FACULTAD DE COMERCIO

TRABAJO DE FIN DE MÁSTER EN RELACIONES INTERNACIONALES Y ESTUDIOS ASIÁTICOS

“EN BÚSQUEDA DE UNA REGULACIÓN PARA EL CIBERESPACIO”

ZAIRA CABRERA RODRÍGUEZ

FACULTAD DE COMERCIO

VALLADOLID, JULIO, 2022

RESUMEN

La revolución tecnológica ha afectado a las estructuras políticas, económicas y sociales. El ciberespacio se ha convertido en un nuevo escenario de conflicto para la sociedad internacional, un potencial terreno de guerra entre Estados soberanos, en el que surgen amenazas con consecuencias sin precedentes. La evolución del ciberespacio se ha caracterizado por un progreso constante e inimaginable que no ha ido en paralelo con su ordenación jurídica. Las consecuencias de coexistir sin una regulación globalmente consensuada alarman a la comunidad internacional. Es por ello, por lo que esta incógnita se aborda desde el Derecho Internacional, y, para intentar dar una solución en materia de seguridad, en la que prime la cooperación, se propone un Tratado Internacional al final del trabajo. La construcción de la gobernanza del mundo en el siglo XXI debe, por tanto, tener en cuenta un gran factor condicionante: el ciberespacio.

Palabras clave*:* Ciber-, Ciberespacio, Estados, Internet, Relaciones Internacionales.

ABSTRACT

The technological revolution has changed political, economic and social structures. Cyberspace is now a new stage for International Relations, a potential arena of war between sovereign States, in which threats with unprecedented consequences emerge. The evolution of cyberspace is characterized by a constant progress which has not been in parallel with its regulation. The consequences of coexisting without a global agreed regulation frighten the international community. This issue is addressed from International Law, which, trying to give a solution to international security, an International Treaty is proposed at the end of the essay, always considering cooperation as the main factor of construction. The construction of the world in the XXI must take into consideration a high conditioning factor: cyberspace.

Key words*:* Cyber-, Cyberspace, States, Internet, International Relations.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTADO DE ABREVIATURAS

CAC: Administración del Ciberespacio de China

EEUU: Estados Unidos

ENISA: Agencia Europea de Seguridad de las Redes y de la Información

ICANN: Corporación de Internet para la Asignación de Nombres y Números

OTAN: Organización del Tratado del Atlántico Norte

TIC: Tecnologías de la Información y Comunicación

UE: Unión Europea

1. INTRODUCCIÓN

Ban Ki-moon, Secretario General de las Naciones Unidas dijo: "Internet es un excelente ejemplo de que los terroristas pueden actuar de manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional"[1].

La revolución de las comunicaciones del siglo XXI ha dado lugar a un nuevo dominio: el ciberespacio. El ciberespacio es un nuevo espacio de interacción internacional, que presenta muchas facilidades a la hora de cooperar y forjar relaciones entre los miembros de la comunidad internacional, pero que también presenta numerosas consecuencias sin precedentes. El mayor problema al que se enfrenta la sociedad internacional actualmente es que no existe regulación ni una Organización Internacional que regule y controle los problemas derivados del ciberespacio. Por lo tanto, el principal objetivo del presente trabajo es realizar una aproximación a la búsqueda de una solución jurídica que permita trasladar garantías de seguridad en sus operaciones a los Estados y sus ciudadanos, ya que las amenazas en el ciberespacio hacen necesarias una regulación internacional.

El trabajo tiene una estructura clara en la que se definen los términos a tratar, se exponen los hechos y se propone una solución.

El segundo capítulo engloba, en primer lugar, la definición e historia de internet, desde sus comienzos con fines militares hasta uso hoy en día en la vida cotidiana de los ciudadanos de a pie. En segundo lugar, después de hacer un breve recorrido por diversas definiciones globales sobre el término *ciberespacio*, ya que no existe una única taxonomía globalmente acordada, se intenta explicar lo que el término en sí implica, haciendo alusión a aquellos ámbitos en los que actúa. En último lugar, se exponen las principales amenazas a las que está expuesto el ciberespacio: cibercriminalidad, ciberterrorismo, ciberespionaje y ciberguerra.

En el tercer capítulo del trabajo se expone lo que ya existe en relación a la regulación y se hace una clara diferencia entre gobernanza tecnológica y gobernanza política. Por un lado, en la gobernanza tecnológica domina la Corporación de Internet para la Asignación de Nombres y Números (ICANN), mientras que en la gobernanza política son muchos los países u organizaciones internacionales que han intentado abordar la problemática internamente y

[1] Organización de las Naciones Unidas: "El uso de internet con fines terroristas", 2013. Disponible en: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

que por lo tanto ya han desarrollados regulaciones internas o intentos de regulación internacional. Además, dentro de la gobernanza política también se diferencian dos vertientes que se explican en detalle: Oriente y Occidente.

En el capítulo cuatro se exponen los principales límites que dificultan una regulación en el ciberespacio. Este tipo de limitaciones puede ser de diversa índole: desde aquellos provenientes del Derecho Internacional, como pueden ser la soberanía y la jurisdicción o la atribución de la responsabilidad, hasta limitaciones de carácter cultural como puede ser la brecha digital. En último lugar, y desde el Derecho Internacional, se propone una solución al problema planteado: una propuesta de Tratado Internacional de carácter multilateral.

La información que se presenta en esta investigación tiene carácter cualitativo, ya que lo que se intenta es profundizar en conceptos como el ciberespacio y el Derecho Internacional y como se interactúa entre ellos. Para ello, se ha realizado una búsqueda exhaustiva de, en su mayoría, artículos científicos y libros especializados en exposiciones de expertos en la materia. Además de eso, se ha recurrido a documentos oficiales de organizaciones internacionales, organismos privados y públicos y Estados. Es, por tanto, un trabajo de investigación de índole teórica que pretende un mayor acercamiento a la materia.

La inquietud de la que nace este estudio consiste en que se ha creado en los últimos años un espacio donde la información se comporta libremente, y que, por tanto, no crece en sintonía con su legislación y da lugar a vacíos legales que repercuten en las acciones de los Estados sin posibilidad de atribuir la responsabilidad del delito al autor de los hechos. Internet constituye, hoy en día, un gran reto a los Estados en la gobernanza del sistema internacional, generando intervenciones de actores no tradicionales cuyas conductas pueden amenazar los ámbitos de la esfera internacional. Es por esto por lo que, para que prime siempre el principio de buena fe, se lleva a cabo este trabajo de investigación en el que se intenta mitigar la carencia de regulación a nivel internacional, proponiendo un Tratado Internacional.

2. EL CIBERESPACIO

2.1. La creación y auge de internet

La aparición de Internet ha cambiado nuestras vidas de un modo que no podíamos imaginarnos y, por supuesto, seguirá cambiándolas. Hoy en día, todo está interconectado y la red es un elemento de vital importancia para las sociedades más desarrolladas. A estas alturas, internet y el mundo digital no solo aumentan en gran medida la comodidad de nuestras vidas, sino que también han incrementado las vulnerabilidades a las que estamos expuestos.

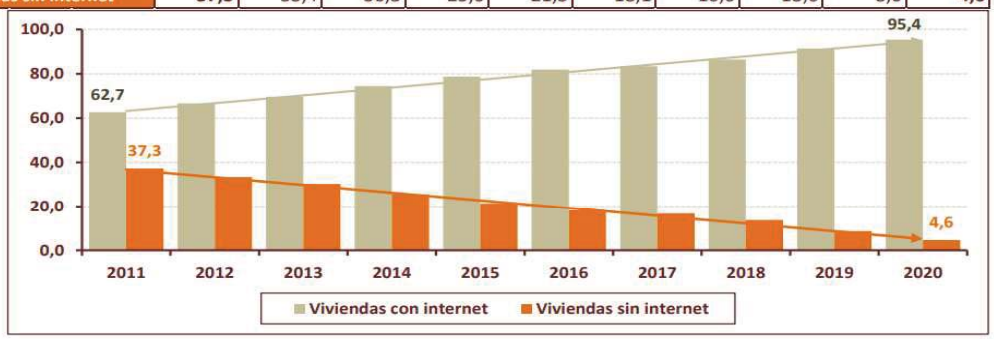
Internet surge en la época de los 60 cuando en las universidades y centros de investigación se desarrollaban los primeros ordenadores. Internet se inició oficialmente en torno al año 1969, cuando en el Departamento de Defensa de los Estados Unidos (EEUU) se desarrolló ARPANET, que consistía en una red de ordenadores que se creó durante la Guerra Fría con el objetivo de no depender únicamente de un ordenador y poder hacer las comunicaciones militares menos vulnerables, por lo que, si se recibía un ataque de Rusia, se pudiera tener acceso a los datos desde cualquier parte del país. En octubre de ese año, Charliy Kline, un estudiante de la Universidad de California en Los Ángeles tecleó un mensaje que decía *login* en un ordenador, y este debía viajar 500km, y el profesor Leonard Kleinrock de la Universidad de Stanford recibió el mensaje, aunque no llegó completo.

El protocolo de Internet y el de Control de Transmisión se desarrollaron a partir de 1973 por el departamento de Defensa de EEUU, de ahí que 1983 se conozca definitivamente como el comienzo de *internet,* cuando el Pentágono decide usar el protocolo TCP/IP y crear, así, la red Arpa Internet. En Europa, las redes comenzaron en los años 80 y en 1989 se creó el World Wide Web (www) para el Consejo Europeo de Investigación Nuclear (Sevilla, 2020).

Desde el momento de su creación, Internet supone un gran reto para los Estados en la gobernanza del sistema internacional, puesto que aparecen nuevos actores no tradicionales cuyas acciones pueden intervenir o amenazar los asuntos nacionales e internacionales. Hablamos de individuos u organizaciones no gubernamentales que están jugando en la esfera internacional en búsqueda de gobernar y tener el dominio (Aguirre y Morandé, 2015). Solo en España, por ejemplo, se ha producido un aumento considerado del acceso de la población a internet en los últimos años:

Figura 1: Porcentaje de viviendas con/sin acceso a internet en España.

PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET										
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Viviendas con internet	**62,7**	66,6	69,7	74,4	78,7	81,9	83,4	86,4	91,4	**95,4**
Viviendas sin internet	**37,3**	33,4	30,3	25,6	21,3	18,1	16,6	13,6	8,6	**4,6**



* Fuente: López *et al*., 2020.

La revolución tecnológica del siglo XXI, con el desarrollo de internet y las Tecnologías de la Información y la Comunicación (TIC), ha afectado las estructuras políticas, económicas y sociales. El auge de internet no solo ha cambiado nuestras vidas, sino que ha ido mucho más lejos, ya que ha dado lugar a la constitución de una nueva dimensión que trasciende las categorías de tiempo y espacio: el ciberespacio. Se presenta aquí un nuevo espacio para la interrelación entre los seres humanos en el que aparece el problema del poder y la gobernanza. Es como si internet fuera la panacea de la sociedad anárquica:

> "Gobiernos del mundo industrial, cansados gigantes de carne y acero, vengo desde el Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido a los del pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No tienen soberanía donde nos reunimos. (...) No tenemos un gobierno elegido, ni es probable que lo tengamos, por lo que me dirijo a vosotros sin más autoridad que la que siempre tiene la propia libertad. Declaro que el espacio social global que estamos construyendo es naturalmente independiente de las de las tiranías que pretenden imponernos. No tenéis derecho moral a gobernarnos ni poseéis ningún método de aplicación que tengamos verdadera razón para temer. (...) Los gobiernos derivan sus justos poderes del consentimiento de los gobernados. (...) El ciberespacio no se encuentra dentro de sus fronteras. (...) Es un acto de la naturaleza y crece por sí mismo a través de nuestras acciones colectivas (...) Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y justa que el mundo que sus gobiernos han creado antes" (Barlow, 1996: 1-2).

El discurso anterior correlaciona la ausencia de reglas con el incremento de las libertades. Sin embargo, no se puede decir que la falta de un gobierno haya dado lugar a un espacio en el que se pueda actuar sin amenazas, al contrario, cada vez se producen más actividades ilícitas, y, a pesar de que la arquitectura de internet presenta ciertas dificultades para el establecimiento de una regulación general. Como afirmó Lawrence Lessing en 1998: "la libertad se conseguirá creando un cierto tipo de Estado, una Constitución para la sociedad, como la crearon nuestros antepasados" (Lessig, 1998: 172).

2.2. La (in)definición del ciberespacio

Antes de comenzar a buscar soluciones para salvaguardar el correcto funcionamiento del ciberespacio, primero es necesario buscar una definición, puesto que el término ciber es muy controvertido y no existe una única taxonomía globalmente aceptada.

Que el ciberespacio se encuentre en una evolución permanente, dificulta el desarrollo de una definición consensuada y, como se expone en la Guía de Ciberdefensa de la Junta Interamericana de Defensa[2], la falta de esa interpretación al término deriva en consecuencias globales:

- No existe una percepción global del término comúnmente aceptada, por lo que en ocasiones se construyen enfoques difíciles de compatibilizar.
- Que la información sea confusa conlleva a que, en ciertas circunstancias, las autoridades, que no terminan de comprender el dominio ciber, lleven a cabo decisiones no idóneas.
- A falta de una estructura firme y organizada, se producen contradicciones a la hora de organizar las estructuras nacionales y además dificulta la colaboración internacional en materia de ciberseguridad.

