Los problemas ciber vistos desde el Derecho internacional. Un gran reto a enfrentar*

Cyber problems seen from International Law perspective. A great challenge to face

Florabel Quispe Remón
Universidad Carlos III de Madrid
ORCID ID 0000-0001-8529-4658
fquispe@der-pu.uc3m.es

Cita recomendada:

Quispe Remón, F. (2024). Los problemas ciber vistos desde el Derecho internacional. Un gran reto a enfrentar. *Eunomía. Revista en Cultura de la Legalidad*, 27, pp. 155-182

DOI: https://doi.org/10.20318/eunomia.2024.9005

Recibido / received: 19/04/2023
Aceptado / accepted: 24/07/2023

Resumen
En primer lugar, el trabajo aborda los problemas que generan los avances tecnológicos utilizados maliciosamente con el fin de dañar a la víctima, los aspectos que pueden influir en estos ataques y los Estados más involucrados en los mismos; así como la respuesta a éstos a través de la ciberseguridad. En segundo lugar, analiza el Derecho internacional aplicable a los ataques producidos en el ciberespacio, que no es otro que el preexistente, como es el caso de la Carta de las Naciones Unidas de 1945, ante la ausencia de normas que regulen el ciberespacio. Este instrumento estaba orientado para hacer frente a ataques en espacios tradicionalmente conocidos como el aéreo, terrestre y marítimo en los que no estaba incluido el ciberespacio. De este modo, se realiza un estudio minucioso sobre el derecho aplicable hoy al ciberespacio y los avances sobre su regulación en el Derecho internacional, a fin de determinar su eficacia y/o necesidad de adoptar normas específicas que regulen el ciberespacio.

Palabras clave
Ciberataque, ciberseguridad, Derecho internacional, ciberespacio, ataque armado, Carta de las Naciones Unidas.

* Este trabajo se ha desarrollado en el marco del proyecto «Ciberamenazas Avanzadas: analítica de mecanismos y vínculos sociopolíticos» (CAVTIONS-CMUC3M).

Abstract
First, the work addresses the problems generated by technological advances used maliciously harm a victim, aspects that can influence these attacks, and the States most involved, as well as the response through cybersecurity. Secondly, it analyzes international law applicable to attacks produced in cyberspace, which is precisely the pre-existing one, as is the case of the United Nations Charter of 1945, in the absence of norms regulating cyberspace. This instrument was aimed a dealing with attacks in spaces traditionally known as air, land and sea, in which cyberspace was not included. Along these lines, am in-depth study is carried out on the law applicable to cyberspace today, and the advances in its regulation in international law, in order to determine the effectiveness and/or need to adopt specific norms regulating cyberspace.

Keywords
Cyberattack, cybersecurity, International law, cyberspace, armed attack, Charter of the United Nations.

1. Introducción

El desarrollo de la tecnología de la información y comunicación es sin duda un gran logro que facilita el trabajo, la vida y proporciona comodidad a las personas naturales y jurídicas, pero el uso inadecuado de ella puede generar diversos problemas a los que tienen que hacer frente las personas, las empresas, las organizaciones internacionales (OOII) y también los Estados. Dentro de dichos problemas están los conocidos como ciberataques, ciber espionaje, ciber amenazas, ciberterrorismo, cibercriminalidad, ciberguerra, etc. –en adelante, problemas *ciber*–. La realidad nos muestra que los ciberataques o ciber amenazas generados por personas, organizaciones criminales, u otros entes, crecen cada vez más e involucran a sujetos de Derecho internacional (DI) y a actores nacionales e internacionales.

Estos ataques engloban una serie de acciones y se caracterizan por su anonimato, y están dirigidos contra uno o varios destinatarios –ciberataques

individuales o masivos–. Esto hace que no se conozca de dónde proviene el ataque ni quién es el autor directo e indirecto, favoreciendo la impunidad. Por ejemplo, es difícil demostrar en un ataque contra un Estado si el atacante es un particular que actúa de manera independiente, o es un órgano de otro Estado, o alguien que actúa por orden de otro Estado o con su aquiescencia.

En los ataques que reciben los Estados, convendría saber qué es lo que genera el ataque, en general. ¿Influyen las relaciones político-sociales entre Estados? ¿qué aspecto o aspectos son las causas? y ¿qué consecuencias tienen para el Estado atacante desde el DI, si se demuestra la autoría directa o indirecta? o ¿cuál es el avance en la regulación de los problemas ciber por parte del DI?

Es indispensable conocer cuál es el papel del Estado en el ciberespacio. Ese universo virtual que jurídicamente no está bajo la soberanía de ningún Estado. Es importante conocer hasta qué punto un Estado podría ser responsable de los ciberataques que reciben las personas y las empresas en su territorio. ¿Son los Estados los encargados de proteger el ciberespacio? o ¿quién debe protegerlo?

Ante los problemas ciber, las víctimas, empresas o Estados, vienen adoptando diversas medidas, conocidas como ciberseguridad, para proteger el ciberespacio, cuyo desarrollo es cada vez mayor, tanto a nivel interno como internacional.

Dada la extensión del trabajo, resulta imposible abordar todos los temas señalados, por ello, este trabajo centra su atención en el desarrollo del DI frente a los problemas ciber y en conocer las medidas adoptadas para enfrentarlos, así como mostrar el *statu quo* de la situación.

El trabajo se divide en dos partes. La primera, tiene por objeto conocer brevemente lo que implican los problemas ciber y quién o quiénes son los sujetos involucrados; y la respuesta a estos actos a través de la ciberseguridad. Luego, teniendo en cuenta los ataques conocidos y con mayor repercusión, se analizarán las relaciones políticas entre los Estados para saber si éstas han repercutido en los ataques y determinar qué Estado o Estados han sido los más atacados y a quién o quiénes se han atribuido dichos ataques. La segunda tiene como propósito analizar de manera detallada las medidas adoptadas a nivel internacional para hacer frente a estos problemas, a fin de conocer si existen pautas de comportamiento frente a los ataques y mecanismos de protección. En esta parte debemos responder si a día de hoy existe un marco legal internacional que regule el ciberespacio, y si los Estados están obligados a cumplirlos. Para ello, acudiremos a la doctrina, a la jurisprudencia de órganos internacionales, a las resoluciones de los órganos de las Naciones Unidas y otras OOII.

2. La tecnología y los cambios que genera: Cibertaques vs. Ciberseguridad

2.1. Un acercamiento a los problemas ciber

La evolución de la tecnología ha cambiado la concepción del Estado respecto a la seguridad para proteger sus intereses. Pasa de preocuparse por proteger sus fronteras físicas en aras de su integridad territorial y soberanía, a enfrentarse a ataques o interferencias del «enemigo» a través del ciberespacio. Nos referimos a los *ciberataques* o *ataques cibernéticos*, definido por el Manual de Tallin como «una operación cibernética, ya sea ofensiva o defensiva, que se espera razonablemente que cause lesiones o la muerte a personas o daños o destrucción de objetos» (Norris, 2013, p. 2).

Estos ataques pueden afectar a la seguridad nacional sin que se identifique al autor, y sin que se sepa si hay algún Estado involucrado. Ante esta situación el capítulo VII de la Carta de la ONU (La Carta), referido al mantenimiento de la paz y la seguridad internacionales, resulta insuficiente, por no decir inaplicable, en determinadas circunstancias, como se verá más adelante.

Si bien, no es objeto del trabajo determinar los tipos de ataques que pudieran existir, mencionamos algunos de ellos, siempre teniendo en cuenta que estos van cambiando y perfeccionándose a la par del avance tecnológico. Entre los más conocidos están: *Malware* - programa malicioso que afecta un sistema informático - troyanos, *dridex*, *spyware*, *ransomware*, *adware*, *botnets*, inyección de código SQL, *phishing*, *Man-in-the-middle* ataques, *Stuxnet*, gusanos, *rootkits*, *Shamoon*, etc. El Instituto Nacional de Ciberseguridad de España (INCIBE) establece una lista de estos ataques: *Pentesting, Adware, Defacement, Man-in-the-middle, Malvertising, Pretexting, Sextorsión, Spear Phishing* (suplantadores de identidad), *Jailbreaking Rooting, Cryptojacking, Data Brokers, Hoax/Bulo, Ciberbullying, Cybersquatting, Warshipping*[1].

Los ataques surgen al mismo tiempo que las tecnologías de la información y éstas van más allá de los ordenadores; incluyen cualquier dispositivo electrónico, como móviles, agendas electrónicas, GPS, tablets, comunicaciones, etc. (Caro Bejarano, 2011, p. 70).

Los problemas ciber constituyen uno de los retos del siglo XXI. Su uso va en aumento y en conflictos, junto a los ataques armados.

2.2. Los ataques cibernéticos en evolución y las relaciones políticas de los Estados

En los ataques ciber no están involucrados todos los Estados, al menos, no en la misma medida. Hay Estados que reciben ataques frecuentemente y Estados que casi siempre están sindicados como presuntos autores. En palabras de Chiappetta, 29 países tienen unidades capaces de proporcionar operaciones ofensivas a través de técnicas cibernéticas y 49 han comprado programas maliciosos (Chiappetta, 2019, p. 61).

