como una realidad virtual paralela, la llamada *second life experience*, que se ha convertido en un cauce significativo de alimentación de la actividad ciberespacial y que ha servido de cobertura para su mitificación y rentabilización social y económica. El impacto de las relaciones sociales cibernéticas en términos cuantitativos y cualitativos es, en parte, consecuencia de esa concepción idílica[59], del mismo modo que, en un plano completamente distinto, un sector de la criminalidad cibernética parece ampararse en esa versión imaginaria que puede hacer creer que en el ciberespacio no son censurables o sancionables las mismas conductas que el espacio físico. En cualquier caso, la impronta del factor humano es esencial como demuestra el hecho de que, a pesar de los avances y complejidades de orden tecnológico, la ingeniería social constituye un componente

[58] MIRÓ (2011) p. 6: "se suele utilizar como sinónimo de ciberespacio el concepto de 'espacio virtual', como antitético al espacio 'real'. La simultaneidad, la unicidad de momentos, puede llevar a la impresión de que el ciberespacio es la ausencia de espacio, quizás fruto del equívoco de asimilar la idea de espacio a la de distancia. Evidentemente, el ciberespacio es real en el sentido de que existe, pero se trata de una `especie nueva´ de espacio, invisible a nuestros directos sentidos y en el que las coordenadas espacio-tiempo adquieren otro significado y ven redefinidos su alcance y límites".

[59] La prensa informa prácticamente a diario de sucesos o situaciones derivadas de este fenómeno. Así, entre otras, "La ilusión de Silicon Valley" (*El País*, 25 de octubre de 2015), "Una revolución con cibergoteras" (*Granada Hoy*, 24 de octubre de 2015), "Protecting the unprotectable: How do you spare the innocent in an online conflict?". Disponible en: <http://www.zdnet.com/article/cyberwar-how-do-you-spare-the-innocent-in-an-online-conflict/>. o "Los usuarios de internet todavía subestiman muchas ciberamenazas" (*ABC*, 16 de septiembre de 2015).

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

clave en el acceso y uso del ciberespacio y es uno de los principales objetivos y métodos de la cibercriminalidad[60].

Ambos fenómenos, realidad frente a virtualidad y mundo físico frente a apariencia paralela virtual[61], se encuentran profundamente enraizados en la conciencia colectiva y se manifiestan como una complicación adicional para su ordenación jurídica porque es más difícil generar el consenso social que sustenta el proceso de normación. Ni socialmente está interiorizada, en todas sus dimensiones y con todas sus consecuencias, la realidad del ciberespacio y su impronta en el resto de las realidades, ni jurídicamente se ha asumido el desafío de ordenar esas realidad atendiendo a sus caracteres propios[62]. Esta percepción sesgada, parcial y, en definitiva, errónea de la llamada realidad virtual tiene su reflejo en el mundo jurídico donde tampoco se advierte la entidad estructural del cambio que impone el ciberespacio. El problema aparece con la calificación misma de la conflictividad cibernética.

III. La calificación de la conflictividad cibernética

El ciberespacio rompe los parámetros tradicionales de comprensión de la conflictividad social y política a nivel interno y, también, internacional, englobando en esa expresión, a efectos prácticos, el conjunto de anomalías, disfunciones y situaciones que pueden suponer una ruptura o una quiebra de la normalidad en la convivencia política y social. El concepto mismo de conflicto armado, que es la expresión extrema de la violencia a la que puede conducir esa conflictividad, se altera en el ciberespacio[63]. La delincuencia y la criminalidad, el espionaje y el terrorismo, como manifestaciones prototípicas de la conflictividad socio-política, muestran también una dimensión diferente en el ciberespacio. El problema de fondo consiste, más allá de ese hecho, en la dificultad que implica la calificación misma de esas acciones, esto es, la adscripción de los ciberataques, como amenazas a la convivencia social, en cada una de esas categorías.

La amenaza cibernética se traduce material y funcionalmente en acciones que pueden ser calificadas como cibercriminalidad, ciberespionaje,

---

60 URUEÑA (2015) p. 3.

61 HEVERLY (2011) p. 1120: contrapone "Virtual Reality" frente a "Global Reality".

62 Esa falta de comprensión del alcance del cambio que implica el ciberespacio puede verse en la argumentación realizada por SOMMER (2000) p. 1145. Sobre la necesidad precisamente de apreciarlo, LESSIG (1999-2000) p. 501.

63 RABOIN (2011) p. 601 y SCHMITT (2012b) p. 283.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

ciberterrorismo o ciberguerra[64]. Un ciberataque puede encajar en cualquiera de esas categorías porque un mismo acto puede cumplir todas esas funcionalidades. La adscripción de ese acto dentro de esa tipología depende no sólo del acto mismo[65] sino, también y sobre todo, de los sujetos, la intención y los efectos. Hay, incluso, la posibilidad de que sea una simple manifestación de ciberactivismo[66]. No es ésta la única dificultad que plantea la gestión de las ciberamenazas.

Un problema adicional, y no de menor entidad, radica en que, aunque parezcan una reproducción de sus homólogas en el espacio físico, las acciones cibernéticas tienen una singularidad propia que va más allá de su localización en el mundo cibernético. Precisamente, por ello, carece de justificación y hasta de sentido gestionarlas mediante una traslación mecánica de las normas, procedimientos y mecanismos creados para el mundo precibernético. La criminalidad cibernética no es igual a la criminalidad física, como tampoco lo son el ciberespionaje, el ciberterrorismo o la ciberguerra.

1. Cibercriminalidad

La cibercriminalidad reúne algunas características que la distancian de la criminalidad del mundo no virtual[67]. En primer lugar, la especificidad del delito cibernético deriva de que ha de realizarse en, desde o mediante el espacio cibernético por lo que la posibilidad de acceso a dicho espacio es *conditio sine qua non* para su comisión[68]. En segundo término, es un fenómeno delictivo que no está acotado territorialmente, ni se puede caracterizar por parámetros clásicos de orden general dependientes del nivel de desarrollo, la política, la raza, la cultura, la religión o cualquier otro. En tercer lugar, la ciberdelincuencia no responde tampoco a parámetros tradicionales individualizados sobre autores y víctimas y

[64] Las amenazas cibernéticas y su adscripción a categorías delictivas son explicadas por PÉREZ (2012) p. 265; URUEÑA (2015) p. 1; SÁNCHEZ (2013) p. 115; HATHAWAY *et al* (2012) p. 817.

[65] FELIU (2012) p. 529.

[66] O'MALLEY (2013) p. 140.

[67] GUTIÉRREZ (2005) p. 69 expone las características especiales de la criminalidad cibernética.

[68] SALOM (2010) p. 137: puede ocurrir que "conductas que hasta entonces existían en el mundo real, pasan a ser conductas prácticamente exclusivas del mundo virtual (…) Incluso ha sido el medio tecnológico lo que ha fomentado el delito, pasando de ser una conducta esporádica en el mundo real, a un delito muy repetido en el mundo virtual".

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

sobre sus mayores o menores amenazas o riesgos. Con el anonimato y la globalidad, cualquiera puede ser autor o acabar siendo víctima[69]. Con su deslocalización temporal y espacial, son impredecibles e incontrolables el momento y el lugar de comisión del acto delictivo o criminal. Por último, es una actividad genética y naturalmente global y transnacional a diferencia de la delincuencia no cibernética que puede ser local, nacional o internacional, pero no siempre y necesariamente lo último como ocurre, generalmente por su propia naturaleza, con la que se produce en el ciberespacio.

Además de estas particularidades, la cibercriminalidad tiene dos significativas señas de identidad: por una parte, muestra un crecimiento exponencial realmente alarmante sobre el que coinciden todas las estadísticas, aun cuando, por distintos motivos, no llega a trasladar el fenómeno en su totalidad[70]; y, por otra parte, se materializa como una nueva amenaza global no sólo por la expansión de sus efectos en el tiempo y el espacio que permite el ciberespacio, sino también porque se ha convertido en un nuevo medio utilizado por o a disposición de los Estados para encauzar la conflictividad internacional[71]. En algunos medios políticos, la cibercriminalidad ha llegado a ser calificada como una preocupación cercana a la que genera el terrorismo.

2. Ciberterrorismo

[69] LIPTON (2011) p. 1103 se ocupa de este problema.