A continuación, se detallarán algunas de las principales definiciones y los enfoques o características que se le atribuyen para tener una idea más clara de lo que el término a tratar engloba, recalcando que no existe un consenso entre las mismas.

Moisés Barrio, letrado del Consejo de Estado, Profesor de Derecho Digital en la Universidad Carlos III de Madrid, Abogado y Consultor, define el ciberespacio como: "El espacio global en el entorno de la sociedad de la información que consiste en el conjunto

[2] Junta Interamericana de Defensa: Guía de Ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar, 2020. Disponible en: https://studylib.net/doc/25814017/guia-de-cyberdefensa---orientaciones-para-el-diseno--plan...

interdependiente de infraestructuras de las TIC, y que incluye internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados propios del internet de las cosas" (Barrio, 2018: 24).

A raíz de la anterior definición, surge el término ciberespacio, el cuál engloba el concepto de *internet*. Es común que, fuera de los círculos de expertos en la materia, se confundan estos términos. No obstante, deben distinguirse para poder entenderlos. La propia Real Academia Española define el ciberespacio de la siguiente manera: "Ámbito virtual creado por medios informáticos"[3] e internet como: "Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación"[4]. Internet es, por tanto, el medio por el que fluyen todas las acciones que ocurren en el ciberespacio, es decir, el medio que crea y canaliza esta conexión.

Al contrario de la anterior definición, en la Guía de Ciberdefensa de la Junta Interamericana no se paran a dar un único significado, sino que explican que el concepto ciberespacio se materializa gracias a la interrelación de ciertos elementos específicos: la infraestructura de tecnologías de información y comunicaciones, el software, la información, los protocolos de transporte, la energía eléctrica y las personas. Sostienen, que ciertos conceptos integrantes, como la información o las personas, no son en sí una parte intrínseca del ciberespacio, sino que el ciberespacio es un espacio donde poder manejar la información o que las personas, ya sea individualmente o en grupos organizados, son las que crean y modifican el ciberespacio. Además, añaden que los dos únicos elementos del siguiente gráfico que mantienen los signos vitales del ciberespacio serían: software y energía eléctrica[5].

Figura 2: Interacción de elementos en el ciberespacio.

* Fuente: Elaboración propia.

[3] Real Academia Española: "Ciberespacio". Disponible en: https://dle.rae.es/ciberespacio
[4] Real Academia Española: "Internet". Disponible en: https://dle.rae.es/internet
[5] Junta Interamericana de Defensa: Guía de Ciberdefensa… *op. cit.*

Finalmente, desde un punto de vista legal, el Manual de Tallín, editado por Michael Schmitt, lo define como: "El entorno formado por componentes físicos y no físicos, caracterizado por el uso de computadoras y el espectro electromagnético para almacenar, modificar e intercambiar datos mediante redes informáticas" (Schmitt, 2017: 564).

Todas estas definiciones nos remiten a un dominio virtual en el que la interacción humana ha creado un espacio con sus propias modalidades y disputas. Es decir, se ha creado una nueva dimensión de expresión política, y las relaciones internacionales entre Estados soberanos no están ajenas a estos desafíos (Aguirre y Morandé, 2015).

El ciberespacio es un espacio con una naturaleza y características artificiales, creadas por el ser humano, y diferentes a todo lo que se conocía hasta ahora. Este espacio no está limitado, es infinito y no susceptible a la temporalidad o espacialidad. Es un espacio mutable, que está en constante avance y cambio, que además evoluciona a una velocidad increíblemente mayor que el resto de los espacios convencionales por su capacidad tecnológica global. El ciberespacio es transnacional y abierto a todo aquel que desee acceder a él desde cualquier lugar (Robles, 2016a).

2.3. Las principales amenazas del ciberespacio

El auge de las TIC ha supuesto que el ciberespacio se haya convertido en un nuevo escenario de conflicto en el que surgen amenazas con consecuencias sin precedentes (Casar, 2012), pues el ciberespacio ya no supone un dominio emergente, sino un potencial terreno de guerra entre Estados soberanos. Por lo tanto, ya que el ciberespacio no está limitado a un único país, el proteger los intereses de todos los actores gubernamentales y no gubernamentales depende de todos, y se debe trabajar en equipo para defender los objetivos comunes.

La ausencia de una única definición globalmente aceptada para el término *ciberespacio* supone, asimismo, una dificultad para calificar las acciones que se llevan a cabo en el mundo virtual. Todos los actos que derivan de las definiciones de los siguientes términos se denominan *ciberataques.* Un ciberataque es básicamente un acto en el que se producen acciones ofensivas en contra de una persona, grupo, institución, etc., que se lleva a cabo a través de sistemas informáticos (Urueña, 2015). Un ciberataque puede entrar dentro de cada una de las categorías que se procederá a explicar, ya que cumple con todas sus funcionalidades: cibercriminalidad, ciberespionaje, ciberterrorismo y ciberguerra (Pérez, 2012).

Sumado a esto, otro problema al que conduce cada uno de estos términos, es que no deben ser confundidos con sus homólogos en el espacio físico, ya que las acciones cibernéticas trascienden las localizaciones. Es por ello por lo que no deben usarse los mismo mecanismos y procedimientos que fueron creados para el mundo precibernético.

2.3.1. Cibercriminalidad

Citando a Jacinto Pérez: "la cibercriminalidad es el conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas" (Pérez, 2021: 183).

La cibercriminalidad tiene ciertas particularidades que la diferencian de la criminalidad en el espacio no virtual (Gutiérrez, 2005). En primer lugar, como la palabra propiamente indica, el delito se comete desde el espacio cibernético y esto puede derivar en 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" (Salom, 2010: 137).

El auge de las TIC ha supuesto que los grupos criminales se hayan dado cuenta de la situación estratégica que ofrece este nuevo espacio y es por ello por lo que los delitos informáticos se han incrementado en los últimos años. Además, la cibercriminalidad no está acotada territorialmente, y esto, sumado al anonimato y a la globalidad implica que un mismo individuo pueda ser el autor de los hechos y terminar siendo a su vez la víctima.

La cibercriminalidad se ha convertido en un nuevo medio a disposición de los actores internacionales para aumentar la conflictividad internacional y, en algunos medios políticos, se han referido a ella como una preocupación muy cercana a la que genera actualmente el terrorismo (Robles, 2016a).

Figura 3: Ejemplos de cibercriménes que pueden cometerse en la red.

* Fuente: Alvarez, 2018.

2.3.2. Ciberterrorismo

El ciberterrorismo va mucho más allá de la ciberdelincuencia. Aunque tienen una gran relación, las causas que motivan a ambos y los beneficios que esperan obtener de sus acciones distan entre sí, ya que el ciberterrorismo busca cambios políticos, mientras que el cibercrimen busca lucrarse económicamente. A su vez, el ciberterrorismo también se diferencia del terrorismo en que supera la dicotomía clásica entre terrorismo interno e internacional, ya que el ciberterrorismo es, en su defecto, global con una proyección internacional (Biller, 2013).

El ciberterrorismo es la confluencia entre el ciberespacio y el terrorismo, "la forma en la que el terrorismo utiliza las tecnologías de la información para intimidar, coaccionar o para causar daños a grupos sociales con fines políticos-religiosos" (Sánchez, 2010: 74). El ciberespacio ha alterado notablemente la estructura y el funcionamiento de las organizaciones terroristas, distando cada vez más de su homólogo no virtual, y haciendo que sea imposible luchar contra este tipo de actividades ilícitas usando los parámetros convencionales.

2.3.3. Ciberespionaje

El ciberespionaje también dista bastante de su homólogo en el mundo no virtual, ya que, en el ciberespacio, una vez obtenida la información, esta se manipula, se borra o se destruye puesto que hay menor riesgo que en el mundo físico, asemejándose las acciones

en muchas ocasiones a la cibercriminalidad (Sánchez, 2013). Ese tipo de acciones de ciberespionaje de unos Estados sobre otros ha tenido un fuerte impacto en las relaciones diplomáticas entre Estados y es que, como Margarita Robles Carrillo expone: "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" (Robles, 2016a: 13).

Existen numerosos sistemas de espionaje. No obstante, a continuación, se enumerarán solo algunos de ellos. En primer lugar, el "Sistema Echelon" es un sistema automatizado de interceptación global de trasmisiones, operado por los servicios de inteligencia de cinco países: EEUU, Gran Bretaña, Canadá, Australia y Nueva Zelanda. La idea de este proyecto es detectar palabras claves para el riesgo de los países integrantes.

Figura 4: El sistema Echelon.

* Fuente: Sacramento, 2006.

En segundo lugar, el sistema "Enfopol" fue una respuesta de Europa al sistema Echelon para estar a la vanguardia en la carrera cibernética. Enfopol, sin embargo, solo actuaba dentro de los límites de la Unión Europea (UE), pero puede interceptar todo tipo de comunicaciones dentro de los perímetros del territorio[6].

2.3.4. Ciberguerra

Hablar de ciberguerra, implica darle al término una connotación negativa, aunque en este nuevo mundo, los daños colaterales se reciben en forma de pérdidas económicas o fugas de información estatal, y no como tradicionalmente han afectado las guerras que se han

[6] Para conocer más sobre estos sistemas de ciberespionaje consultar a Sánchez, 2013.

librado en el espacio físico, que atacaban directamente a la vida de seres humanos. Sin embargo, actualmente, Ucrania cambia el paradigma de nuevo.

Desde el punto de vista militar, el ciberespacio también es un escenario táctico, estratégico y operativo que se diferencia de los espacios marítimo, terrestre, aéreo y exterior. No obstante, tiene una caracterización jurídica complicada ya que no es posible la apropiación en general y es un espacio único, global, infinito y artificial que influye en el resto de los espacios (Robles, 2016a). El ciberespacio es, actualmente, "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" (López de Turiso, 2012: 120). La prueba está en que, por ejemplo, antes de invadir Ucrania, Rusia lanzó una serie de ataques cibernéticos a departamentos gubernamentales y bancarios del país, intentando provocar el colapso de sus sistemas.

La ciberguerra tiene como objetivo encontrar las vulnerabilidades técnicas de los sistemas informáticos del país enemigo para atacarlas o para extraer información sensible. Con lo que, en este caso, a semejanza de la realidad, el ciberespacio actuaría como campo de batalla y los programas informáticos como armas. La cuestión está en, si calificar o no a los ciberataques como uso de la fuerza, pero se indagará más en el uso de la fuerza en el Derecho Internacional en el siguiente capítulo. Existe, en la literatura académica, un consenso sobre el cual un ciberataque en una ciberguerra que acarree consecuencias similares al uso de la fuerza armada vulnera el artículo 2.4 de la Carta de las Naciones Unidas (Roscini, 2014).

Figura 5: Mapa de ciberataques.

* Fuente: Espinosa, 2018

Que las guerras del siglo XXI comiencen a librarse en el ciberespacio no significa que la guerra tradicional vaya a desaparecer, pero sí que la ciberguerra irá ganando más espacio en los conflictos internacionales, puesto que constituye una guerra mejor, más barata y menos sangrienta. Se dan así guerras menos visibles pero muy poderosas con soldados digitales. Es por ello por lo que cada vez los Estados estén invirtiendo más no solo en ofensivas, sino también en defender sus propios intereses internos, ya que, por ejemplo, un ataque cibernético puede acabar con el tendido eléctrico de todo un territorio nacional, puede tirar abajo un sistema operativo del gobierno o puede robar datos de los sistemas estatales. Y es que, cuanto más avanzado esté un país tecnológicamente y más dependa de este nuevo sistema, más vulnerable será frente a los demás (Sánchez, 2010).

Sun Tzu (600 a.C) dijo en su obra *El Arte de la Guerra:* "Por eso, librar y ganar todas las batallas no implica la excelencia suprema; la excelencia suprema consiste enroper la resistencia enemiga sin combatir" (Sun-tzu, 2018). Aunque, si bien es cierto que con los años su pensamiento ha ido ganando valor, ya que se ha trasladado a diversos ámbitos, como su aplicación para los negocios o incluso para guerras comerciales, como la librada entre China y Estados Unidos, puede que esta frase termine de cobrar todo su valor con el ciberespacio y llevarse a cabo en toda su extensión gracias a este nuevo dominio virtual.

Como una primera respuesta desde la política interna de los Estados, la ciberdefensa comprende todos los mecanismos necesarios para garantizar la ciberseguridad, que es entendida como la seguridad de todos, civiles y militares, públicos y privados (Pastor, 2012).

En conclusión, la revolución tecnológica ha facilitado mucho el desarrollo de la criminalidad en el ciberespacio y la conflictividad sociopolítica transnacional en todas sus variantes que se ha visto beneficiada por el rápido crecimiento de las tecnologías y la falta de una respuesta jurídica legislativa o judicial para erradicarla. Una respuesta a esta situación debe venir desde el Derecho Internacional, y aunque no va a ser fácil ponerse de acuerdo en un tema tan complejo ya que la ordenación jurídica está limitada, se intentará abordar este tema en los siguientes capítulos.