Según información existente, EE.UU. es el Estado más atacado, seguido de Reino Unido y España[2]. En los últimos tres años, Reino Unido fue víctima de unos 1.800 ataques cibernéticos perpetrados por hackers respaldados por otros Estados (Cocchine, 2020, p. 271). En este contexto cabe preguntarse ¿qué es lo que motiva el ataque?, ¿influyen en estos, las relaciones sociopolíticas?, ¿las malas relaciones entre Estados afectan a la seguridad de los Estados en discordia? o ¿cuál es el común denominador entre los países más atacados?, ¿quién está detrás de cada ataque? o dada la dificultad de determinar la autoría del ataque, ¿qué Estado o Estados son los sospechosos de estos ataques?

Muchos países han sufrido ciberataques cuya obtención de datos no es un problema, por cuanto existen organismos dedicados a ello, como el Centro de Ciberseguridad Nacional británico; lo difícil es determinar la autoría y las razones de los mismos. Los objetivos y los motivos de los atacantes pueden ser diversos, así como las víctimas, individuales o colectivas, y los daños colosales.

[1] Véase el Instituto Nacional de Ciberseguridad (https://www.incibe.es). Además, véase: Guía de seguridad (CCN-STIC-401), Glosario y abreviaturas, (2015).
[2] Según Agencia EFE (2015).

Kausch agrupa los ciberataques en dos tipos: infracciones para recabar información (espionaje digital) y ataques a sistemas para bloquear o dañar las redes de los adversarios, como las redes gubernamentales, objetivos simbólicos e infraestructura crítica. Para ella

> el valor de los ciberataques como herramienta de coerción directa es limitado dada la naturaleza borrosa tanto de la identidad de autor y el mensaje detrás del ataque, en muchos otros aspectos, sin embargo, los ataques cibernéticos tienen ventajas significativas en el campo de batalla geopolítico en comparación con las herramientas convencionales de influencia internacional. Ellos tienen un alto potencial disruptivo a un costo económico bajo para el atacante. El costo político en forma de riesgo de represalias también es bajo, dados los desafíos para atribuir la autoría. El limbo incierto de las operaciones cibernéticas transnacionales en el DI los hace aún más atractivos, ya que las normas y sanciones no son claras. Combinando un alto potencial disruptivo y un rápido despliegue a bajo costo político y económico, los ataques cibernéticos encajan muy bien para los actores que persiguen una estrategia geopolítica expansiva con recursos limitados y/o capacidades defensivas (Kausch, 2017, p. 2).

La geopolítica y el cibercrimen, dice Chiappetta, se han convertido en un tema de intenso debate internacional, ya que diferentes países se han acusado unos a otros de piratear e interferir con las operaciones y secretos militares de los demás, creando enemistades, aunque todo termina cuando los países intentan superarse unos a otros a través de contraataques. Las naciones desarrolladas han armado su ciberespacio y están listos para atacar cuando son atacados. Sin embargo, si no está bien regulado, el ciberespacio puede ser muy perjudicial para las diferentes economías del mundo (Chiappetta, 2019, p. 71).

Los ciberataques cambian y van a la par del desarrollo de la tecnología. Uno de los primeros grandes ataques, atribuidos a un Estado, fue en Estonia en abril de 2007 (Tikk, Kaska, & Vihul, 2010, pp. 14-33), que duró semanas y afectó a la seguridad nacional de un país y a los ciudadanos, que se quedaron sin servicios (Ganuza Artiles, 2011, pp. 180-184). Así, se «mostró cuán fácil es para un país hostil aprovecharse de potenciales tensiones dentro de una sociedad para causar daño» (McGuinness, 6 de mayo, 2017). Según el International Centre of Defence Studies, hubo suficientes datos para afirmar la relación del Kremlim con la organización y decisión del bloqueo de la embajada de Estonia en Moscú. La embajada estuvo durante semanas asediada y bloqueada (Ganuza Artiles, 2011, p. 178; Cocchine, 2020, p. 250). Para Ganuza, los ciberataques no fueron un hecho aislado, sino que estaban enmarcados dentro de una situación política claramente definida y reunía los requisitos para sufrir un ciber ataque masivo por Rusia, principal sospechoso de instigar y organizar los ataques. Entre ellos, el ingreso de Estonia en la OTAN en 2004, que no gustó a Rusia[3]. Si bien

> el grado de implicación de las autoridades rusas en el conflicto, en las manifestaciones y actos vandálicos en Tallin y en el bloqueo y acoso a la embajada y embajadora en Moscú es difícil de determinar, pero existen multitud de datos que apoyan la tesis de que los enfrentamientos no fueron espontáneos, sino que contaron con la complicidad de las autoridades rusas (Ganuza Artiles, 2011, p. 167).

«Los países hostiles suelen contar con que *hackers* copiones, grupos criminales y actores políticos *freelance* se sumen a ellos» (McGuinness, 6 de mayo, 2017).

[3] En la actualidad, la tentativa de ingreso de Ucrania en la OTAN ha enfurecido a Rusia, y ha comenzado una guerra por el mismo motivo, que esperemos termine pronto.

En el ataque contra Georgia en el 2008 también se sindicó a Rusia. Es el primer caso donde las operaciones cibernéticas se iniciaron y concluyeron conjuntamente con operaciones militares armadas (Ganuza Artiles, 2011, p. 167).

En ambos se advierten un interés, coincidencias e indicios de su participación. Entre los indicios, «la no cooperación en la identificación de los responsables es el principal o único beneficiario de los resultados de la ofensiva cibernética, y los ciber ataques evolucionaban junto con las operaciones armadas y para ello se necesitaba información que solo era accesible por parte de las autoridades políticas y militares rusas» (Ganuza Artiles, 2011, p. 202).

Hay cada vez más ataques cibernéticos contra Estados, cuyas autorías apuntan a otro Estado. Ataques cibernéticos contra las infraestructuras críticas o contra objetivos concretos de un país, pero igualmente estratégicos (Caro Bejarano, 2011, p. 72). Para Caro, los conflictos del mundo físico o real continúan en el mundo virtual del ciberespacio, como sucedió en Estonia, donde se inutilizó mucha de la infraestructura crítica del país, «o los ciberataques sufridos por las redes clasificadas del gobierno norteamericano por atacantes con base en territorio chino o el ataque reconocido por Irán a los sistemas informáticos de decenas de industrias que fueron atacados por un virus y del que Irán dice haberse recuperado» (2011, p. 71).

En 2015, se atacó a la red eléctrica de Ucrania mediante el virus *blackEnergy*, que dejó a miles de personas en la oscuridad por varias horas. «El servicio de seguridad de Ucrania culpó al Gobierno ruso por el ataque» (DW,5 de enero, 2019), al igual que algunas compañías privadas de seguridad de EE.UU. que creían que su origen era ruso.

En el 2016, en EE.UU., con ocasión de las elecciones presidenciales, piratas informáticos filtraron muchos correos electrónicos del Comité Nacional Demócrata. El departamento de Justicia de EE.UU. atribuyó a 12 rusos dicho ataque «que se cree que son agentes de la agencia de inteligencia militar de Rusia (el GRU)» (BBC, 7 de enero, 2017). Este hecho, según los servicios de inteligencia de los EE. UU., había sido dirigido por Vladimir Putin[4] para favorecer a Trump.

Otro ataque importante a escala mundial, que afectó a diversas empresas e instituciones estatales de unos 150 países[5], bloqueando el acceso a sus sistemas informáticos, fue en mayo de 2017, a través del virus *WannaCryptor* o *WannaCry*. Los más afectados fueron Rusia, los trenes alemanes, universidades chinas, cines en Corea del Sur, empresas en Japón, hospitales de Indonesia, policía estatal de India, hospitales de Reino Unido, telecomunicaciones españolas, la empresa francesa Renault, Fedex, PyMEs de Australia[6]. Entre los sospechosos estaban EE.UU. y Corea del Norte. EE.UU. y Reino Unido culparon a Corea del Norte, una acusación que Pyongyang negó y que calificó de «grave provocación política» (DW, 5 de enero, 2019). Por otro lado, «Microsoft responsabiliza a la Agencia de Seguridad Nacional de Estados Unidos» (BBC, 15 de mayo, 2017).

En mayo de 2021, se produjo el ataque a la empresa Colonial, uno de los mayores oleoductos de EE.UU., que paró su actividad y generó un desabastecimiento

[4] Consultar noticia de la BBC *Qué dice el informe de inteligencia desclasificado que culpa a Rusia y a Putin de ordenar ciberataques para influir en las elecciones de Estados Unidos* (BBC, 7 de enero, 2017) (https://www.bbc.com/mundo/noticias-internacional-38545605)

[5] Consultar noticia de la BBC: *El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de unos 150 países (*https://www.bbc.com/mundo/noticias-39903218)

[6] Según la BBC en su artículo *Ciberataque masivo: ¿quiénes fueron los países e instituciones más afectados por el virus WannaCry?* (https://www.bbc.com/mundo/noticias-39929920))

de gasolina en la costa Este de los EE.UU. y el aumento de los precios. El presidente Biden señaló la inexistencia de pruebas orientadas al Kremlin, pero afirmó que el grupo responsable, Darkside, que extorsionó a Colonial, opera desde Rusia (Mars, 13 de mayo, 2021).

Otro ciberataque atribuido a Rusia fue el de 28 de mayo de 2021. *Un ciberataque de origen ruso vuelve a golpear al Gobierno de Estados Unidos* titulaba el periódico El País (Monge, 28 de mayo, 2021). El ciberataque al sistema de correo utilizado por la Agencia de Ayuda Internacional (USAID) del departamento de Estado de EEUU, desde donde prometía supuestamente USAID dar más información sobre el fraude electoral «Alerta especial de USAID: Donald Trump ha publicado nuevos documentos sobre el fraude electoral» (Monge, 28 de mayo, 2021), fue atribuido a piratas informáticos vinculados al espionaje ruso, al grupo Nobelium. El ataque se produjo semanas antes de la reunión entre Biden y Putin, en junio de 2021.