[70] ROBLES (2015a) p. 11: Hay dos motivos principales que explican la dificultad de cuantificar la cibercriminalidad: por una parte, el tráfico no controlado en la *darknet* y la *deep web* y, por otra, lo que se denomina el dilema del iceberg consistente en que no se denuncian todos los delitos sino sólo una parte proporcionalmente mínima de los delitos reales. Ello es debido a la combinación de una doble circunstancia: de un lado, lo que se podría denominar el "microdelito", que se caracteriza como una actividad delictiva destinada a la obtención de un beneficio, dirigida a una multitud de víctimas y traducida en un perjuicio económico mínimo para cada una de ellas individualmente, razón por la cual generalmente no es objeto de denuncia; y, de otro lado, la macrodelincuencia, dirigida a grandes empresas, marcas y sociedades que no denuncian para evitar la pérdida de prestigio que supondría la difusión de sus brechas de seguridad y las pérdidas económicas colaterales.

[71] SIERS (2014) p. 1 explica el caso de Corea del Norte y LAI y RAHMAN (2012) p. 38 hacen lo propio con China.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

El ciberterrorismo es una amenaza diferente del terrorismo que, además, supera la dicotomía clásica entre terrorismo interno y terrorismo internacional porque es, por naturaleza, global y dispone de una proyección universal[72]. Los objetivos del ciberterrorismo, que son considerablemente más amplios que los del terrorismo no virtual[73], se puedan clasificar en dos categorías generales: funcionales y operativos.

Los objetivos y actividades funcionales son aquéllos que contribuyen al mantenimiento, funcionamiento y desarrollo de la organización terrorista como ocurre con la búsqueda de financiación, la propaganda y el adoctrinamiento[74], el reclutamiento y entrenamiento[75] y la comunicación e interconexión entre sus agentes y células. Por su parte, las acciones y funciones de carácter operativo del ciberterrorismo incluyen la búsqueda de información sobre posibles objetivos terroristas, la coordinación y ejecución de acciones[76] y la guerra psicológica[77].

El ciberespacio ha supuesto una alteración estructural en la organización y el funcionamiento de los grupos terroristas y en el rumbo y la dinámica misma de esta actividad criminal, que en poco o en nada se parece a su homólogo no virtual[78], razón por la cual difícilmente se puede luchar contra la misma operando desde los parámetros creados para actuar frente al terrorismo convencional[79].

---

[72] BILLER (2013) p. 275 se ocupa del concepto de ciberterrorismo.

[73] WESTBY (2006-2007) p. 297.

[74] DEREK (2009-2010) p. 577 explica esos usos de la red.

[75] WEIMANN (2005) p. 129 trata especialmente sobre ello.

[76] SIBONI *et al* (2013) p. 3 subrayan que la coordinación se facilita mediante la comunicación a través de Internet con todas sus ventajas en términos de inmediatez y proyección.

[77] La globalidad cibernética, el anonimato y la ausencia, en general, de controles sobre sus contenidos, en particular, en zonas como la *Darknet* o la *Deep Web*, permiten el uso de este medio sin censura para divulgar imágenes, propagar informaciones tergiversadas o lanzar amenazar. Con ello se consigue, asimismo, trasmitir una imagen interna idealista de cohesión, fortaleza y pujanza y sus mensajes están alcanzando un impacto global.

[78] STOCKTON y GOLABEK-GOLDMAN (2014) p. 211; PAREJA en GARCÍA y RODRIGO (2008) p. 57.

[79] DOGRUL *et al* (2011) defienden en su monografía con distintos argumentos la necesidad de reactivar la cooperación internacional a esos efectos. STOCKTON y GOLABEK-GOLDMAN (2014) p. 211 y TEHRANI y MANAP (2013) p. 689 advierten sobre los problemas que plantea una aproximación convencional al ciberterrorismo.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

3. Ciberespionaje

El ciberespionaje es una actividad que supera material, funcional y teleológicamente al espionaje porque éste se circunscribe generalmente a la obtención de información, mientras que aquel comprende, asimismo, la manipulación, gestión, alteración o destrucción que son más factibles en el medio cibernético y con menos límites y riesgos que en el mundo físico. Los medios y técnicas utilizados se pueden asemejar con excesiva frecuencia a los utilizados en el mundo de la cibercriminalidad[80].

El ciberespionaje es también una actividad que ha difuminado los límites entre el espionaje político y el comercial o el industrial y que, además, se extiende a ámbitos personales usados con fines ilícitos[81]. Es, asimismo, un actividad en la que han cobrado protagonismo las acciones de individuos o grupos activistas internacionales que, a su vez, han tenido un fuerte impacto en las relaciones diplomáticas de los principales países del mundo[82]. No debe resultar extraño. La capacidad de obtención de información a través del ciberespionaje es inversamente proporcional a la garantía de respeto de ciertos principios básicos de las relaciones internacionales y, también, y no menos importante, a la garantía de respeto de determinados derechos y libertades individuales de las personas.

La magnitud del ciberespionaje, si se compara con el espionaje no cibernético, es fácilmente contrastable. Sin ir más lejos, el Sistema Echelon, creado entre EEUU, Gran Bretaña, Canadá, Australia y Nueva Zelanda, es un sistema automatizado de interceptación global de las comunicaciones que ha pasado de una vocación concreta a una finalidad global[83]. Es conocido gracias al espionaje industrial porque han sido los intereses económicos de los países implicados y de las multinacionales quienes han llevado este sistema al debate público. El sistema "Enfopol" es la respuesta europea con un plan propio de interceptación de telecomunicaciones que no está exento de polémica en una estructura regional como la UE que parece abanderar la protección de datos personales y en la que algunos de sus líderes políticos se han significado victimizados por el ciberespionaje ajeno. Los sistemas "Carnivore", "Cyber Knight", "Magic Lantern" son modalidades diferentes de control de la información y las comunicaciones con idénticos o mayores niveles de efectividad que prueban las enormes dimensiones de esta actividad.

---

[80] SÁNCHEZ (2013) p. 115 ejemplifica este fenómeno.
[81] HARTNETT (2011) p. 411.
[82] MAROTO (2009) p. 45.
[83] SÁNCHEZ (2012) p. 253.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

En la práctica, los argumentos de seguridad interna o internacional que justifican estas actividades han avalado un crecimiento desordenado y posiblemente excesivo de las mismas que difícilmente puede ser compatible con el respeto de derechos y libertades fundamentales como el derecho a la intimidad, la privacidad, el secreto de las comunicaciones o la protección de datos personales o nuevos derechos como el derecho al olvido o al anonimato.

4. Ciberguerra

En términos militares, también, el ciberespacio constituye un escenario táctico, estratégico y operativo claramente diferente de los espacios terrestre, marítimo, aéreo y exterior. Pero es un ámbito con un uso y una categorización jurídica complejos desde la perspectiva ciberbélica por un doble motivo: por una parte, no es posible un ejercicio de apropiación, en general y como parte del desarrollo de la hostilidades; y, por otra parte, es un espacio ontológicamente único, global, infinito y artificial que interactúa y transversaliza el resto de los espacios. Por ambos razones, principalmente, supone un cambio esencial de escenario desde la perspectiva del conflicto armado.

El ciberespacio se ha convertido, como explica López de Turiso, "en la primera línea de batalla, el primer escenario de combate de cualquier acción bélica moderna, por delante de las acciones realizadas en los escenarios tradicionales"[84]. Raboin afirma que "the emergence of Cyber warfare is more than just another evolutionary step in the development of wartime strategy and methodology; (…) it represents a fundamental transformation in the very nature of the concept of war itself. The notion that cyber warfare will alter the inherent nature of war is ultimately rooted in the conceptual idea that cyber warfare does not merely change the weaponry of modern wars, but that it represents a radical shift in the nature of the wartime battlefield"[85]. La ciberguerra se manifiesta, además, como el escenario presente y futuro de conflicto[86]. Como respuesta, la ciberdefensa

[84] LÓPEZ DE TURISO (2012) p. 139.

[85] RABOIN (2011) p. 604: "Whereas every historical evolution of warfare has occurred within the common sphere of the physical, tangible world, cyber warfare redefines the central wartime battlefield. Yet, the consequences of actions within this new Cyber warfare battlefield are unique because although they occur in the intangible domain of computer networks and information streams, the effects of the actions taken within that domain have very "real" effects in the physical world of our everyday reality".