Tabla 1: Comparación de los términos cibercriminalidad, ciberterrorismo, ciberespionaje y ciberguerra.

	Objetivo	**Ejemplo**
Cibercriminalidad	Lucro económico	El cofundador de Pirate Bay, Gottfrid Svartholm Warg, ataca los servidores de IBM, algunos de los cuales eran propiedad de 13ógica Co., una empresa de consultoría que proporciona servicios al gobierno sueco.
Ciberterrorismo	Cambios políticos, sociales o religiosos.	Internet abre las posibilidades de que los grupos terroristas se publiciten, pudiendo así manipular su propia imagen y reclutar. En la red se pueden encontrar webs como la del Ejército Republicano Irlandés. Además de las páginas oficiales, también se mantienen activos en foros de internet para encontrar consumidores que luchen por la causa.
Ciberespionaje	Extracción de información para su manipulación	En 1998 se produjeron una serie de ciberataques y se robaron miles de documentos con información confidencial sobre la tecnología militar de Estados Unidos. Se irrumpió en la red de la Base Aérea Wright Patterson y luego se conectaron con instituciones de investigación militar.
Ciberguerra	Búsqueda de vulnerabilidades técnicas de los sistemas informáticos del enemigo para penetrarla.	La respuesta del presidente de Ucrania a los ataques rusos durante la guerra fue convocar a todos los hackers del mundo para crear un ciberejército, y así, por ejemplo, Anonymous reaparece y le declara la guerra a Rusia. A todo esto, como respuestas, se crea propaganda falsa gracias a la inteligencia artificial de amos bandos y se destruyen sistemas operativos del otro país.

* Fuente: Elaboración propia.

3. LA GOBERNANZA DEL CIBERESPACIO

La gobernanza de Internet consiste en el desarrollo y la aplicación por los gobiernos, el sector privado y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y utilización de Internet[7].

3.1. La gobernanza tecnológica

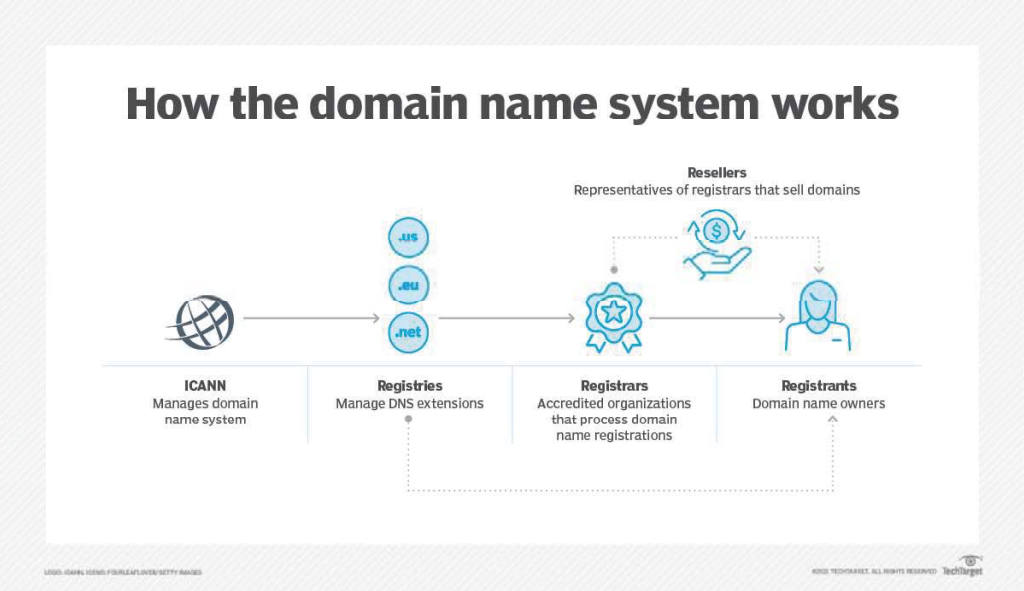
Tecnológicamente hablando, el ciberespacio se encuentra gobernado por la Corporación de Internet para Nombres y Números Asignados (ICANN), una comunidad global que trabaja en conjunto con el objetivo de promover la estabilidad y la integridad de internet. Se trata de una corporación sin ánimo de lucro creada por EEUU y organizada internacionalmente con la responsabilidad de asignar espacios de direcciones IP, identificadores de protocolo genéricos y de país de nivel superior. La ICANN se dedica a preservar la estabilidad operativa de Internet y a desarrollar políticas apropiadas para su misión. En consonancia con el principio de autorregulación máxima en la economía de alta tecnología, ICANN es quizás el ejemplo más destacado de colaboración entre los diversos integrantes de la comunidad de Internet[8].

Actualmente, la ICANN está gobernada por una Junta Directiva internacional que supervisa el desarrollo de políticas, que se encuentra entre sus principales tareas. Además, en ella se encuentran representados todos los miembros de la comunidad cibernética y se rigen por un consenso de abajo hacia arriba.

[7] Unión Internacional de Telecomunicaciones: "La gobernanza de internet". Disponible en: https://www.itu.int/itunews/manager/display.asp?lang=es&year=2004&issue=06&ipage=governance&ext=html

[8] ICANN. Disponible en: http://archive.icann.org/tr/english.html

Figura 6: Cómo trabaja la ICANN.

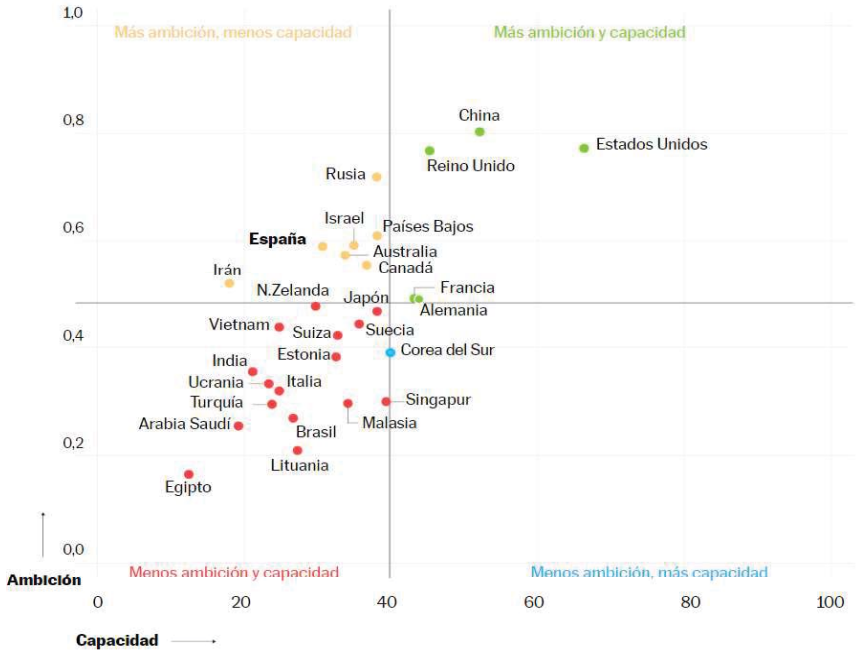


* Fuente: Loshing, 2021.

3.2. La gobernanza política

Antes de dar comienzo a este epígrafe, es interesante contrastar la información que se presentará *a posteriori* con un estudio que hizo la Universidad de Harvard en cuanto a las capacidades y ambiciones de los países en el ciberespacio, siempre teniendo en cuenta que se trata de un dominio totalmente opaco. No obstante, con los elementos que existen se pueden realizar algunas consideraciones referentes a la situación del tablero internacional en el ciberespacio.

Figura 7: Situación de los países con referencia a sus capacidades y ambiciones



* Fuente: Rizzi, 2022.

Un elemento fundamental para definir un mapa de relación de fuerzas en el ciberespacio es las alianzas internacionales que se abordarán en los próximos epígrafes. Existen alianzas de distintas características como el grupo de los Cinco Ojos, la OTAN, la UE, G7 o el QUAD que reflejan el multilateralismo que daría solución al problema planteado.

Como ya se ha presentado a lo largo de esta disertación, el régimen jurídico de las relaciones en el ciberespacio es objeto de un controvertido debate en el plano internacional, pero también en el estatal. Mientras que, por un lado, cada vez se producen más avances en el desarrollo de las TIC, la regulación de las actividades en el ciberespacio no parece progresar al mismo ritmo.

El modelo de Seguridad Colectiva (la Carta de las Naciones Unidas) que se concluyó en 1945 ha permitido que, hasta ahora, se garantice en cierta manera la seguridad internacional, pero el desarrollo de la realidad virtual limita este desafío y hace que la comunidad internacional deba plantearse la operatividad del marco jurídico (Robles, 2019). Para ello, las diferentes organizaciones internacionales y los propios Estados han ido trabajando por su cuenta en políticas internas de ciberdefensa contra amenazas, pero poco se ha podido concluir a nivel de consenso internacional.

La Ciberdefensa, a modo general, es el conjunto de medidas, técnicas y políticas que van enfocadas a proteger los sistemas de información de ciberataques. Militarmente, la ciberdefensa también incluye la capacidad de reacción y ataque durante un conflicto armado en el ciberespacio. La ciberdefensa se sustenta mayormente en tecnología de ciberseguridad probada y desplegada en el sector civil. La ciberdefensa debe, por tanto, prevenir un ciberataque, proteger los sistemas, detectar la ejecución y facilitar la reacción para recuperarse del ataque, de manera que el impacto sea mínimo (Batanero, 2013).

En los siguientes epígrafes se hará alusión a la gobernanza política del ciberespacio que se aplica hoy en día en diferentes puntos del mundo, haciendo una mención especial al caso de ciberseguridad en China. Por un lado, el bloque occidental tiene políticas en las que aplican los valores fundamentales tanto en el mundo digital como en el físico, protegen los derechos fundamentales, la libertad de expresión, los datos personales y la privacidad, ofreciendo un acceso para todos con una gobernanza democrática y eficiente de múltiples partes interesadas que comparten responsabilidad para garantizar la seguridad. Por otro lado, el bloque de Rusia y China, al que se suman cada vez más países autoritarios como es el caso de Irán. Este bloque persigue la idea de controlar todo el territorio soberano, es decir aplicar las fronteras ya existentes al quinto dominio. Aunque se limitaran las libertades de los ciudadanos, es cierto que, siguiendo esta teoría, se podría acabar con el anonimato en el ciberespacio, y, por lo tanto, la trazabilidad del ciberataque sería mucho más fácil.

3.2.1. Occidente

3.2.1.1. La Organización del Tratado del Atlántico Norte

La Organización del Tratado del Atlántico Norte (OTAN) es la primera alianza defensiva que se formó entre los occidentales en 1949. Los Estados que forman parte de esta alianza se comprometen a apoyar militarmente a cualquiera de los aliados de la coalición en caso de que sufran un ataque armado.

Ya hace varios años que la OTAN declaró el ciberespacio como un dominio de operaciones más y, por tanto, intenta que los socios de la organización adapten sus capacidades militares a este terreno emergente. Para ello, ha trabajado en diversos ámbitos como las Reglas de enfrentamiento del ciberespacio. En estas Reglas se busca trasladar la normativa internacional al ámbito del ciberespacio y, por tanto, regularían un ciberconflicto en el caso de que se produjera (Álvarez, 2020).

En último lugar, se ha creado el Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN. Este centro realiza diferentes actividades relacionadas con el ciberespacio, y entre ellas, los miembros de la organización ponen a prueba sus sistemas con el fin de detectar las vulnerabilidades que puedan existir y trabajar en ellas. Algunos de los ejercicios de ciberdefensa que destacan en los últimos años son *Locked Shields* y *Cyber Coallition* (2016), así como *Crossed Swords* (2017) (Álvarez, 2020). Además, el ya nombrado *Manual de Tallín* se ha elaborado en este centro. Dicho manual es el resultado de un análisis que expertos del campo han hecho de la aplicabilidad de las normas internacionales al ciberespacio, que aun siendo opiniones no es vinculante, pero crea el primer cuerpo de ideas sobre la materia (Fonseca *et al.*, 2014).

3.2.1.2. La Unión Europea

A lo largo de estos años, dentro del marco normativo de la UE, se han ido produciendo varios esfuerzos para intentar adaptarse a la nueva realidad. Además, como especifica la organización, "La UE recuerda que en el ciberespacio también rige el Estado de Derecho y los derechos fundamentales, en aras del bienestar social, el crecimiento económico, la prosperidad y la integridad de nuestras sociedades libres y democráticas" (Álvarez, 2018: 7). En su mayoría, las acciones que ha llevado a cabo la Unión Europea en cuanto al ciberespacio son meramente recomendaciones no vinculantes sobre materia de ciberseguridad para proteger tanto a las instituciones públicas como a las privadas de posibles ciberamenazas. Además, la UE tiene su propia Agencia Europea de Seguridad de las Redes y de la Información (ENISA). La ENISA nace en el 2004 para contribuir a la política de ciberseguridad de la UE, colaborando con organizaciones y empresas para fomentar la confianza en la economía digital y garantizando la seguridad de los ciudadanos de la Unión Europea en el entorno digital[9].