Ante tantos ataques el presidente Biden dio por ciertas las sospechas de injerencia rusa en EE.UU. y por primera vez apuntó al Servicio de Espionaje Ruso (Pérez Cruz, 16 de abril, 2021) e impuso sanciones, pero los ataques aumentan usando nuevas herramientas para evitar ser detectados.

Si bien EE.UU. ha sido el principal objetivo del ataque, también se ha apuntado a organizaciones al menos de 24 países y según explicó Microsoft «Estos ataques parecen ser la continuación de los múltiples intentos de Nobelium de atacar agencias gubernamentales relacionadas con la política exterior, a fin de obtener información válida para el espionaje ruso» (Pérez Cruz, 16 de abril, 2021).

Hoy en día, en la guerra entre Rusia y Ucrania advertimos además del ataque armado, el ataque cibernético. A estos ataques se les conoce como guerra híbrida. En palabras de Hoffman, es una amenaza híbrida «cualquier adversario que emplee de manera simultánea y adaptativa una mezcla fusionada de armas convencionales, tácticas irregulares, terrorismo y comportamiento criminal en el espacio de batalla para lograr sus objetivos políticos» (Hoffman, 2009, p. 3). Fridman se refiere como tal a algún tipo de mezcla entre diferentes medios y métodos militares y no militares de confrontación (Fridman, 2018). Ambos ataques son propios de las guerras de este siglo, cuyas consecuencias pueden ser parecidos a los armados, aunque hasta la fecha, afortunadamente, no hemos presenciado consecuencias similares a los armados.

Hoy, «lo ciber se ha convertido en una herramienta muy seria para perturbar a la sociedad con fines militares» (McGuinness, 6 de mayo, 2017), pero

> los ataques de alto nivel con alto impacto siguen siendo raros. En la mayoría de los casos, los medios cibernéticos se utilizaron para llevar a cabo acciones perturbadoras, y de desestabilización del entorno político, y raramente para la destrucción, por las dificultades para lograr efectos claramente controlables y por las estrategias de contención de los Estados. En cambio, la gran mayoría de los ciber incidentes a los que se enfrentan cotidianamente, empresas y particulares no reciben la misma atención mediática (Fonfría & Duch-Brown, 2020, p. 4).

En estos ataques, las víctimas y los atacantes pueden ser diversos, donde el anonimato del atacante impide al o los Estado/s atacados conocer si detrás está algún Estado, a fin de adoptar los mecanismos establecidos por el DI para defenderse, como la represalia o legítima defensa. Es habitual la sospecha y los indicios contra un Estado, pero sin pruebas contundentes.

Lo cierto es que existe relación entre los ciberataques y los temas geopolíticos y económicos (Chiappetta, 2019; Kausch, 2017). Como dice Kausch, a medida que las amenazas cibernéticas y las amenazas físicas se vuelvan indivisibles, es probable que la «geopolítica cibernética» esté a la vanguardia de la futura competencia geopolítica (Kausch, 2017, p. 2).

En los ataques armados en Estonia, Georgia y Ucrania se han utilizado y utilizan ataques cibernéticos. Con otros países las malas relaciones político-sociales también repercuten en los ataques cibernéticos. Hoy por hoy la animadversión de Rusia hacia los Estados de la OTAN y otros que apoyan a Ucrania en esta guerra, que dura tanto y que tanto daño ocasiona, va creciendo y convierte a estos en el punto de mira de Rusia.

Dadas las dificultades para identificar y determinar la responsabilidad de los ciber atacantes, Cocchine propone acudir a la diligencia debida que implica la obligación del Estado de garantizar la no vulneración de intereses y derechos de los demás Estados, dentro de su territorio o jurisdicción y ante su incumplimiento atribuir responsabilidad internacional por no adoptar las medidas necesarias para evitar un hecho ilícito internacional. Este estándar,

> sería extensible por analogía a las operaciones cibernéticas bajo la forma de un nuevo criterio de "ciberdiligencia debida". Este concepto tiene dos ventajas frente a la regla tradicional de atribución. Uno, soslayaría el problema de atribución técnica de un ciberataque, porque impondría a los Estados vigilar a priori las actividades informáticas potencialmente dañinas desarrolladas en su interior. Dos, la ciberdiligencia debida facilitaría la atribución jurídica, porque atribuiría la responsabilidad internacional al Estado que no adopte las medidas preventivas útiles para evitar un ciberataque que cause "daños significativos" a otro. Todo ello sin necesidad de averiguar el "control efectivo" del Estado territorial sobre el grupo no estatal autor del ciberataque, como pide la regla clásica de la atribución (Cocchine, 2021, p. 3).

La «ciberdiligencia debida» incluiría el deber de reaccionar y de prevenir (Cocchine, 2021, p. 3).

Un ciberataque a escala nacional es un problema que afecta a la sociedad, su seguridad y el orden público. El Estado tiene la obligación de asegurar un orden social en el que los derechos y las libertades fundamentales puedan realizarse plenamente (Tikk, Kaska, & Vihul, 2010, p. 104).

2.3. La ciberseguridad y su fortalecimiento frente a los ciberataques

Los orígenes de la palabra «ciberseguridad» se remontan al año 2000 y se desarrolla con un enfoque multidisciplinar, ya que antes se hacía referencia a la protección de la información conocida como «seguridad informática» (Fonfría & Duch-Brown, 2020, p. 2). Su desarrollo es paralelo al desarrollo tecnológico y como respuesta a los ciberataques. La necesidad de las empresas, los Estados u otros organismos de proteger su información, es cada vez mayor. Estos hechos son reprochables moralmente, pero jurídicamente aún, en su mayoría, no han sido regulados, a nivel nacional ni internacional.

Desde la década de los noventa, dice Fonfría, se advierte un cambio cualitativo en la percepción de las amenazas.

> Gradualmente, se estableció una conexión entre infraestructuras de información y las denominadas infraestructuras críticas, aquellas en la que un fallo o un deterioro

> sustancial podría tener consecuencias dramáticas para la sociedad. La implantación de las tecnologías de la información en estas estructuras es una tendencia que avanza rápidamente y que genera enormes riesgos de ciberseguridad. Basta recordar la cantidad de ciberataques recibidos por hospitales durante la pandemia del COVID-19 para hacerse una idea de los riesgos asociados (Fonfría & Duch-Brown, 2020, p. 3).

En este Siglo se ha aceptado que la «seguridad cibernética» debe identificarse como una preocupación para la seguridad nacional e internacional y por ello, las soluciones de ciberseguridad deben estar guiadas y apoyadas con leyes y prácticas integrales (Tikk, Kaska, & Vihul, 2010, p. 7).

Así, la ciberseguridad es el conjunto de mecanismos, herramientas, estrategias y medidas de protección adoptadas por diferentes entes para proteger su ciberespacio, y evoluciona conforme a las nuevas amenazas y ataques. Los Estados han adoptado medidas como el instituto Nacional de Estándares y Tecnología en EE.UU.; el Centro Nacional de Seguridad Cibernética en Reino Unido, el Centro Australiano de Seguridad Cibernética en Austria, el INCIBE en España[7], el «gran firewall» –proyecto Escudo Dorado– en China, un sistema de censura. También la Unión Europea[8] (Piernas López, 2020, p. 203), la OTAN[9], y la ONU[10]. Estados y OOII coinciden en la necesidad de una cooperación eficaz para enfrentarlos. El objetivo de la ciberseguridad es garantizar y proteger los intereses de los distintos entes. Para Fonfría, los Estados asumen nuevas funciones que coinciden con las tres fases de la política de ciberseguridad. Aparece como propietario de redes o sistemas de información que pueden estar en peligro; como el responsable que debe resolver el problema (política de seguridad), y el Estado –o ciertas unidades individuales del Estado– como causante del problema. Las funciones son cada vez mayores y aumenta la complejidad del ámbito de la política de ciberseguridad.

3. La aplicación del Derecho internacional a los ciberataques

La tecnología avanza y con ella los riesgos de ataques cibernéticos entre Estados. El DI, desde 1945 en adelante, ha ido regulando diversos aspectos que han ido surgiendo en la sociedad internacional, y teniendo en cuenta que el problema del ciberespacio es relativamente nuevo, es importante conocer el avance o inacción del DI frente a este espacio y a los problemas que surgen a través de esta vía.

El análisis de los instrumentos internacionales, aplicables a los ataques en los espacios tradicionalmente conocidos, es necesario para ver si son o pueden ser aplicables al ciberespacio. Los Estados son los encargados, mediante normas internacionales, de restablecer el control del uso indebido del ciberespacio y como garantes de la seguridad actúan maximizando el poder o la seguridad o minimizando amenazas (Fonfría & Duch-Brown, 2020, p. 3). Así, la ciberdefensa debe abordarse a nivel internacional (Tikk, Kaska, & Vihul, 2010, p. 7).

---

[7] En 2013 se ha aprobado la Estrategia de Ciberseguridad Nacional por el Consejo de Seguridad Nacional, y basada en esta en 2019, el Plan Nacional de Ciberseguridad, que constituye el primer nivel en la planificación de la Estrategia de Ciberseguridad Nacional.