[86] JURICH (2008-2008) p. 275.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

comprende todas las acciones y medidas necesarias para garantizar la ciberseguridad entendida como la seguridad de todos, civiles y militares, públicos y privados[87].

En poco más de dos décadas, el uso del ciberespacio ha demostrado que la idea de conflicto armado ha dejado de ser la tradicional en términos de actores, medios, escenarios y objetivos, para dar paso a nuevas modalidades y coordenadas, más complejas por un doble motivo: imponen una mecánica nueva y alteran las dinámicas preexistentes que se ven transversalizadas por la impronta del ciberespacio.

En definitiva, la revolución tecnológica ha facilitado el desarrollo de la criminalidad cibernética y de la conflictividad socio-política transnacional en todas sus modalidades pues se ha visto doblemente favorecida, de un lado, por las ventajas de la globalización cibernética y, de otro lado, por las carencias de la respuesta jurídica a nivel legislativo, policial y judicial que se ha mostrado insuficiente para prevenirla, neutralizarla, reprimirla o erradicarla. Esa respuesta ha de estar a la altura del desafío y ha de ser una solución global desde el Derecho internacional. La necesidad de regular el ciberespacio para acabar con esa situación se enfrenta a numerosos obstáculos de naturaleza técnica y jurídica. Pero la problemática de fondo que encierra su ordenación jurídica se explica, también y no en menor medida, por una limitada, parcial y, en cualquier caso, cuestionable asunción de sus efectos sobre el derecho y, en particular, sobre los modelos de organización interna e internacional.

IV. La impronta del ciberespacio en el derecho

El ciberespacio afecta a los modelos de convivencia y de organización política y social pero, por diversos motivos, ese presupuesto no ha sido suficientemente apreciado y no se ha traducido en términos jurídicos. Esa situación se manifiesta, en particular, en el modelo de seguridad de la sociedad internacional y en el modelo de organización jurídico-política configurado en torno al Estado y al derecho del Estado.

1. El modelo de seguridad internacional

Desde el final de la Segunda Guerra Mundial, con la Carta de Naciones Unidas, el orden jurídico internacional se ha construido sobre la base de unos principios estructurales vertebradores de un modelo en el que el uso y la amenaza de la

[87] PASTOR (2012) p. 212.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

fuerza es objeto, por una parte, de una prohibición genérica que sólo admite como excepción la legítima defensa en los términos expuestos en el Artículo 51 de la Carta; y es, por otra parte, una prerrogativa del Consejo de Seguridad, como expresión definitiva del alcance de su responsabilidad en materia de mantenimiento de la paz y la seguridad internacionales.

Desde hace tiempo, la amenaza o el uso de la fuerza cibernética es un hecho que se ha advertido de formas diferentes pero, en cualquier caso, de modo constante y en crecimiento. En estos años, la experiencia cibernética muestra el alcance y la profundidad de los cambios que introduce el acceso y uso del ataque cibernético en el modelo de seguridad y permite distinguir cuatro categorías diferentes de recurso al medio cibernético: el uso clandestino del arma cibernética, el uso paralelo del ciberataque y del armamento tradicional, el uso combinado de ambos y, por último, el uso del ciberataque como alternativa a la acción militar convencional.

A) El concepto de *uso clandestino* del arma cibernética permite catalogar aquellas situaciones en las que el ciberataque se ha utilizado subrepticiamente enmascarando un ataque o conflicto real entre Estados que no se manifiesta abiertamente como tal y se circunscribe a acciones en el ciberespacio. El caso de los ataques a Estonia en 2007 ejemplifica esta modalidad de uso[88], cuyo valor, en términos operativos y de eficacia, reside en la protección combinada que ofrecen el anonimato y el activismo en la Red, la problemática que plantea la trazabilidad y la

[88] El asunto del Soldado de Bronce es el detonante de estos ciberataques respecto de los que, a pesar de la convicción generalizada, no ha podido ser demostrada la implicación de Rusia. El Soldado de Bronce encierra un simbolismo contradictorio porque mientras que para los rusos constituye un monumento a los libertadores de Tallin durante la Segunda Guerra Mundial, en cambio, para los estonios no deja de ser la representación de la dominación soviética. En 2007, el traslado de la estatua al Cementerio militar de las Fuerzas de Defensa estonias tiene como respuesta una sucesión de ciberataques en forma de Denegación de Servicio y Denegación Distribuida de Servicio dirigidos al conjunto de webs, redes y servicios estatales, afectando prácticamente al 100% de las mismas, así como a los servicios de *e-banking* con un porcentaje de incidencia en torno al 90% de las transacciones bancarias. Estonia es un país especialmente vulnerable por su gran dependencia de las TIC, tiene unas dimensiones reducidas y es miembro de la OTAN. Por todo ello, un ciberataque masivo puede provocar una situación de crisis de seguridad nacional y puede, también, ser la vía para contrastar la capacidad cibernética de la Alianza Atlántica. HATHAWAY *et al* (2012) p. 817 y GANUZA (2010) p. 167 se refieren a este caso.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

atribución de responsabilidad al Estado por los hechos individuales y, en definitiva, la opacidad que facilita la tecnología. El resultado es que un conjunto de ciberataques, sin responsable último aparente, puedan llegar a colapsar la estructura de un Estado convirtiéndose en una amenaza potencialmente mayor y más grave que un ataque armado, pero no puede demostrarse su autoría real, ni calificarse como un acto bélico[89].

La experiencia de Estonia como ejemplo del uso clandestino del medio cibernético permite extraer importantes conclusiones. En primer lugar, es la evidencia de que la amenaza cibernética es real y muy atractiva para causar un gran daño con un mínimo riesgo. En segundo lugar, sirve para demostrar la imposibilidad de reaccionar aisladamente y la necesidad de una cooperación internacional para frenar un ataque cibernético[90]. En tercer lugar, es una prueba de la impunidad del ciberataque porque no se puede probar la implicación de Rusia y de los ciudadanos rusos[91]. Para terminar, demuestra que la amenaza cibernética no sólo puede afectar al normal desenvolvimiento de la vida de los ciudadanos de un país, sino que puede atacar su estructura y las infraestructuras críticas nacionales que, además de provocar daños materiales, pueden conllevar asimismo el riesgo de daños físicos para la población.

B) El modelo de *uso paralelo* de acciones convencionales y cibernéticas engloba aquellas acciones cibernéticas desarrolladas de modo paralelo a la acción militar pero sin una conexión estratégica, operativa o táctica en términos militares entre ambas. La acción cibernética no tiene una incidencia directa en el teatro de operaciones o en el dispositivo militar, sino que se concreta en la realización de ciberataques que favorecen a alguna de las partes por el impacto psicológico que conlleva en el desarrollo del conflicto. El ejemplo se encuentra en 2008 en Georgia[92].

---

[89] Sobre la dificultad de calificar los ciberataques en el caso de Estonia como cibercrimen, ciberterrorismo o ciberguerra, SHACKELFORD (2009) p. 232.

[90] WEISSBRODT (2013) p. 347.

[91] La implicación de Rusia y de ciudadanos rusos en los ataques parece no ofrecer dudas por las evidencias prácticas -el tráfico malicioso en lengua rusa o las instrucciones para realizar los ciberataques contenidas en foros, blogs y sitios web rusos-, y por la actitud de las autoridades rusas.

[92] En 2008, Georgia es un país poco dependiente de las TIC, circunstancia ésta que, en términos positivos, lo hace menos vulnerable a los ciberataques y, en sentido negativo, limita también su capacidad de respuesta. El conflicto con Rusia surge por la situación de Osetia del Sur que es un territorio situado en el Cáucaso en la frontera común. En el contexto del conflicto armado, en paralelo a las operaciones

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

La experiencia de los casos de Georgia y Estonia sirve para demostrar la inviabilidad de una respuesta individual frente al ciberataque, la necesidad ineludible de una cooperación internacional y la imposibilidad de acreditar la implicación rusa. Pero, al tratarse de un uso diferente del ciberataque, el caso de Georgia permite extraer conclusiones adicionales que particularizan este supuesto. En primer lugar, en la medida en que las ciberoperaciones están bien planificadas, organizadas y coordinadas en tiempo y espacio con las acciones cinéticas, el ciberataque se convierte en un componente adicional a las operaciones militares[93]. En segundo lugar, el objetivo del ciberataque consiste esencialmente en debilitar la capacidad de respuesta militar y política de Georgia, mediante operaciones psicológicas y propagandísticas. En tercer lugar, la autoría de los ciberataques corresponde a voluntarios que actúan desde diversas localizaciones, dificultando la trazabilidad y la atribución de responsabilidad al Estado, por los hechos cometidos por esos particulares. Los autores no tienen el estatuto de combatientes, ni se les aplican las normas del Derecho Internacional de los Conflictos Armados, a pesar de que, por tratarse de ciberataques en un contexto de conflicto armado, deberían estar sometidos a ese régimen jurídico. Esta situación se reproduce agravada cuando se trata del uso combinado y no sólo del paralelo como en Georgia.