En el 2013 se desarrolló la Estrategia de Ciberseguridad que funciona también como una norma *soft law* para actuar y proteger su territorio (Wagener, 2014). En ella, lo que se propone es que haya cooperación por parte de los Estados con el objetivo de que no se produzcan ciberataques desde sus territorios. Posteriormente, en 2020 la UE publicó una Nueva Estrategia de Ciberseguridad que permite a la UE cooperar con socios globales para promover que el espacio sea global, abierto, estable y seguro basado en el Estado de Derecho, los derechos humanos, las libertades fundamentales y los valores democráticos.

[9] Agencia Europea de Seguridad de las Redes y de la Información. DIsponible en: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_es

Según este documento, "la Estrategia reforzará la resiliencia colectiva europea contra las ciberamenazas y ayudará a garantizar que todos los ciudadanos y las empresas puedan beneficiarse plenamente de unos servicios y herramientas digitales fiables y de confianza"[10]. La propuesta de la Nueva Estrategia de Ciberseguridad nace porque la ciberseguridad es una de las principales prioridades de la Comisión y la piedra angular de una Europa digital y conectada. Durante la pandemia, hubo muchos ciberataques que hicieron que pusieron de manifiesto la importancia de proteger a todos

3.2.1.2. El Consejo de Europa

Se nombra al Consejo de Europa ya que es una organización de importancia en cuanto a la protección de los derechos humanos gracias a, por ejemplo, el Convenio Europeo de Derechos Humanos y al Tribunal Europeo de Derechos Humanos, y por supuesto, esto viene altamente ligado a la protección en el ciberespacio.

Uno de sus mayores hitos es el Convenio sobre la ciberdelincuencia o Convenio de Budapest[11]. Esta norma se considera el primer Tratado Internacional que se crea para combatir la ciberdelincuencia en internet, ya que, además de sus países miembros, entre los que se encuentra España, también se ha sumado EEUU. Este tratado internacional recoge herramientas legales para perseguir penalmente aquellos delitos cometidos en el ciberespacio, ya que nace de la necesidad de aplicar una política penal común. Es, básicamente, un instrumento internacional que busca homogeneizar la forma en que los Estados contratantes abordan la cibercriminalidad, otorgándoles la facultad de "detectar, investigar y sancionar" aquellas conductas descritas en el Convenio y que ponen en peligro los sistemas, redes o datos informáticos. El problema de querer homogenizar la manera en que los países contratantes abordan y definen la cibercriminalidad es que no todos parten de los mismos conceptos ni enfrentan los mismos obstáculos.

Por último, de relevancia para esta investigación, el Consejo de Europa también ha elaborado el Convenio de Prevención del Terrorismo[12], por el que los Estados se comprometen a usar el procedimiento en él consignado para combatir a los terroristas extranjeros.

[10] Comisión Europea: "The EU's Cybersecurity Strategy for the Digital Decade", 2020. Disponible en: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[11] Consejo de Europa: "Convenio de Budapest", 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[12] Consejo de Europa: "Convenio para la prevención del terrorismo", 2005. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22018A0622(01)&from=ES

3.2.2. Oriente

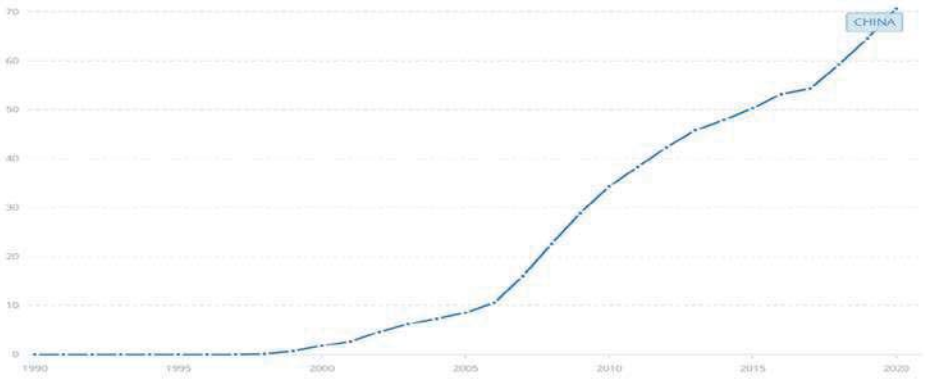
3.2.2.1. China

China se basa en el concepto de cibersoberanía, en lugar del de ciberseguridad, que se enfoca más en la información que los usuarios pueden encontrar en internet. Jon Lindsay presenta el concepto de cibersoberanía de China de la siguiente manera: Toda aquella influencia sobre información, ideas u opiniones que el régimen considera peligrosas y se puedan encontrar en la red deben ser prohibidas (Lindsay, 2015). Para China, esta cibersoberanía es fundamental para así poder mantener su control sobre el país, impulsando la ciberseguridad a través de la cibersoberanía (Raud, 2016).

La postura que China presenta en el ciberespacio está en sintonía con la política exterior del país. En los últimos años, se puede apreciar la postura más asertiva de China, sobre todo en este nuevo campo de batalla, el ciberespacio. Lo que antes era un espacio en el que las empresas de EEUU podían operar libremente, se ha ido convirtiendo en desacuerdos sobre su gestión (Schia y Gjesvik, 2017).

Como se aprecia en la Figura 8, China ha experimentado un aumento explosivo de la conectividad a internet en los últimos 20 años. Como internet y los dispositivos forman parte de la vida de los ciudadanos chinos, el gobierno siente cada vez más la necesidad de controlar el flujo de información que circula en el ciberespacio, y por ello, los dispositivos extranjeros son considerados una amenaza. Por lo tanto, entre las prioridades de China siempre ha estado el poder ser independiente tecnológicamente (Raud, 2016).

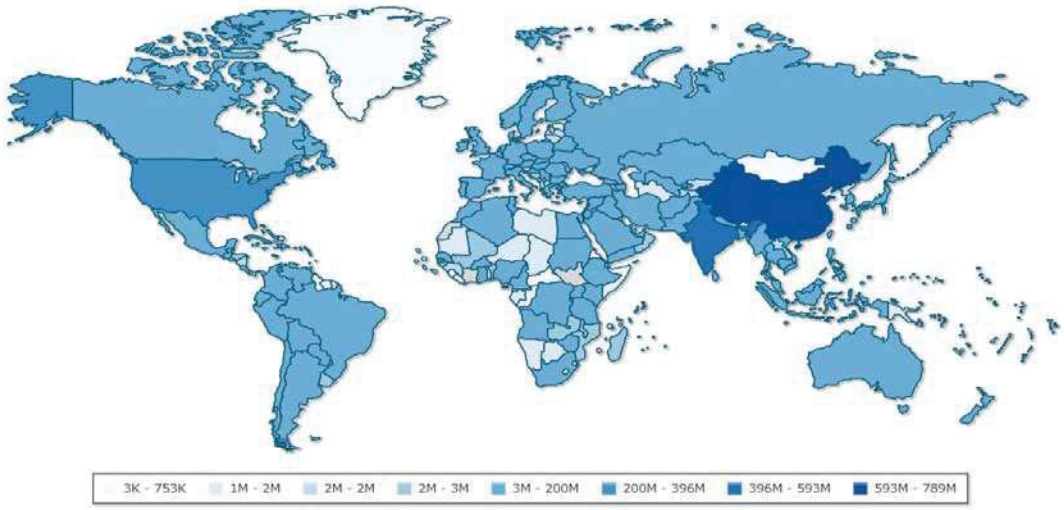
Figura 8: Porcentaje de la población con acceso a internet en China (1990-2020).



* Fuente: Banco Mundial, 2020. Disponible en: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?end=2020&locations=CN&start=1990&view=chart

Tal es el aumento del acceso de la población a internet que, aun siendo un país el cual parte de su población aún sigue en desarrollo, y no teniendo el mayor porcentaje de acceso a internet por población (70% en 2020), sí que se posiciona como el país que más usuarios tiene conectados a internet (Figura 10), y se debe, únicamente, a que China cuenta con la mayor población del mundo en la actualidad. Con lo cual, se pone en evidencia el contexto por el cual el gobierno de China siente la necesidad de controlar el quinto dominio de guerra.

Figura 9: Número de usuarios de internet a nivel global a fecha de 1 de enero de 2020.



* Fuente: IndexMundi, 2020. Disponible en: https://www.indexmundi.com/map/?v=118&l=es

Por otro lado, aunque generalmente en Occidente se ha promulgado la idea de que China es una potencia ofensiva cibernéticamente que pretende robar la información de las instituciones públicas y privadas de Occidente, como se ha visto, *a priori,* lo único que le preocupa a China es su estabilidad interna. No obstante, China, según algunas instituciones, se encuentra entre los países que más ataques cibernéticos produce. No obstante, dicha información se antoja difícil de confirmar, ya que la atribución de los ciberataques continúa siendo un gran desafío, debido a la deslocalización de la amenaza. Un ejemplo es el informe que desarrolló el think tank Council on Foreign Relations en el 2020 en el que sitúa a China, Rusia, Irán y Corea del Norte como los principales ciberatacantes (Figura 10).

Figura 10: Principales ciberataques realizados por países (2005-2020).

* Fuente: Council on Foreign Relations, 2021. Disponible en: www.cfr.org/cyber-operations/

En relación a su estabilidad interna, a finales de 2016, la Administración del Ciberespacio de China (CAC), que está involucrado en la formulación y aplicación de la política en varios temas relacionados con Internet en China, aprobó una nueva norma para la ciberseguridad[13].Esta nueva norma hace referencias explícitas al sistema político chino con la "diseminación de los principales valores socialistas" como se expresa en el Art.6, o la prohibición de actividades en la red que "inciten la subversión de la soberanía nacional, la caída del sistema socialista, el separatismo, mine la unidad nacional…" como se recoge en el Art. 12 (Ramírez, 2017).

La norma se divide en 7 capítulos y 79 artículos. En el primer capítulo, relativo a disposiciones generales, se describe el objeto de la norma y su aplicación al territorio chino. Además, en otros capítulos se presentan medidas proteccionistas, tipificación de delitos o sanciones entre otros aspectos. Para terminar, en el capítulo séptimo se desarrolla una lista de términos relacionados con el ciberespacio y se establece como fecha de entrada en vigor el 1 de junio de 2017.

Cabe hacer una mención especial al Art.37 de la norma, donde se recoge que "la información personal y otros datos importantes recopilados o producidos por operadores de infraestructuras críticas de la información deben ser almacenados en su territorio principal en

[13] Administración del Ciberespacio de China: "Cybersecurity Law": Disponible en: https://www.chinalawtranslate.com/en/cybersecurity-2/

China"[14]. Este artículo persigue que los datos de sus ciudadanos permanezcan en el territorio nacional, haciendo frente, así, a uno de los problemas que dificultan la atribución de las acciones, puesto que se eliminan las fronteras para acceder a los datos de un ciudadano (Ramírez, 2017).

De esta forma, la concepción china de cibersoberanía es más bien defensiva, puesto que pretende asegurarse de que el Partido Comunista de China pueda ejercer el control sin perder su liderazgo. Refleja, en cierto modo, una posición legal en la que se ejerce exclusividad del Estado sobre el mundo virtual, rechazando cualquier forma de injerencia extranjera. La cibersoberanía es aceptada en el panorama político chino como una base para el compromiso con los asuntos cibernéticos globales (Broeders, 2020).

Con posterioridad, la CAC lanzó en 2017 un documento de "Estrategia Internacional de Cooperación en el Ciberespacio"[15], que hace hincapié en la idea de la cibersoberanía ("*As a basic norm in contemporary international relations, the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to-state relations, which also includes cyberspace*") y de desmilitarización del espacio cibernético. En general, el documento sugiere que sean los propios gobiernos los que decidan si se restringe el acceso al ciberespacio global por razones de seguridad nacional (Webster, 2017). Además de ello, se puede considerar a China entre uno de los pocos países abanderados de la solución a la problemática del ciberespacio a través de un tratado internacional.

3.2.2.2. Rusia

Rusia, hoy en día, dista de la ideología occidental y se acerca más al pensamiento chino del control soberano de internet que se ha expuesto en el epígrafe anterior. Para intentar formalizar la idea que tiene Rusia del ciberespacio, en octubre del 2017 el gobierno ruso presentó ante la Asamblea General de las Naciones Unidas un "Proyecto de Convención de las Naciones Unidas sobre Cooperación en la Lucha contra la Ciberdelincuencia"[16]. Y en noviembre del mismo año, se recomendó a los participantes de la mesa redonda

[14] *Ibíd*.
[15] Administración del Ciberespacio de China: "International Strategy of Cooperation on Cyberspace", 2017: Disponible en: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html
[16] Naciones Unidas: "Carta de fecha 11 de octubre de 2017 dirigida al Secretario General por el Representante Permanente de la Federación de Rusia ante las Naciones Unidas", 2017. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/329/62/PDF/N1732962.pdf?OpenElement

parlamentaria del Foro de Gobernanza de Internet que considerara el documento, ya que podría convertirse en un catalizador para la lucha contra las tecnologías de internet (Trepykhalin, 2020). Este documento no es más que un resumen de las ansias de Rusia por querer controlar el ciberespacio alegando que cada Estado podrá adoptar las medidas legislativas necesarias dentro de su territorio y haciendo especial defensa de la protección de la soberanía de los Estados, por la cual ningún Estado Parte podrá ejercer autoridad sobre el territorio cibernético jurisdiccional de otro Estado.