[8] Agencia Europea de Seguridad de las redes y la información (ENISA), creada en el 2004 (https://europa.eu/european-union/about-eu/agencies/enisa_es). Un amplio estudio sobre la Ciberdiplomacia y Ciberdefensa en la Unión Europea véase en Piernas, 2020.

[9] Creó en el 2008, el Centro de Excelencia Cooperativa y Defensa Cibernética de la OTAN con sede en Tallin, Estonia (https://ccdcoe.org/).

[10] Cfr. Informe del Grupo de Trabajo de Composición Abierta de la ONU sobre Ciberseguridad. Un acuerdo producto del consenso de 193 Estados (https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf).

3.1. La Carta de las Naciones Unidas y el mantenimiento de la paz y la seguridad internacionales

El desarrollo de la tecnología es un gran avance en muchos aspectos (Morán Blanco, 2017, p. 199)[11], pero su mal uso genera problemas en la seguridad de los Estados, de las personas, y de las empresas.

El art. 1 de La Carta señala como uno de sus propósitos el mantenimiento de la paz y la seguridad internacionales; y el art. 2, los principios básicos que rigen el comportamiento de los Estados miembros, entre ellos, la igualdad soberana de los Estados, la integridad territorial, la prohibición del uso de la fuerza, el arreglo de controversias por medios pacíficos, de tal forma que no se pongan en peligro la paz y la seguridad internacionales, la justicia, la integridad territorial, etc. Estos principios fueron recogidos y ratificados en la Resolución 2625 (ONU, 1970, p. 11).

Para mantener la paz y la seguridad internacionales, el capítulo VII le otorga el papel de gestor de las medidas a adoptar al Consejo de Seguridad. En este contexto nos preguntamos ¿los ataques cibernéticos que representen una amenaza a la paz, quebrantamiento de la paz, pueden ser abordados bajo el capítulo VII? ¿pueden calificarse como agresión?, es decir, ¿una ciberamenaza, un ciberataque puede alterar la paz y la seguridad internacionales? ¿el Consejo de seguridad tiene facultad para pronunciarse sobre ellos? *A priori* la respuesta es no, porque cuando se adoptó La Carta en 1945, el objetivo de los Estados era mantener la paz y la seguridad internacionales de los ataques armados; se referían al uso de la fuerza por las fuerzas armadas (FFAA) y justamente para prevenir y eliminar amenazas a la paz, y para suprimir actos de agresión u otros quebrantamientos de la paz se adoptaron medidas colectivas (Cap. VII). El fin era evitar cualquier acto de agresión y esta se refería al ataque armado.

Conforme a la Resol. 3314 de la Asamblea General (AG) de la ONU (1974) la agresión es «el uso de la fuerza por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de la ONU». Los actos de agresión están vinculados con las FFAA –invasión, ataque, bombardeo, el envío por un Estado, o en su nombre de bandas armadas, grupos irregulares o mercenarios que lleven a cabo uso de la FFAA contra otro Estado de tal gravedad que sean equiparables a los actos de agresión– (art.3).

Si bien los Estados al adoptar la Carta no se planteaban ni remotamente la regulación del ciberespacio ni de los ciberataques, no se puede descartar la posibilidad de que los ataques en el ciberespacio puedan afectar el concepto de amenaza, ya que cualquier ciberataque a un Estado estaría afectando el principio de soberanía de los Estados, e incluso alterando la paz y la seguridad internacionales, según las consecuencias y los efectos que pueden ocasionar. Si bien el ciberespacio, como ha señala Tsagourias, no ha adquirido ningún estatus legal especial en el Derecho internacional, pero las categorías y principios legales existentes, como el principio de soberanía, se han aplicado al ciberespacio y se utilizan para explicar su estatus legal. Dice este autor que el principio de soberanía no es solo un principio legal independiente, sino que también produce consecuencias legales, es decir, hay una reducción de la soberanía en el ciberespacio, aunque esto no significa, que no

[11] En palabras de Morán, el desarrollo de tecnología de la información y las comunicaciones ha generado un nuevo espacio de relación que otorga beneficios y ventajas también en el ámbito internacional, y tiene como características: la rapidez y facilidad de los intercambios de información y comunicación, la ubicuidad y el bajo coste, la efectividad y el impacto.

haya controversias sobre su alcance y contenido o que no se necesiten aclaraciones adicionales. Requieren interpretación y contextualización. Lo que es cierto es que el principio de soberanía se aplica y seguirá aplicándose en el ciberespacio dando forma y racionalizando el comportamiento estatal y las normas internacionales que se aplican o se aplicaran en el futuro al ciberespacio (Tsagourias, 2021, p. 31).

Lo cierto es que los ataques producidos en el ciberespacio pueden tener los mismos efectos que los ocasionados por el uso de la fuerza al que se refiere la Carta y afectar la soberanía del Estado. Ante esta situación Roscini se pregunta si un ciberataque es una acción por debajo del umbral del uso de la fuerza, o un uso de la fuerza, o un uso de la fuerza equivalente a un ataque armado, y concluye que la fuerza cibernética, a diferencia de las operaciones de la CNE, puede calificarse como un uso de la fuerza «armada» en el sentido del art. 2.4, y que solo los ataques cibernéticos a gran escala en infraestructuras críticas que resulten en daños físicos significativos o pérdidas humanas comparables a las de un ataque armado con armas convencionales darían derecho al Estado víctima a la legítima defensa (art. 51 de la Carta) (Roscini, 2010, p. 130). Hay alguna práctica estatal relevante y *opinio iuris* sobre el derecho a la autodefensa contra ataques cibernéticos, lo que podría conducir a la formación de una norma consuetudinaria, aunque la ambigüedad de la posición de ciertos Estados y OOII, hace que sea difícil predecir su resultado (Roscini, 2010, p. 130).

Hoy por hoy, conforme al DI, la violación del principio de soberanía y el uso de la fuerza (*ius cogens*), generan responsabilidad internacional, y su cumplimiento es obligatorio para todos los Estados, hayan o no ratificado un tratado internacional (Quispe Remón, 2012, p. 169), salvo legítima defensa, y un ciberataque con consecuencias similares al uso de la fuerza, debería generar responsabilidad internacional, siempre que se determina e identifique al autor.

Los principios del art. 2 de la Carta estaban pensados para respetar y proteger la soberanía de los Estados sobre los espacios que tradicionalmente se encuentran bajo su jurisdicción, es decir, el espacio terrestre, marítimo y aéreo, en los que se incluyen el espacio ultraterrestre y los espacios polares a los que se suma el ciberespacio, «un nuevo teatro de operaciones de diverso alcance y naturaleza», como un sexto elemento (Gutiérrez Espada, 2020, p. 242). Ese espacio virtual cuyos límites son una tarea casi imposible de determinar porque como dice De Faramiñan,

> al no ser un espacio físico, sino una realidad virtual que se articula con el enjambre de los ordenadores, servidores y redes del mundo ha generado un ámbito de ilegalidad a través del cibercrimen, del ciberterrorismo y la ciberguerra en su uso malsano. Si bien la ciberguerra es la amenaza más importante, que como principal arma utiliza artificios cibernéticos, tales como los virus informáticos, de tal modo que se les ha bautizado como "armas de interrupción masiva" por el descalabro que puede provocar colapsando los sistemas de vida de una población (2021, p. 528).

No olvidemos que el Estado es una entidad territorial y no virtual como el ciberespacio. La prohibición del uso de la fuerza se refiere a las medidas a adoptar ante ataques armados por parte de los Estados, con excepción de la legítima defensa. Las «guerras» a las que se enfrenta la sociedad actual van más allá del uso de las armas, entendidas como tales; hoy se habla de armas cibernéticas o guerras cibernéticas. Algunos consideran a la ciberguerra como la amenaza más importante que el ciberespacio nos trae. Nos recuerda Gutiérrez Espada que antes de la llegada de internet, las guerras se libraban en los espacios físicos, y es desde la década de los noventa con el desarrollo de la infraestructura tecnológica y el uso de las redes cuando el ciberespacio se convierte en un nuevo campo de batalla posible para las

guerras (Gutiérrez Espada, 2020, p. 242). Los efectos pueden ser letales, causando daños económicos, sociales, humanos e inestabilidad política.

Finalmente, los arts. 2.4 y 51 de la Carta se aplican a cualquier uso de la fuerza, al margen de las armas utilizadas conforme dijo la Corte Internacional de Justicia en la opinión consultiva sobre la Legalidad de la amenaza o el empleo de armas nucleares (1996) que ha sido corroborado por el Grupo de Expertos de Tallin de 2013 (Cocchine, 2020, p. 255).

3.2. Los principios básicos del Derecho internacional: Resolución 2625 (1970)

Esta resolución desarrolla los principios del art. 2 de la Carta, e incorpora otros, y los reconoce como «principios básicos del Derecho internacional». Establece que todos los Estados 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 la ONU. Deja dicho que una guerra de agresión constituye un crimen contra la paz que entraña responsabilidad, y que todo Estado tiene el deber de abstenerse de organizar o fomentar la organización de fuerzas irregulares o de bandas armadas, para hacer incursiones en el territorio de otro Estado, de abstenerse de organizar, instigar, ayudar o participar en actos de guerra civil o en actos de terrorismo en otro Estado, o de consentir actividades organizadas en su territorio para la comisión de tales actos, cuando los actos a que se hace referencia impliquen el recurrir a la amenaza o al uso de fuerza.

Establece la obligación de no intervenir ni directa ni indirectamente en los asuntos de jurisdicción interna de los Estados. Así, son violatorios del DI, no solo la intervención armada, sino cualquier otra forma de injerencia o de amenaza que atente la personalidad del Estado, o de los elementos políticos, económicos y culturales que lo constituyen.