C) El *uso combinado* de la acción cibernética y de la acción militar convencional es una modalidad claramente diferenciada del uso paralelo porque la acción cibernética está integrada en el dispositivo militar en términos estratégicos, tácticos y/o operativos. En este caso, la acción ciberespacial afecta, condiciona, permite o facilita la operación militar convencional, que no sería posible con los mismos parámetros y con idéntica secuencia sin la fase previa cibernética. En esta categoría se sitúan la Operación Huerto[94] y la Operación Gerónimo[95]. En ambos

---

militares y coincidiendo en intensidad y frecuencia con ellas, se producen los ciberataques. La respuesta técnica y política es posible gracias al apoyo internacional recibido por Georgia y avalado por la experiencia previa de Estonia y, también, de Lituania. Sobre este asunto se pronuncian GILES en CZOSSECK *et al* (2011), p. 45; GANUZA (2010) p. 195.

93 En mi opinión, se trata de un componente adicional que justifica su calificación como uso paralelo GILL y DUCHEINE (2013) p. 461 definen esta modalidad como uso combinado porque no establecen otras categorías, ni distinguen entre usos combinado y paralelo.

94 La Operación Huerto consiste en un ataque aéreo israelí sobre un objetivo conocido por los sirios con el nombre clave de Al-Kibar en 2007. La particularidad de este caso radica en que, para llevar a cabo la operación, se utilizó un sistema tecnológico similar al Suter, desarrollado por EEUU, mediante el cual los aviones

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

casos, el ciberataque es parte integrante de una operación militar y factor determinante en la organización y en el éxito de la misión porque, de no haber existido, el resultado habría sido completamente distinto en términos de riesgos y de efectividad. El problema estriba en la más que cuestionable legalidad de esas operaciones desde la perspectiva general del Derecho internacional. La acción unilateral de un Estado violando el principio de soberanía territorial y la jurisdicción de otro Estado, interfiriendo en sus estructuras de control para neutralizarlas o inutilizarlas y, además, no menos importante, infringiendo daños materiales y/o personales es posible, en ambos casos, gracias a una acción cibernética que ha garantizado la consecución del objetivo militar. En esta misma dinámica se sitúa el uso del ciberataque como alternativa frente a la acción militar tradicional.

D) El uso de la acción cibernética como *alternativa* a la acción militar convencional es la expresión definitiva del cambio de parámetros que implica el ciberespacio. La manifestación sobresaliente de este uso es el asunto Stuxnet[96],

---

de combate de la Fuerza Aérea Israelí penetran en el espacio aéreo sirio sin ser detectados por radar. Aunque hay varias teorías, la explicación más convincente apunta que, con ese sistema, se manipula la señal recibida por los radares enemigos, mostrando en sus sensores objetivos falsos, de manera que permite invadir las redes de comunicaciones, ver los sensores del enemigo y controlarlos para alterar la información detectada por los radares.

[95] El contexto en el que se produce la Operación Gerónimo es conocido. Desde los ataques a las Torres Gemelas, el 11 de septiembre de 2001, la detención de Osama Bin Laden constituye una prioridad para EEUU que justifica, como es sabido, la acción contra los talibán en Afganistán. Una década después, el 1 de mayo de 2011, unidades de élite de las fuerzas militares de EEUU abaten a Bin Laden en el transcurso de un tiroteo en Abbottabad, en Pakistán. La operación es posible porque la defensa aérea paquistaní no puede detectar la presencia de los helicópteros de las fuerzas estadounidenses en su espacio aéreo. Al parecer, ello se debe a que los programadores y hackers estacionados en el Comando Cibernético de Estados Unidos en Fort Meade, en Maryland, facilitan la incursión usando la tecnología cibernética para infiltrarse y apagar el sistema de defensa aérea de Pakistán impidiéndole identificar el asalto físico de las unidades enviadas por EEUU. Sobre este caso MOORE (2013) p. 223.

[96] En el origen de este asunto se encuentra la sospecha de que Irán estaba desarrollando un programa nuclear incompatible con el Tratado de No Proliferación de Armas Nucleares que amenaza con desestabilizar la región, atenazada ya por la situación en Israel y la tensión con Arabia Saudita. En 2010,

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

que ha sido calificado como el primer ejemplo de guerra cibernética o como un misil cibernético de precisión de carácter militar. En este caso, el ciberataque se utiliza como alternativa a una acción armada convencional y demuestra su enorme eficacia porque cumple su función eficazmente sin ser detectado y porque, aunque se sospecha de Israel y de EEUU, la imposibilidad de demostrar la autoría dificulta la adopción de contramedidas o limita la capacidad de reacción del Estado afectado. En un sector doctrinal se ha barajado la opción del ciberataque como un ejercicio de legítima defensa anticipada[97]. Desde una posición jurídicamente más sólida se ha analizado como un supuesto de uso de la fuerza[98]. El problema estriba en que la ausencia de una normativa específica para el ciberespacio y las carencias de la aplicación analógica de la normativa creada para el mundo no virtual contribuyen a una indefinición jurídica peligrosa, inquietante y, desde luego, a estas alturas, injustificable.

La experiencia sobre el uso del medio cibernético muestra el alcance del cambio y presagia un futuro marcado por el protagonismo creciente del arma cibernética en detrimento de los medios tradicionales. La doctrina se esfuerza por explicar este fenómeno sobre la base de la normativa en vigor y desde el modelo de seguridad vigente operando mediante una extrapolación o una aplicación analógica[99], que, difícilmente, pueden satisfacer la necesidad creciente de un acuerdo político y de una reglamentación normativa que permita la reordenación del modelo de seguridad internacional en este diferente contexto.

Irán sufre un ataque informático contra sus instalaciones nucleares que se considera entonces el ataque cibernético más grande de la historia. Los sistemas de control de la central nuclear de Bushehr, así como de otras industrias, se ven afectados por un virus con una potencia sin precedentes, denominado Stuxnet. Se trata de un virus muy sofisticado que utiliza técnicas de rootkit para instalarse en el sistema operativo. Una vez dentro de una planta, puede reprogramar las centrifugadoras para hacerlas fallar sin ser detectado y es el primer virus capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas.

[97] GILL y DUCHAINE (2013) p. 471.

[98] WEISSBRODT (2013) p. 378.

[99] Las dificultades para aplicar la normativa de los conflictos armados es analizada por BOOTHBY (2013) p. 387; RABOIN (2011) p. 601; SCHMITT (2014) p. 269; GERVAIS (2012), p. 525; SHACKERFORD y ANDRÉS (2011) p. 971. Sobre la aplicación del principio de prohibición del uso o de la amenaza de la fuerza, DAS (2015) p. 120; GRAHAM (2010) p. 87. Sobre la aplicación de los artículos 4, 5 y 6 del Tratado del Atlántico Norte en caso de ciberataques, GANUZA (2010) p. 208.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

El modelo de seguridad global que sustenta la organización de la sociedad internacional ha de ser reformulado para adaptarse al cambio de circunstancias que implica el ciberespacio y su uso en términos de seguridad internacional. Pero, para ello, también es preciso plantearse en qué medida el ciberespacio puede afectar a los propios modelos de organización jurídico-política.

2. El modelo de organización jurídico-política

En un artículo titulado *Regulating Cyber-Security*, haciéndose eco de una opinión doctrinal generalizada, Sales advierte que "the law and policy of cyber-security are undertheorized. Virtually all legal scholarship approaches cyber-security from the standpoint of the criminal law or the law of armed conflict. Given these analytical commitments, it is inevitable that academics and lawmakers will tend to favor law enforcement and military solutions to cyber-security problems. These are important perspectives, but cyber-security scholarship need not run in such narrow channels. An entirely new approach is needed"[100].