Con anterioridad, en este trabajo de investigación ya se ha hecho referencia al ataque cibernético que sufrió Ucrania justo antes de ser atacada militarmente por tierra, siendo el ciberespacio la antesala de la guerra convencional entre Rusia y Ucrania. En el siguiente gráfico de la ONG Netblocks se muestran las métricas de una pérdida de la conexión a internet en el territorio ucraniano momentos antes de la invasión. La interrupción comenzó en varias ciudades de Ucrania a la vez que las tropas rusas iban avanzando.

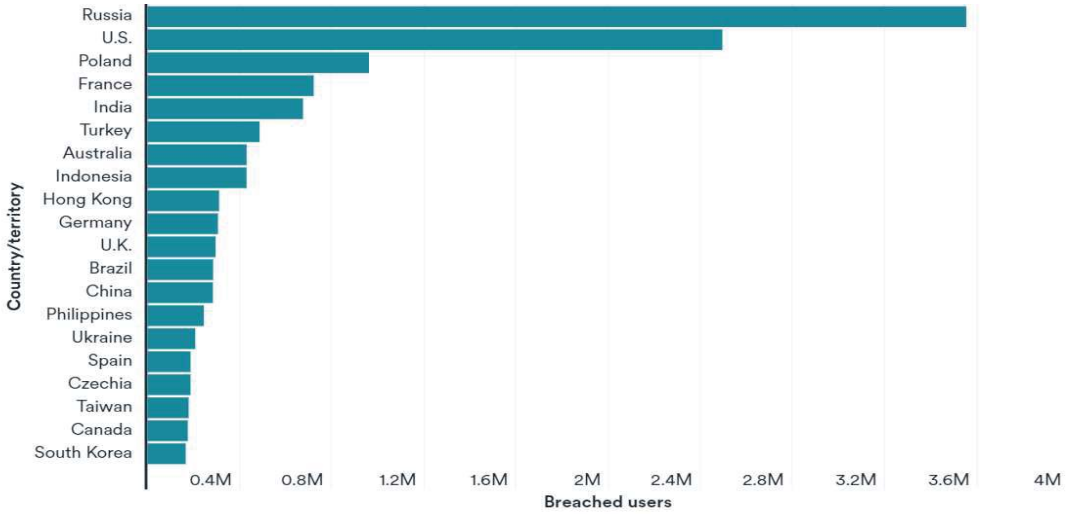
Figura 11: Relación de la conectividad a internet con fechas en Ucrania.

* Fuente: NetBlocks, 2022. Disponible en: https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K

A nivel global, es evidente que la guerra actual entre Rusia y Ucrania producirá consecuencias indeseadas para el resto de los países que también se han visto involucrados. Para poder abordar la seguridad del ciberespacio a nivel global, es necesario que haya un consenso, y, actualmente, con el conflicto entre Rusia y Ucrania más activo que nunca, ningún Estado querrá negociar con Rusia la regulación de internet, puesto que, en estos momentos, la Federación Rusa se encuentra en una posición de inferioridad recibiendo a diario ciberataques desde todos los puntos del mundo, y, por lo tanto, Occidente no considerará

rebajarse para ceder ante alguna de las medidas que Rusia considere estrictamente necesarias para firmar un tratado de regulación internacional del ciberespacio. Para dar evidencia de este desequilibrio de fuerza en el ciberespacio, se presenta un informe realizado por la empresa de VPN SurfShark (Figura 12), en el que se sitúa a Rusia en la tabla como el país que más robo de datos ha recibido en el primer cuatrimestre de 2022 (3,5 millones de usuarios afectados en lo que va de año).

Figura 12: Estadísticas de violaciones de datos del primer trimestre de 2022 (más afectados), TOP 20.



* Fuente: Surfshark, 2022. Disponible en: https://surfshark.com/research/data-breach-impact/statistics

Con todo, en este capítulo se ha podido observar cómo existen dos bloques claramente diferenciados en relación con la gobernanza política del ciberespacio. Si hasta ahora ya era complicado llegar a un acuerdo global sobre la regulación del ciberespacio, en estos días, donde Rusia se aleja cada vez más de la sociedad internacional, se volverá aún más difícil. Que existan, además, ciertas ideologías diferenciadas dificulta aún más el llegar a un acuerdo, ya que cada Estado querrá que se aplique su normativa nacional a la internacional y cederán menos ante el resto de los países en un tema tan controvertido como este.

4. LA REGULACIÓN DEL CIBERESPACIO

La agresión cibernética que Estonia sufrió en el año 2007 se convirtió en un punto de inflexión en ciberseguridad (Anguita y Bartolomé, 2021). Se produjeron una serie de ciberataques contra bancos del país, medios de comunicación y organismos gubernamentales que paralizaron el país, pero, debido a que no se produjeron muertes ni ataques armados en el espacio físico, no se activó el Art. 5 de la OTAN relativo a asistencia mutua[17]. Este suceso marcó un inicio en la preocupación de los Estados por protegerse contra dichos ciberataques y por buscar una regulación internacional de carácter multilateral. No obstante, esta búsqueda se encuentra truncada por numerosos límites de diversa índole que pasamos a analizar a continuación. Como veremos más adelante, debido a estos límites, muchos autores ponen en duda si realmente el ordenamiento jurídico internacional actual tiene la capacidad de regular el recurso a las nuevas tecnologías, cuando estas están siendo especialmente utilizadas como mecanismos de ataques en las relaciones internacionales.

4.1. Límites que dificultan la regulación del ciberespacio

4.1.1. Aplicación de la soberanía y de la jurisdicción nacional

Georgios Zekos ya apuntó en 2007 que el ciberespacio es un espacio amorfo que no ocupa un determinado lugar físico ni geográfico (Zekos, 2007). Esta afirmación cuestiona cómo compatibilizar los conceptos tradicionales de soberanía en el ciberespacio, puesto que, en el caso del espacio virtual, se estaría haciendo referencia a una soberanía a-territorial, a una soberanía supranacional y a una soberanía de no-estados (Rabinad, 2008).

La definición de soberanía, según Antonio Remiro Brotóns, se basa en dos principios: territorialidad y la exclusión de actores externos de estructuras de autoridad domésticas. Expone que sería una situación inmejorable el que el Estado tenga la libertad de escoger las instituciones y políticas que consideren adecuadas de forma autónoma y libre. Uno de sus preceptos es el principio de no intervención de otros Estados en asuntos internos de un

[17] Art. 5: "Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte". En la Carta de la Organización del Tratado del Atlántico Norte, 1949. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es

Estado (Remiro, 2010). La soberanía es un concepto que está arraigado al Estado, ya que solo él puede ejercer los derechos legales y la autoridad de los poderes del Estado (Legislativo, Ejecutivo y Judicial). La soberanía de un Estado no está sometida a ningún poder superior, siendo declarada como uno de los principios básicos del Derecho Internacional y así se establece en la Carta de las Naciones Unidas[18] en su artículo 2.1 ("La Organización está basada en el principio de igualdad soberana de todos sus Miembros").

Dentro del plano jurídico, la soberanía garantiza que un Estado ejerza de manera plena y exclusiva sus competencias sobre su territorio, siendo este limitado al espacio físico, y, por tanto, su aplicación en el ciberespacio no es tan evidente. Las características del ciberespacio, y, en especial su intangibilidad, dificultan la aplicación de la soberanía sobre este espacio. No obstante, aunque el Estado no tiene soberanía sobre el ciberespacio *per se*, sí la tiene sobre las infraestructuras cibernéticas[19] y sobre las actividades relacionadas con esta infraestructura, ya que estas infraestructuras sí se encuentran en su territorio. De esta manera, el Estado tendrá competencias sobre algunos ámbitos relacionados con el ciberespacio. Como bien afirma María Rabinad, "en Internet convergen distintas soberanías, cada cual con sus particularidades. Ninguna puede imponerse sobre otra, ya que el principio rector de la red de redes es la no-territorialidad de la soberanía como concepto revolucionante" (Rabinad, 2008: 94).

A su vez, otra competencia Estatal que deriva de la soberanía es la jurisdicción sobre los delitos cibernéticos. El ejercicio de jurisdicción en este tipo de actividades permitirá establecer qué Estado tiene la responsabilidad de condenar al transgresor de las normas (Raboin, 2011).

4.1.2. Deslocalización de la amenaza

En el ciberespacio prima el anonimato, y, dado que es tan fácil suplantar la identidad, es prácticamente imposible averiguar de qué ordenador procede el ciberataque o quién está detrás de la pantalla. Por consiguiente, si la evolución de los conflictos internacionales ha hecho que se deba volver a plantear el concepto de amenaza y que se haya tenido que incorporar en los diccionarios términos como *ciberguerra,* el concepto del ciberespacio

[18] Naciones Unidas. "Carta de las Naciones Unidas", 1945. Disponible en: https://www.un.org/es/about-us/un-charter

[19] Una estructura cibernética puede ser definida como los recursos de comunicación, almacenamiento y computación sobre los que opera un sistema de información (Llorens, 2016)

conduce directamente a la deslocalización de la amenaza, que se podría considerar como el primer obstáculo para garantizar la seguridad (Robles, 2016b).

La posibilidad de descubrir el origen de cualquier operación cibernética genera una problemática transcendental, ya que la dificultad técnica de determinar los autores de las operaciones afecta directamente a la atribución de responsabilidad del Estado (Schmitt, 2015). En teoría, se defiende que todos los Estados soberanos tienen un deber de diligencia debida por el que se debe impedir cualquier operación cibernética que afecte a los derechos de otro Estado y que hayan sido iniciadas en su territorio o a través de él. De acuerdo con el Manual de Tallin: "Un Estado no deberá permitir que la infraestructura cibernética localizada en su territorio o que se encuentra bajo control gubernamental exclusivo sea utilizada para llevar a cabo actos que ilegítimamente afecten los derechos de otros Estados" (Schmitt, 2017: 278). Siguiendo a Margarita Robles Carrillo (2016b), la deslocalización de la amenaza a la que se hace referencia anteriormente, según varios autores, puede ser: subjetiva, instrumental, material, espacial y teológica.

En primer lugar, la *deslocalización subjetiva* de la amenaza se debe a dos motivos: por un lado, porque cualquier individuo privado puede llegar a poner en peligro la seguridad internacional y, por otro lado, porque cualquiera, ya sean Estados o individuos, puede ser autor de ciberoperaciones criminales. La supremacía del anonimato o la ya comentada dificultad de atribución de responsabilidad a los Estados, junto a los problemas de trazabilidad que el ciberespacio plantea, se unen para que, tanto los individuos asciendan a la esfera internacional como a que los Estados desciendan a la criminalidad.

En segundo lugar*, la deslocalización instrumental* se produce debido a la incapacidad de identificar todos los medios o instrumentos por los que se puede generar una amenaza y de actuar conforme a una normativa para limitar su uso. Las armas cibernéticas no se pueden gestionar de la misma manera que se han regulado las armas tradicionales desde los acuerdos posteriores a la Segunda Guerra Mundial.

En tercer lugar, la *deslocalización funcional* va ligada a las funciones que puede cumplir un ciberataque ya que estas varían en función del autor, el destinatario, la intención y los efectos. Ligado a lo anterior, en cuarto lugar, se considera la *deslocalización material* que viene dada por la dificultad para calificar las ciberoperaciones delictivas en comparación con el mundo físico siendo complicado discernir los objetivos para clasificarlas como cibercrimen, ciberespionaje, ciberterrorismo o ciberguerra.

En quinto lugar, la *deslocalización espacial* se debe a que la conflictividad interna o internacional, en el ciberespacio no tiene una adscripción clara en términos territoriales, lo cual dificulta la capacidad para determinar si un conflicto es interno o transnacional. La localización de un ciberataque en el ciberespacio, su itinerario o destinatario, entre otras variables, siguen unos parámetros muy distintos a los del mundo no virtual. En general, el problema de la trazabilidad es una constante en el mundo cibernético al que se suma el problema de atribución de la responsabilidad, en particular, a los sujetos de Derecho Internacional.

En último lugar, y después de entender los anteriores problemas a los que conduce la deslocalización de una ciberamenaza, se culmina con la *deslocalización teológica*. Esta expresa la gran dificultad de identificar de forma inmediata qué objetivos tiene un ciberataque, ya que puede deberse a una gran cantidad de motivos.

En la siguiente tabla se presentan cada una de las deslocalizaciones de una amenaza para sintetizar mejor las ideas expuestas.