> Ningún Estado puede aplicar o fomentar el uso de medidas económicas, políticas o de cualquier otra índole para coaccionar a otro Estado a fin de lograr que subordine el ejercicio de sus derechos soberanos y obtener de él ventajas de cualquier orden. También deberán abstenerse de organizar, apoyar, fomentar, financiar, instigar o tolerar actividades armadas, subversivas o terroristas encaminadas a cambiar por la violencia el régimen de otro Estado y de intervenir en una guerra civil de otro Estado (Resolución 2625 [1970]).

Reconoce el derecho inalienable de los Estados de elegir su sistema político, económico, social y cultural sin injerencia de ningún tipo, y conducir sus relaciones internacionales en lo económico, social, cultural, técnico y comercial, conforme con los principios de igualdad soberana y no intervención. Los Estados deben cumplir sus obligaciones internacionales de buena fe y vivir en paz con los demás. En este sentido, los hechos cometidos a través del ciberespacio por un Estado contra otro Estado con el fin de causar daños, puede considerarse como un acto al que se le aplique la Carta y los principios.

Por otro lado, el Estado que recibe un ciberataque podría acudir a la legítima defensa, pero esto tiene un hándicap, la identificación del agresor, ya que no es tarea fácil y menos inmediata, lo que descartaría su aplicación. Si transcurrido un tiempo se identifica al autor del ciberataque, ya no prosperaría, dado que la inmediatez es un requisito de este principio. Ejercerla más allá de la inmediatez constituiría una violación del DI.

La legítima defensa sería posible frente a un ciberataque que no llega al umbral de un ataque armado, pero que prepara un inminente ataque armado con armas convencionales (Roscini, 2010, p. 130). La ausencia de fronteras en el ciberespacio y la posibilidad que el perpetrador se esconda detrás de *botnets* (Albert Ferrero, 2013, p. 84)[12] o suplantación de IP, podría dificultar la identificación del origen del ciberataque y la aplicación de la ley de responsabilidad estatal, y dado que, en ocasiones, estos ataques provienen de diversos puntos, la represalia se hace difícil porque atacar a los atacantes no surtiría efecto por la imposibilidad de concentración de objetivos y por la duda de si el atacante realizó el ataque deliberadamente o su infraestructura fue secuestrada sin su conocimiento (Ganuza Artiles, 2011, p. 173). Así, el concepto de disuasión en el ciberespacio debe cambiar y basarse en la prevención y en una colaboración internacional y no en una represalia inmediata.

3.3. Ausencia de Tratados que regulen el ciberespacio

Los ataques son cada vez más frecuentes y los mecanismos para repeler inexistentes, por ello la necesidad de saber la forma en que el DI enfrenta estos entre Estados. Qué órgano u órganos serían los competentes para conocer y determinar las responsabilidades.

No existen tratados que regulen específicamente los ciberataques ni el ciberespacio, ni órganos internacionales con competencia expresa para conocer los ciberataques entre sujetos de DI. No obstante, muchos autores coinciden que el DI en vigor es aplicable a las actividades humanas en el ciberespacio, especialmente las que se refieren al uso de la fuerza y a la responsabilidad internacional que resulte de su empleo ilegal (Gutiérrez Espada, 2020, p. 239). Se están refiriendo al entramado jurídico mencionado, la Carta de la ONU, la Resolución 2625 y otros documentos de la ONU. En la misma línea, sobre la necesidad de un tratado internacional que prohíba el uso de la fuerza cibernética entre los Estados, Roscini nos recuerda que la guerra cibernética ya es una realidad y, ante la ausencia de reglas específicas de *ius ad bellum*, nos quedamos con las disposiciones contenidas en la carta de la ONU y en el DI consuetudinario. Estas reglas parecen ser lo suficientemente flexibles como para extenderse a armas que no existían cuando se concibieron: después de todo, esto ya sucedió en el pasado con respecto a las armas nucleares (Roscini, 2010, p. 130).

Por ello, para Fidler, gran parte de las normas que se aplican a problemas de ciberseguridad proceden de pre-derecho internacional cibernético, entre ellos, los principios de no intervención, no uso de la fuerza y ataques sobre objetivos civiles en conflictos armados. La excepción es el espionaje porque el DI no lo prohíbe ni regula (Fidler, 2015, p. 11). Muchos autores coinciden en las dificultades para aplicar el Derecho internacional al ciberespacio (Tsagourias & Buchan, 2021)

En este contexto, Chiappetta recomienda que las naciones se unan para formular leyes y que los órganos de gobierno controlen el uso de armas cibernéticas entre los Estados. Es necesario aumentar la coordinación internacional en este espacio y proteger la resiliencia y la estabilidad de la economía digital mundial. La falta de política hace que los actores malintencionados utilicen como deseen internet, sin ninguna consecuencia (Chiappetta, 2019, p. 72).

[12] Definido como un conjunto de robots informáticos que actúan automáticamente. Se emplea para enviar correos basura no solicitados con fines publicitarios (spams) a direcciones de correo electrónico y para descarga de ficheros que ocupan gran espacio y que consumen gran ancho de banda, o que se reciben, sin permiso o autorización del receptor y de remitentes desconocidos en la mayoría de los casos, con fines publicitarios.

4. Las medidas adoptadas sobre la regulación en el ciberespacio en los últimos años desde el Derecho internacional

Además del DI preexistente, los Estados y las OOII están adoptando medidas para garantizar la seguridad en el ciberespacio a fin de proteger la seguridad del Estado y la de su población. La aproximación de la doctrina a la ciberseguridad se ha producido desde el punto de vista de la seguridad colectiva (Segura Serrano, 2017, p. 291). Sobre la naturaleza jurídica del ciberespacio, por cuanto la infraestructura de internet es tanto pública como privada y que las normas que se le aplican son nacionales e internacionales, Segura Serrano opta por el concepto de *commons* «imperfecto» cuya caracterización «apunta a que podría alcanzarse en un futuro un régimen jurídico claramente internacionalizado para los recursos básicos del ciberespacio, siguiendo los contornos del concepto de patrimonio común de la humanidad» (Segura Serrano, 2017, p. 292).

Si bien hay un consenso sobre la aplicación de normas preexistentes al ciberespacio, esto no significa que el problema esté resuelto, es más, la regulación adecuada conforme a los desafíos que plantea el tema constituye un gran reto para el DI. Urge la adopción de normas específicas que regulen el ciberespacio, y en este camino resultará muy útil, como señala Gutiérrez Espada, «la concertación de un texto internacional con el acuerdo de los Estados sobre los Principios jurídicos fundamentales del DI» (Gutiérrez Espada, 2020, p. 242). Es indispensable la adopción de un tratado específico para su regulación en la que los Estados juegan un papel determinante a través de su soberanía. Pero como señala Tsagourias refiriéndose al ciberespacio «la producción de leyes no es un resultado inevitable de la soberanía porque la soberanía también puede frustrar el proceso internacional de producción de leyes. Sin embargo, si los intereses y necesidades de soberanía de los estados comienzan a converger en torno a ciertos temas, la soberanía puede generar nuevas leyes. Aunque esto parece ser inalcanzable en este momento» (Tsagourias, 2021, p. 31).

Un aspecto a tener en cuenta en la aplicación de la Carta en el ciberespacio es que conforme al capítulo VII, es el Consejo de Seguridad el que adopta las sanciones y si detrás de un ataque cibernético está un Estado miembro del Consejo de Seguridad con derecho a veto, no habrá sanción por parte de la ONU. Esta es una dificultad estructural para tener en cuenta, más aún en este espacio. La realidad muestra que la aplicación de la Carta respecto al uso de la fuerza en espacios tradicionalmente conocidos no surte efectos, es más, es inexistente. Lo estamos viendo en el caso de la invasión de Rusia a Ucrania (Quispe Remón, 2022, pp. 1-9).

4.1. Adopción de Adopción de decisiones en el marco de las Naciones Unidas: El papel de la Asamblea General

La seguridad de la información es un tema que forma parte del programa de la ONU desde que Rusia presentó en 1998 el proyecto de resolución en la Primera Comisión de la AG, «los avances en la informatización y telecomunicaciones en el contexto de la seguridad nacional» que fue aprobada en enero de 1999 (A/RES/53/70).

En esta Resolución, la AG reconoce que los avances científicos y tecnológicos pueden tener aplicaciones civiles y militares, y destaca la importancia de mantener y fomentar el progreso científico y tecnológico en bien de las aplicaciones civiles. Resalta la importancia de los avances para el desarrollo de la civilización, la ampliación de las oportunidades de cooperación para el bien común de todos los Estados, cuya eficacia está condicionada a una amplia cooperación internacional.

Muestra preocupación ante la posibilidad de que estos medios y tecnologías se utilicen con fines incompatibles a garantizar la estabilidad y la seguridad internacionales y afecten negativamente a la seguridad de los Estados. Incide en que se debe impedir la utilización ilícita de los recursos y las tecnologías de la información con fines delictivos o terroristas.

En este contexto pide a los Estados que promuevan el examen multilateral de los peligros actuales y posibles en el ámbito de la seguridad de la información, así como una participación activa, haciendo llegar al Secretario General (SG) sus opiniones y observaciones sobre: la evaluación general de los problemas de la seguridad de la información, determinación de criterios básicos relacionados con la seguridad de la información, en particular con la injerencia no autorizada o la utilización ilícita de los sistemas de información y de telecomunicaciones y de los recursos de información. Asimismo, ve la conveniencia de elaborar principios internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información.