La aproximación jurídica al ciberespacio se ha caracterizado, en efecto, en términos generales, por estar focalizada en el derecho penal o en el derecho de los conflictos armados, desplazando de su lugar natural al resto de los sectores del ordenamiento jurídico. Por la fuerza de los hechos, por pura mecánica o por necesidad, el papel de esos sectores del ordenamiento jurídico ha sido mayor y prácticamente protagónico en el ciberespacio cuando ambos deben ser, por principio, un último recurso. Aunque es necesario que el modelo jurídico del ciberespacio se sitúe en un contexto normativo global, natural y normalizado[101], superando esa dinámica convencional originaria, aún es más urgente que esa operación se realice aceptando que no se trata sólo de un mero desplazamiento del núcleo normativo hacia el centro desde los extremos que significan el derecho penal o el derecho de los conflictos armados. Hay que adoptar una aproximación conceptual y metodológica capacitada para asumir la trascendencia del desafío. El punto de partida es sencillo: si el ciberespacio ha terminado con las coordenadas de tiempo y espacio, tal y como se han conocido hasta ahora, siendo como son parámetros relativamente físicos y objetivos, ¿qué no hará con las fronteras de los Estados y con sus competencias territoriales que son una creación socio-política y jurídica?

La combinación de una errónea percepción socio-psicológica del ciberespacio y de una gestión jurídica basada en la aplicación analógica del derecho, y centrada

[100] SALES (2013) p. 1507.
[101] MOLINA (2015) p. 7.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

en los ámbitos penales, lleva a una situación en la que se está obviando el problema principal que es de orden constitucional, esto es: la falta de reconocimiento de los efectos y la asunción de las consecuencias del ciberespacio sobre las modalidades de organización política, social y jurídica imperantes a lo largo de la historia de la humanidad que han pivotado en torno a los conceptos de poder y soberanía territorial[102].

La organización socio-política y jurídica del poder vigente en la actualidad se construye sobre el Estado soberano como categoría jurídico-política que, *ad internum*, monopoliza el poder sobre su territorio y población creando las sociedades internas institucionalizadas y jerarquizadas y que, *ad externum*, compartimentaliza la sociedad internacional estructurándola como una sociedad de sujetos jurídicamente iguales y soberanos[103]. Ese modelo global de organización se sustenta en la existencia de espacios sometidos al régimen jurídico de la soberanía y espacios no susceptibles de apropiación estatal, internacionalizados, sujetos a la calificación de patrimonio común de la humanidad o en régimen de libertad, como ocurre con el alta mar, pero incluso en ese caso con un preciso marco normativo. En el caso del ciberespacio no se ha articulado aún un régimen jurídico en uno u otro sentido y no cabe, incluso, la posibilidad de proceder a su delimitación porque es potencialmente infinito, porque está formado por componentes físicos -que pueden ser objeto de apropiación o, al menos de localización- y por componentes virtuales -que no permiten ninguna de ellas- y, sobre todo, porque transversaliza el resto de los espacios afectando a su funcionamiento e, incluso, potencialmente, a su estructura[104]. Por el momento, el ciberespacio refleja distorsionado el modelo de ejercicio de competencias soberanas del mundo no virtual.

El ciberespacio es global, transnacional, no conoce ni funciona con límites o fronteras y, además de ser congénitamente descentralizado, se encuentra en un

---

[102] Sobre la afectación de la soberanía, RABINAD (2008) p. 85; SOMMER (2000), p. 1189; HEINTSCHEL (2012) p. 7; JENSEN (2012) p. 815; KANUCK (2010) p. 1571; GOLDSMITH (1998) p. 475.

[103] GÓMEZ DE ÁGREDA (2012) p. 179: "partiendo de la concepción westfaliana que rige en la política del los Estados-Nación, Internet y el ciberespacio son intrusos que propician un reequilibrio de fuerzas en que la asimetría se convierte en una estrategia por sí misma".

[104] GÓMEZ DE ÁGREDA (2012) p. 180: el Derecho internacional "está tremendamente mal dotado para responder a situaciones como ésta y la atribución de responsabilidades –pilar sobre el que se sostiene todo el sistema- se lleva a cabo más con criterios políticos que científicos o jurídicos".

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

constante proceso de mutación funcional y, a veces, hasta estructural. Como explica Shackelford, "cyberspace has eroded the connection between territory and sovereignty"[105] y, con ello, el eje sobre el que se articula el modelo de organización estatal y el internacional. Por ello, es necesario replantearse la operatividad de los modelos tradicionales de organización jurídico-política para ordenar esta realidad difícilmente aprehensible con los esquemas tradicionales de organización del derecho en torno al Estado y para reordenar las realidades preexistentes que se ven afectadas funcional y estructuralmente por la dinámica del mundo virtual.

El ciberespacio altera, por una parte, los parámetros clásicos de organización política porque implica una superación extrema del marco de acción y control estatales y porque pone de manifiesto la incapacidad del Estado para afrontar individualmente su gestión, circunstancias ambas que, a su vez, impiden seguir operando con el Estado como núcleo exclusivo y protagónico de poder. Impone, asimismo, cambios en los parámetros tradicionales de organización jurídica porque obliga a replantearse dos extremos esenciales del ejercicio de la soberanía: el marco de aplicación de la legislación cuando se trata del ciberespacio y el ámbito de ejercicio de la jurisdicción que dependerá de los títulos competenciales propios y de la existencia o no de conflictos competenciales positivos o negativos con otros Estados[106].

En definitiva, el modelo de estructuración y de funcionamiento molecular del poder en torno al concepto de Estado y de soberanía territorial, consolidado antes de la aparición del ciberespacio, no está preparado para asumir su evolución y desarrollo. Si en el siglo XX, el fenómeno de internacionalización de la vida social conduce a la superación de la división históricamente establecida entre política exterior y política interna, en el siglo XXI, el ciberespacio supone la ruptura de la dicotomía entre espacio internacional y ámbito estatal.

A pesar de ello, el ciberespacio no parece merecer el análisis de fondo y la reflexión compartida y consensuada que, en la década de los sesenta y setenta, permitió la prematura calificación de determinados espacios, particularmente el exterior, como patrimonio común de la humanidad y la articulación de un régimen jurídico singular como lo eran los espacios a los que iba destinado. Sin duda ha faltado, sobre todo, voluntad política y una concienciación o, incluso, un liderazgo

[105] SHACKELFORD (2009) p. 214. REIDENBERG (2005) p. 1951: "The current Internet technology creates ambiguity for sovereign territory because network boundaries intersect and trascend national borders".

[106] Sobre el ejercicio de la jurisdicción, RABOIN (2011) p. 601; REIDENBERG (2005) p. 1951; WILSKE y SCHILLER (1997) p. 117; SINGH (2014) p. 599; LEITSTEIN (1999) p. 565.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

capaz de apreciar este cambio estructural. En lugar de ello, su regulación ha derivado en una acumulación de normas y de estructuras con ámbitos de aplicación territorial, material y competencial diferentes que traducen una aproximación internacional estructuralmente fragmentaria y funcionalmente centrada en el objeto de cada organización. En cualquier caso, nada parecido a un planteamiento global y coherente sobre la necesidad de regular el ciberespacio atendiendo a sus caracteres, naturaleza y condicionantes singulares que lo desmarcan del resto de los espacios conocidos hasta ahora y objeto de regulación del Derecho Internacional cuya primera función es precisamente la ordenación del ejercicio de las competencias.

Conclusiones

El capítulo de conclusiones sirve, en primer término, para advertir sobre el fenómeno de la "afganización" del ciberespacio[107]. La convivencia de burbujas de seguridad y de insurgencia y, dentro de ellas, el crecimiento alarmante de la criminalidad y de la conflictividad cibernéticas son el resultado de una explosiva mezcla de falta de voluntad política, inconsciencia social e indolencia jurídica.