Tabla 2: Tabla explicativa de los términos de deslocalización de un ciberataque.

Deslocalización	Definición
Subjetiva	Cualquier individuo privado puede llegar a poner en peligro la seguridad internacional y cualquiera, ya sean Estados o individuos, puede ser autor de ciberoperaciones criminales.
Instrumental	Incapacidad para identificar todos los medios o instrumentos por los que se puede generar una amenaza y de actuar conforme a una normativa para limitar su uso.
Funcional	La función del ciberataque puede depender del autor, el destinatario, la intención y los efectos.
Material	La dificultad para calificar las ciberoperaciones delictivas. Pueden ser: actos criminales, de espionajes, terroristas o bélicos.
Espacial	La conflictividad en el ciberespacio no tiene una adscripción clara en términos territoriales y eso dificulta la capacidad para determinar si un conflicto es interno o transnacional.
Teológica	La dificultad de identificar de forma inmediata qué objetivos tiene un ciberataque.

* Fuente: Elaboración propia.

La deslocalización de la amenaza desde una perspectiva subjetiva, instrumental, funcional, material, espacial y teológica puede actuar como argumento definitivo para trabajar en una ordenación jurídica global del ciberespacio. No obstante, debido a que hay una errónea concepción del ciberespacio, no existe un acuerdo comúnmente generalizado sobre la definición de los términos que lo engloba. Además, a la falta de consenso hay que añadir el no poder reconocer el alcance de un ciberataque ni la entidad de la amenaza, con los riesgos que ello conlleva. Esto provoca que no exista una confianza mutua entre los sujetos de Derecho Internacional para poder llegar a una unanimidad política y social de base.

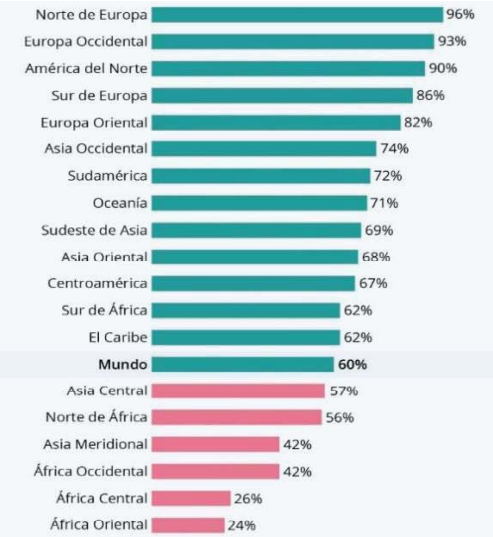
4.1.3. La brecha digital

Además de los anteriores problemas que la situación presenta, hay un reto cultural que es mucho más complicado de mitigar a corto plazo: la brecha digital a nivel munduak

La Organización de las Naciones Unidas, en su Hoja de Ruta para la Cooperación Digital[20], alerta que el mundo está cambiando de analógico a digital rápidamente. La digitalización a la que se hace referencia en los primeros capítulos no se da por igual en todo el mundo, y, por lo tanto, existe un gran desequilibrio entre los países que da como resultado la brecha digital.

La brecha digital es una desigualdad que se produce con respecto al uso, acceso e impacto de las TIC, especialmente debido a la falta de infraestructuras de telecomunicaciones. En este punto juegan un papel importante los gobiernos nacionales, ya que de ellos depende la inversión en el desarrollo tecnológico y en la creación de marcos regulatorios. No obstante, para los países que se encuentran al final de la Figura 13, es mucho más urgente dotar de infraestructuras sanitarias y favorecer la aparición de gobiernos que aboguen por la paz y el reparto de la riqueza de sus territorios, por escasa que sea.

Figura 13: Tasa de penetración de internet por región del mundo en enero de 2021.



* Fuente: Datareportal, 2021. Disponible en: https://datareportal.com/reports/digital-2021-global-overview-report

[20] Naciones Unidas: "Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital", 2020. Disponible en: https://www.un.org/es/content/digital-cooperation-roadmap/

La brecha digital entre países es un factor muy relevante en la búsqueda de una regulación global del ciberespacio y la brusca oscilación que se presenta supone un gran desafío para el acuerdo que se persigue alcanzar. Los países que aún se encuentran menos desarrollados no tienen interés en trabajar por encontrar una solución que les proteja de internet, ya que la carencia del acceso al ciberespacio no les hace tan vulnerable en la materia como lo pueden ser los países que dependen en su mayoría del espacio virtual para desarrollar sus actividades.

Dada la necesidad de participación colectiva de todas las partes involucradas en la gobernanza de internet, se propone la exigencia de financiación y sostenibilidad de recursos para reducir la brecha digital. Aun así, mientras se trabaja en mejorar las capacidades de los Estados menos involucrados, la solución puede proponerse dentro del marco regulatorio de los países más avanzados tecnológicamente, puesto que estos son los que más urgencia tienen para encontrar un equilibrio en la red, ya que esta dependencia tecnológica sin precedentes de los Estados del ciberespacio genera una mayor capacidad para atacar, pero también los convierte en blancos más vulnerables frente al resto de actores participantes.

4.1.4. Ius ad bellum

Por otro lado, otro de los límites a los que se enfrenta la búsqueda de una regulación para el ciberespacio tiene que ver con la acomodación de las normas de la guerra (*ius ad bellum*) al espacio cibernético.

4.1.4.1. La prohibición del uso de la fuerza

La prohibición del uso de la fuerza armada se encuentra recogida en el Art. 2.4. de la Carta de las Naciones Unidas, que establece que “Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas”[21]. Es tal su importancia, que la Comisión de Derecho Internacional, órgano subsidiario de Naciones Unidas encargado de la codificación, la ha declarado oficialmente norma de *ius cogens* o norma imperativa el pasado año 2019[22].

[21] Naciones Unidas: “Carta de las Naciones Unidas”, 1945, *op. cit.*
[22] Naciones Unidas: “Informe de la Comisión de Derecho internacional, 71º período de sesiones (29 de abril a 7 de junio y 8 de julio a 9 de agosto de 2019). Disponible en: https://legal.un.org/ilc/documentation/spanish/reports/a_74_10.pdf

A la hora de aplicarlo al espacio cibernético, es complicado establecer cuándo una operación está violando la prohibición del uso de la fuerza del artículo 2 de la Carta de Naciones Unidas. En primer lugar, porque habría que determinar el alcance del término fuerza para identificar cuál es la fuerza que se considera prohibida. En segundo lugar, habría que tomar como referencia los estándares que fija el Derecho Internacional para configurar una violación (Gervais, 2012). La doctrina mayoritaria entiende que el uso de la fuerza que está prohibido es el de la fuerza "armada" (Llorens, 2016: 802). Teniendo esto en cuenta, habría que valorar, entonces, si las operaciones cibernéticas se consideran fuerza armada y, por tanto, estarían comprendidas dentro del artículo 2 de la Carta de las Naciones Unidas. Ahora bien, la Corte Internacional de Justicia, en la Opinión consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares[23] señaló que la Carta de Naciones Unidas no hace referencia a un tipo de arma específico, el empleo de cualquier arma se considera uso de la fuerza. A su vez, también se hace referencia a ello en el Manual de Tallin, al afirmar que una operación cibernética que constituya una amenaza o un uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o es en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas, es ilegal (Schmitt, 2017).

La versatilidad y variabilidad del ciberespacio, sumado a que la Carta no establece criterios para definir ataques como uso de la fuerza, dificultan la determinación de los ataques cibernéticos como una violación de la prohibición del uso de la fuerza, ya que su trazabilidad funcional puede variar, y se puede tratar tanto de un pequeño acto como de una acción que acarree consecuencias negativas a gran escala.

Para intentar darle una solución a este problema, la doctrina ha dispuesto unos criterios para evaluar los ciberataques, entre los que destacan: i) el criterio instrumental, ii) el criterio basado en el objetivo y iii) el criterio de las consecuencias. El criterio instrumental tiene en cuenta las armas implicadas, por ello una operación cibernética no se considerará como fuerza armada ya que carece de coerción militar. El criterio basado en el objetivo considerará un ciberataque como fuerza armada siempre que este ataque cualquier infraestructura crítica de un Estado[24]. Por último, el criterio de las consecuencias analizará las consecuencias que conlleva el ataque cibernético y lo considerará como fuerza armada si son equivalentes a las

[23] Corte Internacional de Justicia: "Opinión consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares", 1996. Disponible en: https://www.icj-cij.org/public/files/advisory-opinions/advisory-opinions-1996-es.pdf

[24] Una infraestructura crítica de un Estado es aquella infraestructura que es indispensable para los servicios esenciales y su perturbación o destrucción supondría un grave impacto sobre los mismos al no haber otras alternativas disponibles (Gutiérrez, 2020).

realizadas por una fuerza militar, por ejemplo, la destrucción de una central nuclear provocando un elevado número de muertes (Llorens, 2016).

4.1.4.2. La legítima defensa

La legítima defensa también aparece recogida en la Carta de las Naciones Unidas. Concretamente, el Art. 51 de la Carta establece que "ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales (…)"[25].

La legítima defensa sería, por tanto, un derecho de los Estados para recurrir al uso de la fuerza en caso de ser objeto de un ataque armado, aunque sujeto a ciertos requisitos, pues, la respuesta armada del Estado que está siendo afectado deberá ser inmediata, necesaria y proporcional al ataque que ha sufrido. Además, debe notificarlo inmediatamente al Consejo de Seguridad (Värk, 2013). A continuación, analizaremos detenidamente estos requisitos para ver si un ataque cibernético puede llegar a cumplirlos y, por tanto, el Estado atacado podría recurrir a la legítima defensa.

i) Necesidad

El requisito de necesidad se refiere a que el uso de la fuerza por parte del Estado atacado sea necesario para repeler los ataques cibernéticos que están teniendo, lugar siempre y cuando ninguna otra medida menos lesiva pueda emplearse.

ii) Proporcionalidad

La proporcionalidad se aplica a la fuerza que deba emplearse como respuesta a un ciberataque armado. María Pilar Llorens establece que: "El requisito de la proporcionalidad limita la escala, el alcance, la duración y la intensidad de la respuesta necesaria para poner fin a un acto que dio lugar al ejercicio de la legítima defensa" (Llorens, 2016: 810). Cabe añadir que la respuesta no tiene por qué ser de la misma naturaleza que el ataque, por lo que en respuesta a un ciberataque se podría actuar con otro tipo de operación física convencional.

[25] Naciones Unidas: "Carta de las Naciones Unidas", 1945, *op. cit.*

iii) Inmediatez

La inmediatez implica que no debe haber un espacio temporal muy amplio entre el ataque armado y la respuesta de legítima defensa. No obstante, este requisito requiere de un tiempo determinado ya que se necesita conocer la proximidad temporal entre ambas acciones, el periodo necesario para identificar al transgresor de la norma y el tiempo que se considere necesario para preparar la respuesta (Llorens, 2016). La inmediatez podría ser el requisito que más problema acarree por la dificultad para identificar al atacante.

Asimismo, la legítima defensa no debe actuar como represalia para castigar al Estado atacante sino simplemente para repeler el ataque. Es por esto que, una vez que el ataque haya finalizado, no queda espacio para que la legítima defensa se siga utilizando como justificante (Pérez, 2021).

Resumiendo lo expuesto en estos epígrafes, el ciberespacio, al introducir un cambio de naturaleza estructural, presenta nuevas oportunidades, pero también nuevos desafíos que representan un empoderamiento sin precedentes de nuevos actores no estatales e instituciones que luchan por gobernar este nuevo dominio internacional. Es más, este espacio es considerado por muchos ya como el quinto dominio de la guerra. Actualmente, hay numerosas normas universales y regionales que se encargan de regular diferentes ámbitos del ciberespacio, pero aún no se ha conseguido una aproximación global a su régimen jurídico. Por ello, en el próximo epígrafe se abordará la búsqueda de una regulación internacional de carácter multilateral y holístico del ciberespacio, intentando dar una solución al conflicto existente desde la cooperación internacional.

4.2. Propuesta de regulación del ciberespacio: Conclusión de Tratado Internacional Multilateral

La única manera de abordar los desafíos que plantea el ciberespacio es a través de la cooperación internacional de carácter multilateral y de la creación de una serie de normas y principios vinculantes aplicables a todos los sujetos de Derecho Internacional. La necesidad de defender el ciberespacio no se debe únicamente a la protección de la estabilidad económica o política, sino que, además de eso, en estos momentos, vidas humanas también pueden verse afectadas por una mala práctica en el ciberespacio. Por consiguiente, existe consenso entre los expertos internacionales en que la infraestructura de internet se considere un bien público global, y se regule atendiendo a esta concepción (Segura, 2017).

Conforme a esto, se busca una gobernanza política global de internet, y una acción de esta envergadura requiere que haya ciertos puntos clave que no deban romperse como, por ejemplo, que la autoridad y la soberanía sean colectivas y compartidas, implicando ello la participación de múltiples partes que se relacionen entre sí, abarcando cuestiones económicas, técnicas o políticas que afectan a las TIC.