Desde entonces se han adoptado diversas resoluciones en las que se plasman, la importancia del avance de la tecnología y los medios de información para el desarrollo.

Solicita al SG el estudio de los peligros reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para reducirlos, y la preparación de un estudio con la asistencia de un grupo de expertos gubernamentales[13]. En 2004 teniendo en cuenta la Resol. 58/32, el SG estableció el grupo de expertos, y examinó las amenazas reales y potenciales en el ámbito de la seguridad de la información y las posibles medidas de cooperación para enfrentarlas, así como los conceptos internacionales pertinentes orientados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. Desde la Resol. 53/70, el SG incluye en sus informes anuales un punto «los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional», con las opiniones de los Estados Miembros.

Más tarde mediante la Resol. 60/45 del 8 de diciembre de 2005, la AG reitera las resoluciones anteriores y pide a los Estados «seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese sentido de manera compatible con la necesidad de preservar la libre circulación de la información». Se deben revisar los conceptos internacionales pertinentes orientados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. Reitera al SG que, con asistencia del Grupo de expertos Gubernamentales sobre avances en la Información y las Telecomunicaciones en el contexto de la seguridad internacional (GEG) que se establecerá en 2009, siga examinando las amenazas reales y potenciales en el ámbito de la seguridad de la información y las posibles medidas de cooperación para enfrentarlas. Desde el 2010, el SG presenta informes anuales a la AG con las opiniones de los Estados Miembros de la ONU sobre el tema[14].

[13] A/Res/57/53, de 30 de diciembre de 2002 (https://www.itu.int/net/wsis/docs/background/resolutions/57-53-es.pdf))

[14] Entre los informes se tiene: A/65/154 (2010), A/66/152 y A/66/152/Add.1 (2011), A/67/167 (2012), A/68/156 y A/68/156/Add.1 (2013), A/69/112 y A/69/12/Add.1 (2014), A/70/172 (2015).

4.2. Primer informe del Grupo de Expertos Gubernamentales

En 2010, mediante Resol. 65/201, la AG presentó el primer informe «Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional» del GEG sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, creado en 2009 conforme a la Resol. 60/45. De este informe se advierte que las amenazas reales y potenciales en la esfera de la seguridad de la información constituyen uno de los problemas más graves del siglo XXI. Las fuentes de estas amenazas son diversas y se manifiestan como actividades desestabilizadoras dirigidas por igual contra particulares, empresas, elementos de la infraestructura nacional y gobiernos. Sus efectos generan grandes riesgos para la seguridad pública, la seguridad de las naciones y la estabilidad de la comunidad internacional en su conjunto.

El uso creciente de las tecnologías de la información y las comunicaciones (TIC) en infraestructuras esenciales crea nuevos puntos vulnerables y oportunidades para la desestabilización. Por la compleja interconectividad de las telecomunicaciones y de internet, cualquier dispositivo de las TIC puede llegar a ser una fuente o blanco de un uso indebido cada vez más refinado. Reconocen que las tecnologías, por su naturaleza, son de doble uso; por un lado, apoyan a un robusto comercio electrónico, y por otro pueden ser utilizados para amenazar la paz internacional y la seguridad nacional.

El origen, la identidad del autor o los móviles pueden resultar difíciles de determinar, pero por los blancos elegidos, los efectos provocados u otras pruebas que evidencien los hechos pueden deducirse los autores, que pueden estar en cualquier parte del mundo. Estas características, dicen, son las que facilitan el empleo de las tecnologías de la información y las comunicaciones para causar perturbaciones.

La incertidumbre en cuanto a la atribución y la falta de una comprensión común crea el riesgo de inestabilidad y de percepciones erróneas. Señalan que cada vez son más los informes de que los Estados están desarrollando TIC como instrumentos de guerra y para fines de inteligencia y políticos. Muestran preocupación porque los particulares, los grupos u organizaciones, incluidas las delictivas, inicien por cuenta de terceros actividades desestabilizadoras en línea.

El refinamiento y la escala crecientes de la actividad delictiva aumentan la probabilidad de actos perjudiciales. El GEG deja dicho que, si bien no son muchas las indicaciones de uso terrorista de las tecnologías de la información y las comunicaciones para ejecutar operaciones desestabilizadoras, es posible que esto se intensifique en el futuro.

Así, para estos expertos, la lucha contra estos problemas del siglo XXI depende del éxito de la cooperación, entre asociados movidos por ideas similares. Es importante la colaboración entre los Estados y entre éstos y el sector privado y la sociedad civil, y las medidas para mejorar la seguridad de la información, y debe seguir el diálogo entre los Estados a fin de reducir los riesgos y proteger la infraestructura nacional e internacional.

Dado el trabajo del GEG, la AG pidió al Secretario General que continúe el estudio de los peligros existentes y potenciales en el ámbito de la seguridad de la información y las posibles medidas de cooperación para enfrentarse al problema, teniendo en cuenta las evaluaciones y las recomendaciones del informe de 2010, con

la asistencia del GEG que volvería a crearse en 2012, en 2016 y con la del último GEG creado en el 2019.

4.3. Segundo informe del Grupo de Expertos Gubernamentales

El SG remite a la AG (A/68/98 de 24 de junio de 2013), el segundo informe del GEG. Se advierte la preocupación del GEG por los problemas indicados en el primer informe y una serie de recomendaciones para promover la paz y la estabilidad en el uso de las TIC por parte de los Estados. Incluye recomendaciones sobre la adopción de medidas voluntarias de los Estados para incrementar la confianza y la transparencia, y la cooperación internacional para crear capacidad en la esfera de la seguridad de las TIC, especialmente en los países en desarrollo.

De este informe se destaca que el reconocimiento de la aplicación por parte de los Estados de normas derivadas del DI vigente que sean pertinentes para el uso de las TIC, es esencial a fin de reducir los riesgos para la paz, la seguridad y la estabilidad internacionales. No descarta dadas las características singulares de las tecnologías de la información y las comunicaciones la elaboración de normas adicionales.

La conclusión del GEG en este informe es que el DI, y en particular la Carta de la ONU, son aplicables y esenciales para mantener la paz y la estabilidad y para promover un entorno abierto, seguro, pacífico y accesible para las tecnologías de la información y las comunicaciones. Señala que la soberanía del Estado, las normas y los principios internacionales que nacen de ella, son aplicables a la realización de actividades relacionadas con las TIC por parte de los Estados y a su jurisdicción sobre la infraestructura de esas tecnologías dentro de su territorio. Asimismo, que estas iniciativas deben ir de la mano del respeto de los derechos humanos (DDHH) y las libertades fundamentales reconocidos en la Declaración Universal de los Derechos Humanos y otros instrumentos internacionales.

Se debe intensificar la cooperación entre los Estados en la lucha contra el uso de las TIC con fines delictivos o de terrorismo. Inciden en que los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les pueda imputar. «Los Estados no deben valerse de agentes que cometan esos hechos por cuenta de ellos. Los Estados deben asegurarse de que su territorio no sea utilizado por agentes no estatales para hacer uso ilícito de las TIC» (A/68/98 de 24 de junio de 2013). Hay consenso sobre la aplicabilidad al ciberespacio del DI existente, en particular la Carta de la ONU, y las reglas básicas sobre responsabilidad internacional.

4.4. Tercer informe del Grupo de Expertos Gubernamentales

En el informe de 2015 del GEG (A/70/174) se vuelve a insistir en la importancia de la tecnología, pero también en el riesgo que pueda implicar. El SG en el prólogo dice que

> pocas tecnologías han sido tan poderosas como las tecnologías de la información y las comunicaciones a la hora de producir cambios en las economías, las sociedades y las relaciones internacionales. El ciberespacio afecta a todos los aspectos de nuestras vidas. Las ventajas que ofrece son innumerables, pero también conlleva riesgos. Solo se puede lograr que el ciberespacio sea un entorno estable y seguro mediante la cooperación internacional, y la base de esta cooperación deben ser el DI y los principios de la Carta de las Naciones Unidas (A/70/174).

Señala que a todos los Estados les interesa un ciberespacio más seguro, y las iniciativas que se tomen deben respetar el compromiso mundial de favorecer que internet sea abierta, segura y pacífica.

El punto III del informe se refiere a las normas, reglas y principios de comportamiento de los Estados. Un objetivo es seguir determinando qué normas pueden ser voluntarias y no vinculantes para el comportamiento responsable de los Estados y fortalecer un entendimiento común para aumentar la estabilidad y la seguridad en el entorno mundial de las tecnologías de la información y comunicaciones. Según este informe estas normas voluntarias y no vinculantes del comportamiento responsable de los Estados pueden reducir los riesgos para la paz, la seguridad y la estabilidad internacionales.

> Por tanto, las normas no tratan de limitar ni prohibir acciones que, por lo demás, son compatibles con el DI. Las normas reflejan las expectativas de la comunidad internacional, establecen criterios para un comportamiento responsable de los Estados y permiten que la comunidad internacional evalúe las actividades e intenciones de estos. Las normas pueden ayudar a prevenir los conflictos en el entorno de las TIC y contribuir a su utilización con fines pacíficos para permitir que la plena realización de esas tecnologías incremente el desarrollo social y económico mundial (A/70/174).

Señalan que los informes anteriores muestran la existencia de un consenso incipiente sobre el comportamiento responsable de los Estados en lo referente a la seguridad y al uso de las TIC derivado de las normas y los compromisos internacionales existentes.