El ciberespacio introduce un cambio de naturaleza estructural[108] que, además, continúa en un proceso de mutación al ritmo que impone la evolución tecnológica y social pero, globalmente, sin una dirección clara. Podría pensarse que, en su impronta estructural, ya es definitivo en el doble sentido de que no permite vuelta atrás, ni tampoco parece previsible un nuevo avance de la misma naturaleza y alcance. La experiencia sobre la magnitud, la continuidad y el impulso del avance tecnológico no permite, sin embargo, descartar ninguna opción, incluida la posibilidad de nuevos cambios de orden estructural. Desde esa perspectiva, la idea de proceder a su regulación mediante la extrapolación o la aplicación analógica de la normativa creada para el mundo no virtual o la propuesta de encajar ese mundo diferente por naturaleza en las estructuras creadas con anterioridad a la aparición del ciberespacio son, ambas[109], poco factibles, teóricamente infundadas, escasamente prácticas y peligrosamente conservadoras.

A esos efectos, la referencia más clara al tiempo que más problemática se encuentra, nuevamente, en materia de seguridad como garantía esencial de toda

[107] ENRÍQUEZ (2012) p. 114.

[108] DE SALVADOR (2014) p. 2 explica la problemática estructural que plantea el ciberespacio en los ámbitos económicos, industriales, tecnológicos y sociales.

[109] Los distintos aspectos de este problema son analizados por GOLDSMITH (2001) p. 15 y CHERRY (2012-2013) p. 381.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

organización. La separación tradicional entre seguridad internacional, seguridad y defensa del Estado y seguridad interna, pública o ciudadana, quiebra con el ciberespacio ante la nueva categorización de la amenaza. La división entre conflictos internacionales, conflictos internos internacionalizados y conflictos puramente internos se ha visto superada más allá de lo que pretenden trasladar conceptos como el de guerra híbrida o asimétrica. El modelo clásico de conflictividad interestatal se ha desdibujado con la incorporación de nuevos actores no estatales, nuevos medios y motivaciones y nuevas modalidades de conflictividad internacional por parte también de los propios Estados.

La idiosincrasia de la amenaza cibernética contribuye, además, a difuminar los límites entre los espacios tradicionalmente reservados a la conflictividad internacional y a la criminalidad en sentido estricto. Si la solución de la primera entraba en la esfera de acción del Derecho internacional y la lucha contra la segunda correspondía a los derechos internos, en particular, el ámbito penal, y, en caso necesario, a modalidades de cooperación transfronteriza o transnacional, la situación cambia cuando la amenaza no es fácil ni potencialmente subsumible en la primera o en la segunda categoría. Y no lo es en un doble sentido: primero, para determinar si se opera desde el Derecho internacional o desde el derecho interno; y, después, de ser esta última opción, para precisar si es un problema de seguridad exterior y defensa del Estado o de seguridad pública, interna o ciudadana, correspondiendo, respectivamente, a las Fuerzas Armadas o a las Fuerzas y Cuerpos de Seguridad del Estado su gestión y eventual solución siguiendo los procedimientos establecidos por vía constitucional[110]. La delimitación de funciones y responsabilidades y la definición de la naturaleza del problema, seguridad exterior o interna, depende de la calificación misma de la amenaza y, en general, de la conflictividad cibernética.

La conflictividad cibernética no admite una categorización tan aparentemente automática como la que se produce en el mundo físico. En el plano objetivo, un ciberataque puede ser desde un acto de activismo, delictivo, espionaje, terrorista o bélico, dependiendo del autor, la intención y los efectos. En el plano subjetivo, los Estados pueden llegar a actuar en el terreno de la pura delincuencia, mientras que los actores no estatales, incluido un simple individuo con un dispositivo en su poder, puede constituir una amenaza a la seguridad internacional.

A pesar de todo ello, en el marco internacional no se ha producido una respuesta a la altura del desafío, sino que se está operando mediante una acumulación de estructuras entre organizaciones, organismos, agencias y foros de

[110] OPDERBECK (2012) p. 797 estudia los cambios en EEUU.

ENERO-ABRIL 2016 • ISSN 0718-9389 • e-ISSN 0719-2150 • VOL. 7 • Nº 1
DOI 10.7770/RCHDYCP.V7N1.1025

distinta naturaleza, que interseccionan con los nacionales y que traducen una aproximación internacional estructuralmente fragmentaria y funcionalmente centrada en el objeto, competencias y objetivos de cada una de las organizaciones que, a su vez, coexisten con los nuevos organismos y foros con atribuciones en este ámbito.

El resultado es que no hay un régimen jurídico global para el ciberespacio. Prácticamente tres décadas después del nacimiento de Internet y del Manifiesto Barlow contra la soberanía en el ciberespacio[111], no hay un tratado internacional ni una organización internacional capacitados para organizar y gestionar globalmente el ciberespacio. Hay normas y organizaciones que se ocupan sectorialmente de determinados ámbitos materiales porque afectan a su esfera originaria de competencias. Sólo hay una perspectiva fragmentada, especializada y tecnológica del ciberespacio como si fuese un mundo paralelo o ficticio, pero no un mundo tan real como el mundo no virtual y capacitado para afectarlo. Esa aproximación fragmentaria al ciberespacio es un error porque implica una sucesión y acumulación de soluciones coyunturales que no pueden responder a la alteración estructural que implica el ciberespacio. Es una aproximación coyuntural, dispersa y puntual incapaz de hacer frente al reto del ciberespacio que constituye el cambio estructural más profundo que han conocido tanto el modelo de organización estatal como el internacional en toda su historia.

El Derecho internacional es el instrumento para proceder a la ordenación jurídica del ciberespacio que requiere no sólo un tratado de alcance general en su participación y en sus contenidos, aglutinando el conjunto del derecho del ciberespacio sino, también, una organización internacional del ciberespacio capaz de gestionar la imprescindible y ya ineludible cooperación entre los Estados.

Referencias

ARIMATSU, Louise (2012): *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations*". En *4th International Conference on Cyber Conflict*. Tallin: NATO CCE COR Publications, 2012, p. 91-109.

ASLLANI*et al*. (2013): *Viewing Cybersecurity As A Public Good: The Role Of Governments, Businesses, And Individuals*. En *Journal of Legal, Ethical and Regulatory Issues*, vol. 16, Nº 1, 2013, p. 7-14.

111 Disponible en: <https://nomadasyrebeldes.files.wordpress.com/2012/05/manifiesto_de_john_perry_barlow-1.pdf>. [Fecha de consulta: 20 de enero de 2016].

BILLER, Jeffrey Thomas. (2013): *Cyber-Terrorism: Finding A Common Starting Point*. En *Journal of Law, Technology & The Internet,* vol. 4, Nº 2, 2013, p. 275-351.

Blue COAT. *Do Not Enter. Blue Coat Research Maps the Web's Shadiest Neighborhoods*. Disponible en: https://www.bluecoat.com/blogs/2015-09-30/research-maps-webs-shadiest-neighborhoods (Fecha de consulta: 20 de enero de 2016).

BOOTHBY, William H (2013). *Methods and means of Cyber Walfare*. En (New Port: *International Law Studies*, vol. 89, 2013, p. 387-405.

CANDAU ROMERO, Javier (2013): *Estrategias nacionales de ciberseguridad. Ciberterrorismo*, En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, *Cuadernos de Estrategia*, Nº 149, diciembre 2010, p. 259-323.

CARAYANNIS, Elias *et al.* (eds.) (2014): *Cyber-Development, Cyber-Democracy and Cyber-Defense*. Nueva York: Springer, 2014. p. 279-301.

CHERRY, Miriam A.(2013) *Cyber Commodification*. En *Maryland Law Review*, vol. 72, 2012-2013, p. 381-451.

COLLIER *et al*. (2013): *Four domains of cibersecurity: a risk based systems approach to cyber decisions*. En *Environ Syst Decis*, Nº 33, 2013, p. 469-470.

CONSEJO DE EUROPA (2013): *The cybercrime legislation of Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law*, Data Protection and Cybercrime Division, Estrasburgo 27 de febrero de 2013. Disponible en: www.coe.int/cybercrime (Fecha de consulta: 20 de enero de 2016).

CRAIGEN *et ali* (2014): *Defining Cybersecurity*. En *Technology Innovation Management Review*, octubre 2014, p. 13-21.

OECD (2012): *Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, 2012. Disponible en: http://oe.cd./security. (Fecha de consulta: 20 de enero de 2016).

DAS, Pratik Ranjan (2015): *Linking Cyber Attacks and The Use of Force in Public International law: An Exercise in Interpretation*. En *Nalsar International Law Review*, vol. 1, Nº 1, 2015, p. 120-140.