En noviembre de 2005 tuvo lugar en Túnez la Cumbre Mundial de Sociedad de Información, considerada el inicio de las negociaciones a nivel multilateral en relación con internet (Kummer, 2007). Esta Cumbre Internacional de 2005 ha sido uno de los desencadenantes de posteriores negociaciones en materia de ciberseguridad internacional. De esta manera, se ha tratado de llegar acuerdos sectoriales en materia de ciberdefensa, en sintonía con las políticas gubernamentales de los principales actores del dominio global. No obstante, para que se produzca un acuerdo integral, se deben resolver primero las amenazas y los límites analizados en el presente trabajo de investigación.

A pesar de las dificultades para su conclusión, en este trabajo no queremos dejar de proponer la solución más idónea a la problemática del ciberespacio: la conclusión de un tratado internacional de carácter multilateral y holístico, con disposiciones vinculantes.

La Convención de Viena sobre el Derecho de los Tratados, aprobada en 1969, destaca en su preámbulo "la importancia cada vez mayor de los tratados como fuente del derecho internacional y como medio de desarrollar la cooperación pacífica entre las naciones, sean cuales fueren sus regímenes constitucionales y sociales"[26]. Los Tratados Internacionales, entre otras muchas funciones, sirven para establecer las condiciones de paz respecto de un objeto. Un Tratado Internacional establece el principio *Pacta sunt servanda,* que obliga, por tanto, a todas las partes contratantes a actuar de acuerdo con él. Siguiendo a lo establecido en la Convención de Viena, el proceso de elaboración de los Tratados Internacionales se divide en varias fases.

A continuación, presentamos nuestra propuesta de Tratado Internacional, en el que se recogen los principales puntos que se deberían tratar para buscar el mantenimiento de la paz en el ciberespacio entre Estados y Organizaciones Internacionales.

[26] Naciones Unidas: "Convención de Viena sobre el Derecho de los Tratados", 1969. Disponible en: https://www.oas.org/xxxivga/spanish/reference_docs/convencion_viena.pdf

CONVENCIÓN SOBRE COOPERACIÓN INTERNACIONAL EN EL CIBERESPACIO

UNITED NATIONS

2022

CONVENCIÓN SOBRE COOPERACIÓN INTERNACIONAL EN EL CIBERESPACIO

Preámbulo

Los Estados partes en la presente Convención,

Decididos a contribuir a la realización de los propósitos y principios de la Carta de las Naciones Unidas,

Considerando la función fundamental de los tratados en la historia de las relaciones internacionales,

Reconociendo el carácter consensual de los tratados y su importancia cada vez mayor como fuente del Derecho internacional,

Reafirmando la necesidad de que todos los Estados cumplan en todo momento el derecho internacional aplicable, incluidos el derecho internacional humanitario y el derecho internacional de los derechos humanos

Observando las relaciones de los Estados en la utilización del ciberespacio,

Reconociendo que el ciberespacio, como espacio virtual generado artificialmente, desempeña una función esencial en el desarrollo de las sociedades,

Desando evitar que el ciberespacio continúe siendo una zona de conflictos internacionales,

Profundamente preocupados por las consecuencias humanitarias que tendría un mal uso de las armas cibernéticas en forma de ciberataques y reconociendo la necesidad de regular completamente el uso de estas,

Considerando que cualquier uso de armas cibernéticas sería contrario a las normas del Derecho internacional aplicables en los conflictos armados, y, en particular, los principios y las normas del Derecho internacional humanitario,

Reconociendo que la paz y la seguridad, el desarrollo y los derechos humanos son pilares del sistema de las Naciones Unidas y sirven de fundamento a la seguridad colectiva, y que el desarrollo, la paz y la seguridad y los derechos humanos están interrelacionados y se refuerzan mutuamente,

Recordando que, de conformidad con la Carta de las Naciones Unidas, los Estados deben abstenerse en sus relaciones internacionales de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas, y que ha de promoverse el establecimiento y mantenimiento de la paz y la seguridad internacionales con la menor desviación posible de los recursos humanos y económicos del mundo hacia los armamentos,

Reconociendo que una prohibición jurídicamente vinculante del uso de la fuerza en el ciberespacio constituye una contribución importante para el logro y el mantenimiento de una paz universal,

Poniendo de relieve la conveniencia de lograr la adhesión universal al presente Tratado,

Resueltos a actuar de conformidad con los siguientes principios:

Principios:

El derecho inmanente de todos los Estados a la legítima defensa individual o colectiva reconocido en el Artículo 51 de la Carta de las Naciones Unidas;

La solución de controversias internacionales por medios pacíficos de manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia, de conformidad con el Artículo 2, párrafo 3, de la Carta de las Naciones Unidas;

La renuncia a recurrir, en las relaciones internacionales, a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas, de conformidad con el Artículo 2, párrafo 4, de la Carta de las Naciones Unidas;

La no intervención en los asuntos que son esencialmente de la jurisdicción interna de cada Estado, de conformidad con el Artículo 2, párrafo 7, de la Carta de las Naciones Unidas.

Han acordado lo siguiente:

Artículo 1

Las Altas Partes Contratantes se comprometen a respetar y a hacer respetar la presente Convención en todas las circunstancias.

Artículo 2

Definiciones

A los efectos de la presente Convención, las siguientes expresiones se entenderán como se precisa a continuación:

a) Por “ciberespacio”, al espacio virtual creado por medios cibernéticos, el cuál no tiene límites y cualquier individuo o Estado puede interactuar con el mundo entero sin barreras;
b) Por “ciberataque” al ataque organizado contra el sistema informático de un gobierno o empresa, con el objetivo de bloquearlo, dañarlo o extraer información;
c) Por “ciberarma” a un elemento malicioso que se utiliza para realizar un ataque a un sistema cuya utilización equivale al uso de la fuerza o de un ataque armado prohibido por el artículo 2, párrafo 4 de la Carta de Naciones Unidas y el derecho internacional consuetudinario.

Artículo 3

Objeto y fin

El objeto de la presente Convención consiste en:

Establecer normas internacionales comunes lo más estrictas posible para regular o mejorar la regulación del uso del ciberespacio;

Prevenir los ciberataques y el uso de las ciberarmas

Con el fin de:

Contribuir a la paz, la seguridad y la estabilidad en el ámbito regional e internacional;

Promover la cooperación, la transparencia y la actuación responsable de los Estados parte en el ciberespacio, fomentando así la confianza entre ellos.

Artículo 4

Ámbito de actuación

La presente Convención se aplicará a todas las ciberarmas comprendidas en los siguientes ámbitos:

a) Activistas;
b) Delictivas;
c) Espías;
d) Terroristas.

Artículo 5

Aplicación general

Cada Estado parte aplicará la presente Convención de manera coherente, objetiva y no discriminatoria, teniendo presentes los principios mencionados en él.

Cada Estado parte establecerá y mantendrá un sistema nacional de control, incluida una lista nacional de control, para aplicar lo dispuesto en la presente Convención.

Cada Estado parte designará uno o más puntos de contacto nacionales para intercambiar información sobre cuestiones relacionadas con la aplicación de la presente Convención. Cada Estado parte notificará su punto o puntos de contacto nacionales a la Secretaría que se establece en el artículo 18 y mantendrá actualizada dicha información.

Artículo 6

Prohibiciones

Un Estado parte no utilizará ni autorizará ninguna de las ciberarmas comprendidas en el Artículo 4 de la presente Convención.

Artículo 7

Cooperación y asistencia internacionales

Cada Estado parte cooperará con los demás Estados partes para facilitar la aplicación de la presente Convención.

Cada Estado parte tendrá derecho a solicitar y recibir asistencia de otros Estados partes, cuando sea viable, para el cumplimiento de sus obligaciones en virtud de la presente Convención.

Artículo 8

Reunión de los Estados partes

Los Estados partes se reunirán bienalmente para considerar y, cuando sea necesario, tomar decisiones sobre cualquier cuestión relativa a la aplicación o implementación de la presente Convención, de conformidad con sus disposiciones pertinentes, o sobre medidas adicionales para el desarme nuclear.

La primera reunión de los Estados partes será convocada por el Secretario General de las Naciones Unidas en el plazo de un año a partir de la entrada en vigor de la presente Convención. Las siguientes reuniones de los Estados partes serán convocadas por el Secretario General de las Naciones Unidas con carácter bienal, a menos que los Estados partes acuerden otra cosa.

Artículo 9

Enmiendas

Todo Estado parte podrá, en cualquier momento después de la entrada en vigor de la presente Convención, proponer enmiendas a él. El texto de la propuesta de enmienda se comunicará al Secretario General de las Naciones Unidas, quien lo distribuirá entre todos los Estados partes y recabará la opinión de estos sobre la conveniencia de examinar la propuesta.

Artículo 10

Solución de Controversias

En caso de controversia entre dos o más Estados partes sobre la interpretación o aplicación de la presente Convención, las partes interesadas se consultarán con miras a resolver la controversia mediante negociación o cualquier otro medio pacífico de su elección, de conformidad con el Artículo 33 de la Carta de las Naciones Unidas.

Artículo 11

Universalidad

Cada Estado parte alentará a los Estados que no sean partes en la presente Convención a firmarla, ratificarla, aceptarla, aprobarla o adherirse a ella, con el objetivo de lograr la adhesión universal de todos los Estados a la Convención.

Artículo 12

Firma, ratificación, aceptación, aprobación o adhesión

La presente Convención estará abierta a la firma de todos los Estados en la Sede de las Naciones Unidas en Nueva York desde el 3 de junio de 2022 hasta su entrada en vigor.

La presente Convención estará sujeta a la ratificación, aceptación o aprobación de cada Estado signatario.

Tras su entrada en vigor, La presente Convención estará abierta a la adhesión de todo Estado que no la haya firmado.

Los instrumentos de ratificación, aceptación, aprobación o adhesión se depositarán ante el Depositario, el Secretario General de Naciones Unidas.

Artículo 13

Entrada en vigor, duración y reservas

La presente Convención entrará en vigor noventa días después de la fecha en que se deposite ante el Depositario el quincuagésimo instrumento de ratificación, aceptación o aprobación.

La presente Convención tendrá una duración ilimitada.

No se admiten reservas a la presente Convención.

Artículo 14

Relación con otros acuerdos

La presente Convención se aplicará sin perjuicio de las obligaciones contraídas por los Estados partes respecto de acuerdos internacionales vigentes en los que sean partes, cuando esas obligaciones sean compatibles con el Tratado.

5. CONCLUSIONES

La revolución tecnológica del siglo XXI, junto con el desarrollo de Internet y las TIC, ha dado lugar a la constitución de una nueva dimensión que trasciende las categorías de tiempo y espacio: el ciberespacio. A partir de lo anteriormente analizado, hemos llegado a varias conclusiones con relación a la problemática abordada en el capítulo introductorio, puesto que nos hemos dado cuenta de que el ciberespacio, el quinto dominio de guerra, carece de legislación global y poco se ha podido concluir a nivel internacional.

El primer problema con el que nos encontramos al iniciar nuestra investigación es que el término ciber es muy controvertido y, por lo tanto, no existe una única taxonomía globalmente aceptada. Por ello, el segundo capítulo refleja la necesidad de dar inicio al presente estudio realizando unas precisiones terminológicas de cierta importancia para poder establecer las bases conceptuales de lo que se desarrollará *a posteriori*.

Un consenso global en la definición del ciberespacio es el primer paso para que exista una regulación, y este ha sido uno de los mayores problemas a la hora de intentar trabajar conjuntamente en ello. Es por esto por lo que, después de recopilar definiciones de varios expertos en la materia, se concluye que el ciberespacio es infinito, no susceptible a la temporalidad o espacialidad y, además, mutable, evolucionando a una velocidad mayor que el resto de los espacios contemporáneos debido a su capacidad tecnológica global.

Cabe añadir que, este espacio no está ajeno de amenazas, siendo las principales hoy en día la cibercriminalidad, el ciberterrorismo, el ciberespionaje y la ciberguerra. Ya que este tipo de acciones es cada vez es más frecuente, surge la necesidad de buscar una respuesta jurídica que solucione este conflicto, y es en este momento cuando nos damos cuenta de que ya existen unas primeras aproximaciones tanto en el ámbito tecnológico como político.

Tras haber analizado dichas aproximaciones, hemos llegado a una segunda conclusión: existen dos bloques claramente diferenciados en torno a la gobernanza política del ciberespacio que dificultan el desarrollo de una normativa internacional, ya que cada uno tiene su propia percepción de cómo debe ser regulado. Por un lado, el bloque occidental defiende la libertad digital y la gobernanza democrática, mientras que, por otro lado, el bloque de China y Rusia persigue la idea de controlar todo el territorio soberano, aplicando las fronteras físicas a las virtuales. Es por ello, que, para solventar esta problemática, después de llegar a un acuerdo global sobre la definición, es necesario establecer las bases del ciberespacio a nivel internacional, para poder llegar a un acuerdo conjunto.