El GEG recomienda, entre otros aspectos ya mencionados en los informes anteriores, a los Estados, en consonancia con los propósitos de la ONU, su deber de colaborar en la elaboración y aplicación de medidas para incrementar la estabilidad y la seguridad en el uso de las TIC y evitar las prácticas en la esfera de las TIC que se consideran que son perjudiciales o que pueden poner en peligro la paz y la seguridad internacionales.

Deja dicho que los Estados, para garantizar la utilización segura de las TIC, deben acatar las resoluciones 20/8 y 26/13 del Consejo de DDHH sobre la promoción, la protección y el disfrute de los DDHH en internet, así como las resoluciones 68/167 y 69/166 de la AG sobre el derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los DDHH, incluido la libertad de expresión. Incide en la importancia de la cooperación y al derecho inmanente de adoptar medidas compatibles con el DI.

El punto VI aborda la aplicación del DI al uso de las TIC. «La adhesión de los Estados al DI, en particular a las obligaciones que les competen en virtud de la Carta, constituyen un marco esencial para sus acciones en lo que respecta a la utilización de las TIC, así como para promover un entorno abierto, seguro, estable, accesible y pacífico en la esfera de estas tecnologías» (A/70/174).

El GEG considera esencial el compromiso de los Estados con los principios de la Carta y otras normas de DI, para la aplicación del DI a la utilización de estas tecnologías.

«La soberanía de los Estados y las normas y principios internacionales dimanantes de la soberanía se aplican a la realización de actividades relacionadas con las TIC por parte de los Estados, así como a su jurisdicción sobre la infraestructura de esas tecnologías dentro de su territorio» (A/70/174). Del informe se

advierte que la forma en que el DI se aplica al uso por los Estados de las TIC es: que los Estados ostentan la jurisdicción sobre las infraestructuras de TIC ubicadas en su territorio; los Estados, en la utilización de las TIC, deben observar los principios del DI. Las obligaciones existentes en virtud del DI son aplicables al uso por los Estados de las TIC.

Subrayando las aspiraciones de la comunidad internacional de lograr el uso de la TIC con fines pacíficos para el bien común de la humanidad y recordando que la Carta se aplica en su totalidad, señala que los Estados tienen el derecho de adoptar medidas compatibles con el DI como se reconoce en la Carta. Además, se refiere a otros principios jurídicos internacionales, si procede, los de humanidad, necesidad, proporcionalidad y distinción. Señala que los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puede imputar en virtud del DI. No obstante, para el GEG, «la determinación de que cierta actividad relacionada con las TIC se ha puesto en marcha o se ha originado de alguna manera en el territorio o en la infraestructura de las TIC de un Estado podría no ser suficiente en sí misma para atribuir dicha actividad a ese Estado» (A/70/174).

Mediante la Res. 75/32 de diciembre del 2020, la AG, con el fin de enfrentar las amenazas y garantizar un entorno abierto, confiable y seguro en la esfera de la TIC de manera compatible con la necesidad de preservar la libre circulación de la información, exhorta a los Estados Miembros a guiarse por los tres informes del GEG, así como a apoyar las medidas de cooperación mencionadas en los informes.

4.5. Código internacional de conducta para la seguridad de la información

Además, de lo mencionado *supra*, existe una iniciativa promovida por Rusia, China y otros países sobre la elaboración de nuevos acuerdos. Recordemos que fue a propuesta de Rusia que la ONU incorpora el estudio sobre las TIC y en el 2011, los Representantes Permanentes de China, Rusia, Tayikistán y Uzbekistán enviaron una Carta al Secretario General de la ONU, indicando que el desarrollo de las tecnologías más recientes de la información y la telecomunicación pueden ser usadas con fines incompatibles con los objetivos de mantener la estabilidad y la seguridad internacionales, razón por la que los problemas comunes en la esfera de la seguridad de la información se resuelvan mediante la cooperación internacional y respeto mutuo.

Con este fin estos países prepararon un código internacional de conducta para la seguridad de la información (Código de Conducta) y solicitaron la celebración de deliberaciones internacionales en el marco de la ONU sobre dicho código a fin de promover que se logre cuanto antes un consenso sobre las normas y reglas internacionales que rijan las actividades de los Estados en el espacio de la información.

En la resolución (A/66/359) de 14 de septiembre de 2011, por la que se aprueba el Código de Conducta, la AG destaca la necesidad de aumentar la coordinación y la cooperación entre los Estados en la lucha contra la utilización con fines delictivos de la tecnología de la información; reafirma la necesidad de una visión común sobre las cuestiones relativas a la seguridad de internet y el aumento de la cooperación a nivel nacional e internacional; y deja de nuevo establecido que «la determinación de las cuestiones de política pública de la internet es el derecho soberano de los Estados, que tienen derechos y responsabilidades en lo que concierne a las cuestiones de política pública que suscita la internet en el plano internacional». Considera que la confianza y a la seguridad en el uso de las TIC son

un pilar esencial de la sociedad de la información, por ello la necesidad de alentar, conforme a la resolución 64/211 de 2009 la «creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales».

El propósito del Código de Conducta es: determinar los derechos y responsabilidades de los Estados en el espacio de la información, promover su desempeño constructivo y responsable y fomentar su cooperación para hacer frente a las amenazas y los problemas comunes en el espacio informático, para garantizar que las TIC, inclusive en red, se utilicen solo en favor del desarrollo social y económico y el bienestar de la población a fin de mantener la estabilidad y la seguridad internacionales.

La adhesión al Código es voluntaria y abierta a todos los Estados. El compromiso que adquieren, entre otros, son: Cumplir con la Carta de la ONU y otras normas reconocidas universalmente que rigen las relaciones internacionales, como el respeto a los DDHH y libertades fundamentales, a la diversidad y el sistema social de todos los países; los Estados tienen derechos y responsabilidades sobre la protección de su espacio informativo y su estructura de información crítica contra amenazas, ataques.

De lo visto, advertimos que unos apuestan por la aplicación al ciberespacio de la Carta de 1945, otras normas y principios, y otros destacan la necesidad de regular este espacio a través de un tratado específico. No hay consenso y como señala Serrano Segura, hay dos posiciones, la de EEUU y los países occidentales y la de Rusia, China y otros países.

> Los primeros abogan por una aplicación analógica de las normas existentes al ciberespacio y los otros, por nuevas normas. La falta de consenso se atribuye a aspectos políticos y estratégicos, políticas (Internet abierto y protección de los derechos humanos frente a internet cerrado y mayor control estatal) como estratégicas (defensa de la actual ventaja tecnológica frente a ruptura del *statu quo*) (Serrano Segura, 2020, p. 5).

Para Cocchine, es poco probable que los Estados adopten un tratado en el campo cibernético en un futuro inmediato, así acudiendo a Tsagourias y Schimitt afirma que una de las razones está en que los Estados más vulnerables a las amenazas cibernéticas son también aquellos con más capacidades tecnológicas para realizar acciones cibernéticas, por lo que difícilmente querrán ver su libertad de acción en el ciberespacio limitada por un tratado internacional. En esa línea, dice, es más probable que vaya consolidándose una nueva interpretación en torno a las normas convencionales ya existentes, que recoja la práctica actual de los Estados sobre el *jus ad bellum* en el ciberespacio. «Con el paso del tiempo, la práctica internacional puede influenciar la interpretación y aplicación de las disposiciones contenidas en tratados internacionales, hasta dar vida –eventualmente– a una costumbre internacional» (Cocchine, 2020, p. 272).

Lo cierto es que son los Estados los responsables de garantizar un entorno seguro y pacífico en la esfera de las TIC, donde la cooperación internacional es esencial y para que ésta sea eficiente se debe establecer mecanismos para la participación del sector privado, mundo académico y organizaciones de la sociedad civil (A/RES/75/32).

Como ya se dijo, en 2019, la AG de la ONU aprobó la propuesta de Rusia, con apoyo de China, sobre la regulación del cibercrimen, que prevé la creación de un

comité de expertos en 2020 para elaborar una Convención internacional exhaustiva para combatir el uso de las tecnologías de comunicación e información con propósitos delictivos. Sería un tratado universal más completo a diferencia del Convenio de Budapest.

Como resumen en la tabla siguiente se presenta cronológicamente el avance del tema en la ONU.

DOCUMENTO	AÑO	TEMA/TÍTULO
RES 2625	1970	Principios básicos del Derecho internacional
RES 3314	1974	Define a la agresión «como el uso de la fuerza por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado».
RES 53/70	1999	La Federación de Rusia presentó proyecto de Resolución en comisión de Asamblea General "Los avances en la informatización y telecomunicaciones en el contexto de la seguridad nacional".
CONVENCIÓN DE BUDAPEST	2001	Primer Convenio sobre delitos cibernéticos.
RES 58/32	2004	Secretario General estableció el grupo de expertos gubernamentales (GEG), y examinó las amenazas reales y potenciales en el ámbito de la seguridad de la información y las posibles medidas de cooperación para enfrentarlas.
RES 60/45	2005	Invita a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese sentido de manera compatible con la necesidad de preservar la libre circulación de la información.
RES 65/201	2010	Primer informe «Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional» del GEG. Así, para estos expertos, la lucha contra estos problemas del siglo XXI depende del éxito de la cooperación, entre asociados movidos por ideas similares. Destacan la importancia de la colaboración entre los Estados y entre éstos y el sector privado y la sociedad civil, y las medidas para mejorar la seguridad de la información, y brindan recomendaciones para proseguir el diálogo entre los Estados a fin de reducir los riesgos y proteger la infraestructura nacional e internacional.
A/66/359	2011	Aprobación del Código de Conducta, preparado por Rusia, China y otros países, para la seguridad de la información y solicitaron la celebración de deliberaciones internacionales en el marco de la ONU sobre dicho código a fin de promover que se logre cuanto antes un consenso sobre las normas y reglas internacionales que rijan las actividades de los Estados en el espacio de la información. Establece: • Cumplir con la Carta de la ONU y normas reconocidas universalmente que rigen las relaciones internacionales y que consagran, entre otras cosas, el respeto a la soberanía, la integridad territorial y la independencia política de todos los Estados, el respeto a los DDHH y libertades fundamentales y el respeto a la diversidad en la historia, la cultura y el sistema social de todos los países. • No utilizar las tecnologías de la información y las comunicaciones, inclusive en red, para realizar actividades hostiles o actos de agresión, plantear amenazas a la paz y la seguridad internacionales ni contribuir a la proliferación de armas informáticas o tecnologías conexas.