DE SALVADOR CARRASCO, Luis (2014): *Los problemas estructurales en el planteamiento de la ciberseguridad*. En *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 09/2014, 03 de julio de 2014, p. 1-27.

DÍAZ DEL RÍO DURÁN, Juan (2010): *La ciberseguridad en el ámbito militar*. En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, *Cuadernos de Estrategia*, Nº 149, diciembre 2010, p. 217-256.

DOGRUL *et al* (2011): *Developping an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*, En *3rd Conference on Cyber Conflict*, Tallin: NATO CCE COR Publications, 2011, p. 29-43.

ENRÍQUEZ GONZÁLEZ, Carlos (2012): *Estrategias internacionales para el ciberespacio*. En *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, Nº 126, febrero 2012, p. 66-116.

DEREK John Ilar (2009): *Cyber Fatwas and Classical Islamic Jurisprudence*. En *Journal of Computer & Information Law*, vol. XXVII, 2009-2010, p. 577-592.

FELIU ORTEGA, Luis (2012): *La ciberseguridad y la ciberdefensa*. En *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, Nº 126, febrero 2012, p. 32-65.

GANUZA ARTILEZ, Néstor (2010) *La situación de la ciberseguridad en el ámbito internacional y en la OTAN*. En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, *Cuadernos de Estrategia*, Nº 149, diciembre 2010, p. 167-216.

GERVAIS, Michael (2012): *Cyber Attacks and the Laws of War*. En *Berkeley Journal of International Law*, vol. 30, 2012, p. 525-579.

GILES, Keir (2011): *Information Troops – A Russian Cyber Command*. En CZOSSECK *et ali* (eds.), *Proceedings 2012 4th International Conference on Cyber Conflict*, Tallin: NATO CCE COR Publications, 2011, p. 45-60.

GILL, Terry y DUCHEINNE, Paul (2013): *Anticipatory Self-Defense in the Cyber Context*. En *International Law Studies*, vol. 89, 2013, p. 461-463.

GOLDSMITH, Jack L (1998): *The Internet and the Abiding Significance of Territorial Sovereignty*. En *Indian Journal of Global Legal Studies*, vol. 5, Nº 2, 1998, p. 475-491.

GOLDSMITH, Jack L (2001): *The Internet and the Legitimacy of Remote Cross-Border Searches*. En *Public Law and Legal Theory Working Papers*, University of Chicago Law School, Chicago, 2001. 16 p.

GÓMEZ DE ÁGREDA, Ángel (2010): *Global Commons en la era de la incertidumbre*. En *Boletín de Información del CESEDEN*, Nº 317, 2010, 53-62.

GÓMEZ DE ÁGREDA, Ángel (2011): *El ciberespacio factor transversal en los Global Commons.* En REQUENA Y DÍEZ DE REVENGA, M. (coord.), *La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a nuevas amenazas*. Madrid: Instituto Universitario General Gutiérrez Mellado, 2011, p. 1321-1331.

GÓMEZ DE ÁGREDA, Ángel (2012): *El ciberespacio como escenario de conflictos. Identificación de las amenazas*. En *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, Nº 126, febrero 2012, p. 160-195.

GÓMEZ DE ÁGREDA, Ángel (2013): *Ciberdespacio*. En *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 57/2013, 19 de junio de 2013, p. 1-9.

GÓMEZ DE ÁGREDA, Ángel (2013): *The force of change.* Disponible en: http://deagreda.blogspot.com.es/2013/10/la-naturaleza-del-ciberespacio.html. (Fecha de consulta: 20 de enero de 2016).

GONZÁLEZ CUSSAC, José L. (2010): *Estrategias legales frente a las ciberamenazas*. En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, *Cuadernos de Estrategia*, Nº 149, diciembre 2010, p. 85-127.

GRAHAM, David E. (2010): *Cyber Threats and the Law of War*. En *Journal of National Security Law & Policy*, vol. 4, 2010, p. 87-102.

GUITIÉRREZ FRANCÉS, María Luz (2005): *Reflexiones sobre la ciberdelincuencia hoy (en torno a la ley penal en el espacio)*. En *Redur*, Nº 3, 2005, p. 69-92.

HATHAWAY *et al. (2012): The Law of Cyber-Attack*. En *California Law Review*, vol. 100, 2012, p. 817-885.

HEINTSCHEL VON HEINEGG, Wolff (2012): *Legal Implications of Territorial Sovereignty in Cyberspace*. En *4th International Conference on Cyber Conflict.* Tallin: NATO CCE COR Publications, 2012, p. 7-19.

HEVERLY, Robert A. (2011): *Breaking the Internet: International Efforts to Play the Middle Against The Ends – A Way Forward*. En *Georgetown Journal of International Law*, vol. 42, 2011, p. 1083-1121.

JENSEN, Eric T. /2013): *Cyber Attacks: Proportionality and Precautions in Attack*. En *International Law Studies*, vol. 89, 2013, p. 198-217.

JENSEN, Eric T. (2012): *Sovereignty and Neutrality in Cyber Conflict*. En *Fordham International Law Journal*, vol. 35, 2012, p. 815-841.

JOYANES AGUILAR, Luis (2010): *Introducción: estado del arte de la ciberseguridad*. En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, *Cuadernos de Estrategia*, Nº 149, diciembre 2010, p. 29-34.

JURICH, Jon P. (2008): *Cyberwar and Customary International Law: The Potential of a Bottom-up Approach to an International Law of Information Operations*. En *Chicago Journal of International Law*, Nº 9, 2008, p. 275-295.

KANUK, Sean (2010): *Sovereign Discourse on Cyber Conflict Under International Law*. En *Texas Law Review*, vol. 88, 2010, p. 1571-1597.

KESSLER, Oliver y WERNER, Wouter (2013): *Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare*. En *Leiden Journal of International Law*, vol. 26, 2013, p. 793-810.

LAI, Robert y RAHMAN, Syed (2012): *Analytic of China Cyberattack*. En *The International Journal of Multimedia & Its Applications*, vol, 4, Nº 3, 2012, p. 38-56.

LEITSEIN, Todd D. (1999): *A Solution for Personal Jurisdiction on the Internet*. En *Louisiana Law Review*, Vol. 59, Nº 2, 1999, p. 565-590.

LIPTON, Jacqueline (2011): *Combating Cyber-Victimization*. En *Berkeley Technological Law Journal*, vol. 26, 2011, p. 1103-1156.

LÓPEZ DE TURISO Y SÁNCHEZ, José (2012): *La evolución del conflicto hacia un nuevo escenario bélico*. En *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, Nº 126, febrero 2012, p. 120.

LESSIG, Lawrence (1999): *The Law of the Horse: What Cyberlaw Might Teach*. En *Harvard Law Review*, vol. 112, 1999-2000, p. 501-549.

MAURER, Tim (2011): *Cyber Norm Emergence at the United Nations. An Analysis of the Activities at the UN Regarding Cyber-Security*. Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2011. 70 p.

MIQUELON-WEISMANN, Miriam (2005): *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*. En *The John Marshall Journal of Information Technology & Privacy Law*, vol. 23, Nº 2, 2005, p. 329-361.

MIRÓ MIRALLES, Fernando (2011): *La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*. En *Revista Electrónica de Ciencia Penal y Criminología*, Nº 7, 2011. Disponible en: http://criminet.ugr.es/rec. (Fecha de consulta: 20 de enero de 2016).

MOLINA MATEOS, José M (2015) *Aproximación jurídica al ciberespacio*. En *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 57/2015, 08 de junio de 2015, p. 1-20.

MOORE, Stephen (2013): *Cyber Attacks and the Beginnings of an International Cyber Treaty*. En *North Carolina Journal of International Law*, Vol. XXXIX, 2013, p. 223-257.

NIKITAKOS, Nikitas y MAVROPOULOS, Panos (2014) *Cyberespace as a State's Element of Power*. En CARAYANNIS, *et al* (ed). *Cyber-Development, Cyber-Democracy and Cyber-Defense*, Nueva York: Springer, 2014, p. 259-277.

OECD (2012): *Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, 2012. Disponible en: http://oe.cd./security. (Fecha de consulta: 20 de enero de 2016).

O'MALLEY, George (2013): *Hacktivism: Cyber Activisme or Cyber Crime?*. En *Trinity College Law Review*, vol. 16, 2013, p. 137-160.