Si tuviéramos los dos problemas anteriores resueltos, el tercer paso sería encontrar una opción de regulación global y, por ello, se cuestiona la aplicabilidad del Derecho Internacional al ciberespacio. Después de analizar los distintos ámbitos del Derecho Internacional que podrían aplicarse al ciberespacio, nos encontramos con varias limitaciones. En primer lugar, se debe establecer el régimen jurídico del ciberespacio para poder decidir qué competencias tiene un Estado sobre este espacio, y, de esta manera, se podrá determinar la responsabilidad del Estado respecto de las actividades delictivas que se cometen. Además, también es indispensable determinar qué actos pueden ser atribuidos al Estado, ya que de esto dependen cuestiones importantes como la responsabilidad internacional y la legítima defensa. Asimismo, también concluimos con que el uso de la fuerza establecido en la Carta de las Naciones Unidas puede proveer a corto plazo una respuesta a este tipo de operaciones en el ciberespacio, aunque sería necesario que se adaptase a este nuevo dominio.

Se debe reconocer que los esfuerzos multilaterales desplegados hasta ahora no han sido ni pueden ser suficientes para dar respuesta a la amenaza que confrontamos, por lo que debería ser trasladado al seno del Consejo de Seguridad de las Naciones Unidas para que se desarrollen medidas jurídicamente vinculantes para toda la comunidad internacional. El desarrollo de tratados internacionales, por su parte, suele demandar bastante tiempo. No obstante, es momento de comenzar a tratar de solucionar un problema que afecta, cada vez, a más población.

A partir de todo lo anterior, concluimos con que el desafío principal que presenta el régimen jurídico de las operaciones en el ciberespacio se da por la determinación de las normas obligatorias a aplicar, que debe ser incluido como un marco normativo voluntario. Este tipo de nuevas normas que se apliquen deben tener carácter transitorio. El proceso debe de ser progresivo y voluntario. Es por ello, por lo que, para poder solucionar los tres primeros problemas que hemos presentado en nuestras consideraciones finales, proponemos un Tratado Internacional de carácter multilateral y holístico.

El desafío clave del siglo XXI será incorporar una capacidad híbrida de gobernar que incorpore el espacio físico y el cibernético, puesto que ya no es amenaza latente, los ataques cibernéticos están más presentes que nunca, y es deber de toda la sociedad internacional poner fin a esta problemática, puesto que el deber principal del Estado es proteger la seguridad de su territorio y sus ciudadanos.

6. BIBLIOGRAFÍA

6.1. Doctrina

Aguirre Azócar, D. y Morandé Lavín, J. (2015). *El ciberespacio y las relaciones internacionales en la era digital.* Instituto de Estudios Internacionales - Universidad de Chile. Pre-publicación del libro Cátedra Michel Foucault, Escuela Chile-Francia.

Álarez, I. (2018). "Delitos informáticos y ley LOPD BOE". Disponible en: https://irvinsmx.wordpress.com/2018/09/20/delitos-informaticos-y-ley-lopd-boe/

Álvarez Rodríguez, I. (2020). "El Derecho del ciberespacio. Una aproximación", *IDP: revista de Internet, derecho y política*, (30):1-13.

Anguita Olmedo, C. y Bartolomé, M. (2021). "El reto de la gobernanza global en ciberseguridad. La gestión de la Unión Europea (UE) y la Organización de Estados Americanos (OEA)". En Sánchez-Gutiérrez, B. y Pineda, A. (coords.). *Comunicación política en el mundo digital: tendencias actuales en propaganda, ideología y sociedad* (pp. 623-648). Madrid: Dykinson.

Barlow, J. P. (1996). "A Declaration of the Independence of Cyberspace". Disponible en: https://www.eff.org/es/cyberspace-independence

Barrio Andrés, M. (2018). *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet.* Valencia: Tirant Lo Blanch.

Batanero, J. C. (2013). *Ciberdefensa. IX Ciclo de Conferencias UPM TASS.* Madrid: Indra.

Biller, J. T. (2013). "Cyber-Terrorism: Finding A Commun Starting Point". *Journal of Law, Technology & The Internet*, 4(2):275-351.

Broeders, D. (2020). *Governing Cyberspace.* Londres: Rowman & Littlefield.

Casar Corredera, J. R. (2012). "Introducción". En *El ciberespacio. Nuevo escenario de confrontación. Monografías del CESEDEN 126* (pp. 9-39). Madrid: Centro Superior de Estudios de la Defensa Nacional.

Espinosa, C. (2018). "Security Inside". Disponible en: https://securityinside.info/5-mapas-de-ciberataques-para-impresionar-like-a-pro/

Fonseca, C. E. (2014). "El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra". *Revista de la ESG*, 127-144.

Gervais, M. (2012). "Cyber Attacks and the Laws of War". *Berkeley Journal of International*, 30(2):525-579.

Gutiérrez Espada, C. (2020). *La responsabilidad internacional por el uso de la fuerza en el ciberespacio.* Madrid: Thomson Reuters-Aranzadi.

Gutiérrez Francés, M. L. (2005). "Reflexiones sobre la ciberdelincuencia hoy (en torno a la ley penal en el espacio)", *Redur*, (3): 69-92.

Kummer, M. (2007). "The debate on Internet governance: From Geneva to Tunis and beyond". *Information Polity*.

Lessig, L. (1998). "Las Leyes del Ciberespacio". *Thëmis*, (44):171-179.

Lindsay, J. R. (2015). "The Impact of China on Cybersecurity, Fiction and Friction", *International Security,* 39(3):7-47

Llorens, M. P. (2016). "Los desafíos del uso de la fuerza en el ciberespacio". *Anuario Mexicano de Derecho Internacional*, (17):785-816.

López de Turiso y Sánchez, J. (2012). "La evolución del conflicto hacia un nuevo escenario bélico". En *El ciberespacio. Nuevo escenario de confrontación. Monografías del CESEDEN 126* (pp. 117-166). Madrid: Centro Superior de Estudios de la Defensa Nacional.

López Gutiérrez, J., *et al*. (2020). *Estudio sobre la Cibercriminalidad en España.* Madrid: Ministerio del Interior. Gobierno de España.

Loshin, P. (2021). "ICANN (Internet Corporation for Assigned Names and Numbers". Disponible en: https://www.techtarget.com/whatis/definition/ICANN-Internet-Corporation-for-Assigned-Names-and-Numbers

Pastor Acosta, O. (2012). "Capacidades para la defensa en el ciberespacio". En *El ciberespacio. Nuevo escenario de confrontación. Monografías del CESEDEN 126* (pp. 205-252). Madrid: Centro Superior de Estudios de la Defensa Nacional.

Pérez Arias, J. (2021). "Cibercriminalidad: hacia la nueva realidad -virtual- del derecho penal", *Revista Internacional de Doctrina y Jurisprudencia*, 26(2):175-193.

Pérez Cortés, M. (2012). "Tecnologías para la defensa en el ciberespacio". En *El ciberespacio. Nuevo escenario de confrontación. Monografías del CESEDEN 126* (pp. 253-306). Madrid: Centro Superior de Estudios de la Defensa Nacional.

Pérez Sierra, I. (2021). "La legítima defensa del Estado frente a ataques cibernéticos según el Derecho internacional". *Global Strategy Report*.

Rabinad, M. G. (2008). "La soberanía del ciberespacio: Algunas reflexiones sobre el concepto de Estado, soberanía y jurisdicción frente a la problemática que presenta Internet", *Lecciones y Ensayos*, (85):85-107.

Raboin, B. (2011). "Corresponding Evolution: International Law and the Emergence", *Journal of the National Association of Administrative Law Judiciary*, 31(2):602-668.

Ramírez Morán, D. (2017). "Ciberseguridad en China". *Documento Informativo del IEEE*, (1):1-7.

Raud, M. (2016). "China and Cyber: Attitudes, Strategies, Organisation". *NATO Cooperative Cyber Defence Centre*

Remiro Brotóns, A. (2010). *Derecho Internacional: Curso General.* Valencia: Tirant Lo Blanch.

Rizzi, A. (2022). "¿Quién tiene más ciberpoder? Una radiografía de las capacidades de EEUU, China, Rusia y otras potencias". *El País*. Disponible en: https://elpais.com/internacional/2022-01-30/quien-tiene-mas-ciberpoder-una-radiografia-de-las-capacidades-de-ee-uu-china-rusia-y-otras-potencias.html

Robles Carrillo, M. (2016a). "El ciberespacio: Presupuestos para su ordenación jurídico-internacional". *Revista chilena de derecho y ciencia política*, 7(1):1-43.

Robles Carrillo, M. (2016b). "Las Fuerzas Armadas ante el reto de la ciberseguridad". En Orza Linares, R. y Olarte Encabo, S. (coords.). *Estudios sobre derecho militar y defensa* (pp. 415-441). Madrid: Aranzadi.

Robles Carrillo, M. (2019). "El régimen jurídico de las operaciones en el ciberespacio: estado del debate". *Documento del Opinión del IEEE,* (101):1-18.

Roscini, M. (2014). *Cyber Operations and the Use of Force.* Oxford: Oxford University Press.

Salom Clotec, J. (2010). "El Ciberespacio y el crien organizado". En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*. *Cuadernos de Estrategia 149* (pp. 128-164). Madrid: Instituto Español de Estudios Estratégicos.

Sánchez Medero, G. (2010). "Los estados y la ciberguerra". *Boletín de Información del CESEDEN*, (317):63-76.

Sánchez Medero, G. (2010). "Ciberespacio y el Crimen Organizado. Los nuevos desafíos del siglo XXI", *Revista Enfoques*, 10(16):71-87.

Schia, N. N. y Gjesvik, L. (2017). "China's cyber sovereignty". *Norwegian Institute for International Affairs Policy Brief,* (2):1-4.

Schmitt, M. (2015). "In Defense of Due Diligence in Cyberspace". *The Yale Law Journal Forum*, (125):74-75.

Schmitt, M. N. (2017). *Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge Universtity Press.

Segura Serrano, A. (2017). Ciberseguridad y Derecho Internacional. *Revista Española de Derecho Internacional*, 69(2):291-299.

Sevilla Robles, M. A. (2020). "Resumen sobre Internet". *Centro Universitario de Ciencias Económico Administrativas, Departamento de Sistemas de Información, Universidad de Guadalajara.*

Sun-tzu. (2018). *El Arte de la Guerra.* Madrid: Dojo Ediciones.

Trepykhalin, V. M. (2020). "Informe de enfoque en un país: legislación de la Federación Rusa sobre Internet y deliberaciones en las Naciones Unidas". *ICANN.*

Urueña Centena, F. J. (2015). "Ciberataques, la mayor amenaza actual". *Documento de Opinión del IEEE*, (9):1-18.

Värk, R. (2013). "The Legal Framework of the Use of Armed Force Revisited". *Baltic Security & Defence Review*, 15(1):56-94.

Wagener, H. (2014). "La ciberseguridad en la Unión Europea". *Documento de Opinión del IEEE,* (77bis): 1-19.

Webster, G. (2017). "Observations on China's New International Cyberspace Cooperation Strategy". *Lawfare*.

Zekos, G. I. (2007). State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction. *International Journal of Law and Information Technologies*, 15(1):1-37.

6.2. Documentos oficiales

Comisión Europea: "The EU's Cybersecurity Strategy for the Digital Decade", 2020. Disponible en: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Consejo de Europa: "Convenio de Budapest", 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo de Europa: "Convenio para la prevención del terrorismo", 2005. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22018A0622(01)&from=ES

Corte Internacional de Justicia: "Opinión consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares", 1996. Disponible en: https://www.icj-cij.org/public/files/advisory-opinions/advisory-opinions-1996-es.pdf

Junta Interamericana de Defensa: "Guía de Ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar", 2020. Disponible en: https://studylib.net/doc/25814017/guia-de-cyberdefensa---orientaciones-para-el-diseno--plan...

Naciones Unidas. "Carta de las Naciones Unidas", 1945. Disponible en: https://www.un.org/es/about-us/un-charter

Naciones Unidas: "Carta de fecha 11 de octubre de 2017 dirigida al Secretario General por el Representante Permanente de la Federación de Rusia ante las Naciones Unidas", 2017. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/329/62/PDF/N1732962.pdf?OpenElement

Naciones Unidas: "Convención de Viena sobre el Derecho de los Tratados", 1969. Disponible en: https://www.oas.org/xxxivga/spanish/reference_docs/convencion_viena.pdf

Naciones Unidas: "Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital", 2020. Disponible en: https://www.un.org/es/content/digital-cooperation-roadmap/

Naciones Unidas: "Informe de la Comisión de Derecho internacional, 71º período de sesiones (29 de abril a 7 de junio y 8 de julio a 9 de agosto de 2019). Disponible en: https://legal.un.org/ilc/documentation/spanish/reports/a_74_10.pdf

Organización de las Naciones Unidas: "El uso de internet con fines terroristas", 2013. Disponible en: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Organización Tratado Atlántico Norte: "Carta de la Organización del Tratado del Atlántico Norte", 1949. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es

Unión Internacional de Telecomunicaciones: "La gobernanza de internet". Disponible en: https://www.itu.int/itunews/manager/display.asp?lang=es&year=2004&issue=06&ipage=governance&ext=html