OPDERBECK, David W. (2012): *Cybersecurity and Executive Power*. En *Washington University Law Review*, vol. 89, Nº 4, 2012, p. 795-845.

PODMANABHAB, Vijay M. (2013): *Cyber Warriors and the Jus in Bello*. En *International Law Studies*, vol. 89, 2013, p. 288-308.

PAREJA ALCARAZ Pablo. (2008): *El nuevo terrorismo internacional: características, factores explicativos y exigencias*. En GARCÍA, Caterina y RODRIGO, Ángel (eds). *La seguridad comprometida. Nuevos desafíos, amenazas y conflictos armados*, Madrid: Ed. Tecnos, 2008, p. 57-69.

PASTOR ACOSTA *et al* (eds.)(2009): *Seguridad nacional y ciberdefensa*, Madrid: Cuadernos Cátedra ISDEFE-UPM, 2009. 179 p.

PASTOR ACOSTA, Oscar (2012): *Capacidades para la defensa en el ciberespacio*. En *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, Nº 126, febrero 2012, p. 205-252.

PÉREZ CÓRTEZ, Manuel (2012): "Tecnologías para la defensa en el ciberespacio", *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, Nº 126, febrero 2012, p. 253-306.

PETRATOS, Pythagoras (2014): *Cybersecurity in Europe: Cooperation and Investment*. En CARAYANNIS, *et al* (ed). *Cyber-Development, Cyber-Democracy and Cyber-Defense*, Nueva York: Springer, 2014, p. 279-301.

RABINAD, María Gimena (2008): *La soberanía del ciberespacio. Algunas reflexiones sobre el concepto de Estado, soberanía y jurisdicción frente a la problemática que presenta Internet*. En *Lecciones y Ensayos*, Nº 85, 2008 p. 85-107.

RABOIN, Bradley (2011): *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*. En *Journal of the National Association of Administrative Law Judiciary*, vol. 31, Nº 2, 2011, pgs. 601-668.

RAMÍREZ MORÁN, David (2014): *La ciberdefensa en la Cumbre de Gales de la OTAN*. En *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 13/2014, 15 de octubre de 2014, p. 1-26.

REIDENBERG, Joel R. (2005): *Technology and Internet jurisdiction*. En *University of Pennsylvania Law Review*, vol. 153, 2005, p. 1951.

ROBLES CARRILLO, Margarita (2015): *El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico*. En *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis, 124/2015, p. 1-18.

ROBLES CARRILLO, Margarita (2015): *Las Fuerzas Armadas ante el reto de la ciberseguridad*. En OLARTE ENCABO, Sofía (dir). *Estudios sobre Derecho militar y defensa*, Madrid: Thomson Reuters Aranzadi, 2016. 502 p.

RYAN *et al*. (2010): *International Cyberlaw: A Normative Approach*. En *Georgetown Journal of International Law*, vol. 42, 2010-2011, p. 1161-1197.

SALES, Nathan (2015): *Regulating Cyber-Security*. En *Northwestern University Law Review*, vol. 107, Nº 4, 2013, p. 1503-1568, en concreto, p. 1507.

SALOM CLOTEC, Juan (2010): *El ciberespacio y el crimen organizado*. En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, *Cuadernos de Estrategia*, Nº 149, diciembre 2010, p. 128-164.

SÁNCHEZ MEDERO, Gema (2012): *Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del S. XXI*. En *Revista CENIPEC*, Nº 31, 2012, p. 239-267.

SÁNCHEZ MEDERO, Gema (2013): *El ciberespionaje*. En *Derecom*, Nº 13, 2013, p. 115-124.

SATOLA, David y JUDY, Henry (2010): *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum*. En *William Mitchell Law Review*, vol. 37, Nº 4, 2011, p. 1744-1804.

SCHMITT, Michael N. (2012): *International Law in Cyberpace: The Koh Speech and Tallin Manual Juxtaposed*. En *Harvard International Law Journal*, vol. 54, 2012a, p. 13-37.

SCHMITT, Michael N. (2012): *Attack as a Term of Art in International Law: The Cyber Operations Context*. En *4th International Conference on Cyber Conflict*, 2012b, Tallin: NATO CCE COR Publications, 2012, p. 283-293.

SCHMITT, Michael N. (2013): *Classification of Cyber Conflict*. En *International Law Studies*, vol. 89, 2013, p. 233-251.

SCHMITT, Michael N. (2014): *The Law of Cyber Warfare: Quo Vadis?*. En *Standford Law & Policy Review*, vol. 25, 2014, p. 269-299.

SHACKELFORD, Scott J. (2009): *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. En *Berkeley Journal of International Law*, vol. 27, Nº1, 2009, p. 193-251.

SHACKELFORD, Scott y ANDRES, Richard B.(2011): *State Responsability for Cyber Attacks: Competing Standards for a Growing Problem*. En *Georgetown Journal of International Law*, vol. 42, 2011, p. 971-1016.

SIBONI *et al*. (2013): *The Threat of Terrorist Organizations in Cyberspace*. En *Military and Strategic Affairs*, vol. 5, Nº 3, 2013, p. 3-29.

SIERS, Rhea. (2014): *North Korea: The Cyber Wild Car*. En *Journal of Law and Cyber Warfare*, Nº 4, 2014, p. 1-12.

SINGH, Avinash. (2014): *Inclusive Adjudication Mechanism for Jurisdictional Issues in Cyberspace*. En *The International Journal of Social Sciences and Humanities Invention*, vol. 1, Nº 8, 2014, p. 599-611.

SOFAER, Abraham D. (2001): *Toward an International Convention on Cyber Security*. En SOFAER, Abraham D. y GOODMAN, Marc (eds.). *The Transnational Dimension of Cyber Crime and Terrorism*, Stanford University, Hoover Institution Press, 2001, p. 221-248.

SOMMER, Joseph H. (2000): *Against Ciberlaw*. En *Berkeley Technological Law Journal*, vol. 15, 2000, p. 1145-1232.

STOCKTON, Paul N. y GOLABECK-GOLDMAN, Michele. (2014): *Prosecutiong Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*. En *Standford Law & Policy Review*, vol. 25, 2014, p. 211-268.

SYMANTEC: *Tendencias de seguridad cibernética en América Latina y el Caribe*, junio, 2014. Disponible en: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf. (Fecha de consulta: 20 de enero de 2016).

TAIPALE, Kim A. (2010): *Cyber-deterrence*. En *Law, Policy and Technology: Cyberterrorism, Information Warfare, Digital and Internet Inmobilization,* IGI Global 2010, p. 1-36.

TEHRANI, Pardis M. y MANAP, Nazura A. (2013): *A Rational Jurisdiction for cyber terrorism*. En *Computer Law & Security Review*, Nº 29, 2013, p. 689-701.

TEPLINSKY, Melanie J. (2010): *Fiddling on the Roof: Recent Developments in Cybersecurity*. En *American University Business Law Review*, vol. 2, Nº 2, 2013, p. 225-322.

TIKK *et al*. (2010): *International Cyber Incidents. Legal Considerations*, Tallin: Cooperative Cyber Defence Center of Excelence, 2010. 132 p.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2009): *El ciberdelito: Guía para los países en desarrollo*, División de Aplicaciones TIC y Ciberseguridad del UIT-D, Abril, 2009.

URUEÑA CENTENO, Francisco J. (2015) *Ciberataques, la mayor amenaza actual*. En *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 09/2015, 16 de enero de 2015, p. 1-18.

WEGNER, Henning. (2014): *La ciberseguridad en la Unión Europea*. En *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 77bis/2014, 14 de julio de 2014, p. 1-22.

WEIMANN, Gabriel (2005): *Cyberterrorism: The Sum of All Fears?*. En *Studies in Conflict & Terrorism*, Nº 28, 2005, p. 129-149.

Weissbrodt, David (2013): *Cyber-conflict, Cyber-crime, and Cyber-Espionage*. En *Minnesota Journal of International Law*, vol. 22, 2013, p. 347-387.

WESTBY, Jody R. (2006): *Countering Terrorism with Cybersecurity*. En *Jurimetrics*, vol. 47, 2006-2007, p. 297-313.

WILSKE, Stephan y SCHILLER, Teresa (1997): *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*. En *Federal Communication Law Journal*, vol. 50, Nº 1, *1997*, p. 117-178.