DOCUMENTO	AÑO	TEMA/TÍTULO
A/68/98	2013	La conclusión del GEG en este informe es que el DI, y en particular la Carta de las Naciones Unidas de 1945, son aplicables y esenciales para mantener la paz y la estabilidad y para promover un entorno abierto, seguro, pacífico y accesible para las tecnologías de la información y las comunicaciones. Este informe deja claro, el consenso que existe sobre la aplicabilidad al ciberespacio del DI existente, en particular la Carta de la ONU, y las reglas básicas sobre responsabilidad internacional.
MANUAL DE TALLIN	2013	Documento no vinculante, pero sí de referencia para estos temas, que van en la misma línea de lo establecido en los informes, es decir, sobre la aplicación de la Carta a los hechos derivados del ciberespacio. Actualización en 2017.
A/70/174	2015	Primero, señala que, para garantizar la utilización segura de las TIC, deben acatar las resoluciones 20/8 y 26/13 del Consejo de DDHH sobre la promoción, la protección y el disfrute de los DDHH en internet, así como las resoluciones 68/167 y 69/166 de la AG sobre el derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los DDHH, incluido el derecho a la libertad de expresión. Segundo, vuelve a reiterar que para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de las TIC, es aplicable el Derecho internacional, en particular la Carta de la ONU
	2019	Aprobación de la propuesta de Rusia, con apoyo de China, sobre regulación del cibercrimen
RES 75/32	2020	Exhorta a los Estados Miembros a guiarse por los tres informes del GTG, así como a apoyar las medidas de cooperación mencionadas en los informes

Fuente: Elaboración propia

4.6. Otras iniciativas en el marco de las Naciones Unidas

4.6.1. La Oficina de lucha contra el terrorismo

Cuenta con un equipo especial para la lucha contra el terrorismo que ha formado distintos grupos de trabajo. El Grupo de Trabajo Sobre la Lucha Contra el Uso de Internet Con Fines Terroristas, creado para cooperar con la ONU respetando los DDHH, y teniendo en cuenta otras obligaciones que emanan del DI y estudiar formas de coordinar esfuerzos, a nivel regional e internacional, para luchar contra el terrorismo en todas sus formas en internet; y usar internet como instrumento para luchar contra la propagación del terrorismo reconociendo que los Estados pueden necesitar asistencia en esto.

Esta oficina ha puesto en marcha un programa de ciberseguridad y nuevas tecnologías para fomentar y mejorar las capacidades de los Estados Miembros y las organizaciones privadas en la prevención y mitigación del uso indebido de los avances tecnológicos por los terroristas y extremistas violentos. El fin es mitigar la amenaza y asegurar «que las nuevas tecnologías sigan siendo una fuerza para el bien y no una fuerza para el mal» (Voronkov, 26 de septiembre, 2019).

4.6.2. Relator especial sobre derecho a la privacidad

Creado en 2015 (Resol. 28/16), cuyo mandato ha ido renovándose (ONU, 2018), el último en julio del 2021, con el fin de crear un entorno digital seguro, promoviendo y protegiendo el derecho a la privacidad, un aspecto importante si se quiere garantizar

el ejercicio de otros derechos, como el desarrollo y la libre expresión, la capacidad de participar en la vida política, económica, social y cultural, entre otros. El Relator examina las políticas y las leyes gubernamentales sobre la interceptación de las comunicaciones digitales y la recopilación de datos privados; contribución para garantizar la compatibilidad de las obligaciones nacionales con las internacionales en materia de DDHH, etc.

4.6.3. Oficina de asuntos de desarme

Según la ONU, los avances más relevantes se han producido en esta oficina que, desde 2003, cuenta con un GEG; y desde 2018, con un Grupo de Trabajo de Composición Abierta que estudia, entre otros asuntos, todo lo relacionado con las amenazas existentes y potenciales en el ciberespacio, el comportamiento responsable de los EEMM en este ámbito o la aplicación del DI (ONU, 2020, p. 1).

En el 2018, la AG presentó el informe A/73/505, *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, sobre el informe de la primera comisión de Desarme y seguridad internacional. Esta Comisión presenta dos propuestas planteadas por los Estados: Una encabezada por EE.UU. y otra por Rusia. La primera, de 8 de octubre, sobre Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional presentada por el representante de Estados Unidos en nombre de cuarenta y ocho Estados (A/C.1/73/L.3). Focaliza su atención en la importancia de aplicar los informes anteriores del GEG y en el establecimiento en 2019 de un Grupo de Expertos. La segunda, de 8 de noviembre, sobre Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, planteada por el representante de la Federación de Rusia, en nombre de treinta Estados, que focaliza su atención en el comportamiento responsable de los Estados (A/C.1/73/L.27/Rev.1).

4.6.4. La Unión Internacional de Telecomunicaciones (UIT) y sus avances

Tiene como fin fomentar la confianza y la seguridad en el uso de las TIC; atribuir el espectro de frecuencias radioeléctricas y las órbitas de satélite en el mundo; elaborar las normas técnicas que garantizan la interconexión de redes y tecnologías; y potenciar el acceso a las TIC para las comunidades menos atendidas del mundo[15].

En 2007 lanzó la Agenda de Ciberseguridad Mundial como marco para la cooperación internacional orientado a mejorar la seguridad y la confianza en la sociedad de la información. Sus proyectos sobre la ciberseguridad son: desarrollo de Estrategias de ciberseguridad, con publicación de guías, consejos para ayudar a desarrollarlas, y un banco de datos; creación de Equipos de Respuestas a incidentes informáticos (CSIRT) para ayudar a los EEMM a crear capacidades a nivel nacional y regional, desplegarlas y ayudar a establecer y mejorar los CSIRT; realización de ciber ejercicios a nivel regional y nacional para ayudar en la preparación, la protección y las capacidades de respuesta a incidentes de los países sobre ciberseguridad; seguimiento a las estrategias de los Estados sobre ciberseguridad (Departamento de Seguridad Nacional, 14 de septiembre, 2020). Posee información de los países con Estrategias Nacionales de Ciberseguridad y una guía para crear una estrategia nacional de ciberseguridad (ITU, 2018, p. 76).

[15] Ver su página web (https://www.itu.int/es/Pages/default.aspx#/es)

Realiza encuestas para medir el compromiso de los países con la ciberseguridad y elabora desde 2015 el *Global Cybersecurity Index* (GCI), conforme al Programa Mundial de Ciberseguridad de la UIT, analizando cinco pilares: legal, técnico, organizativo, desarrollo de capacidades y cooperación (ITU, 2018, p. 76). Del último GCI (2020) se advierte que la ciberseguridad es un problema de desarrollo y urge abordar la creciente brecha de cibercapacidad entre países desarrollados y en desarrollo fomentando el conocimiento, mejorando las habilidades y creando las competencias.

Advierte el aumento de los países en la promulgación de las leyes y regulaciones de ciberseguridad en áreas como la privacidad, el acceso no autorizado y seguridad en línea; asimismo la necesidad de establecer estrategias y mecanismos para desarrollar capacidades y ayudar a los gobiernos y a las empresas a prepararse mejor y mitigar los crecientes riesgos cibernéticos. «Más de la mitad de los países del mundo ahora tienen un equipo de respuesta a incidentes informáticos (CIRT) y casi dos tercios tienen algún tipo de estrategia nacional de seguridad cibernética que guía su postura general de seguridad cibernética» (ITU, 2020, p. iv). En este informe participaron 194 países, incluida Palestina.

La ITU durante la COVID compartió información sobre iniciativas, acciones, recursos y proyectos de ciberseguridad, dirigidas al sector público y privado, pequeñas y medianas empresas, usuarios finales y menores, creados para ayudar a garantizar que las comunidades estén conectadas de manera segura. Puso en marcha la Plataforma de Resiliencia de la Red Global para que los reguladores, los responsables políticos y actores interesados, compartan información, conozcan las iniciativas y medidas mundiales diseñadas para ayudar a garantizar que las comunicaciones permanezcan conectadas, y rentabilizar todo el poder y el potencial de las TIC en la crisis (ONU, 2020, p. 4).

4.7. Iniciativas fuera de la ONU

La OTAN promovió la adopción del Manual de Tallín (2013 y 2017) (Cooperative Cyber Defence Centre of Excellence, 2017)[16] que hoy constituye una referencia importante cuando se habla de qué DI es el aplicable al ciberespacio, aunque no es vinculante. Va en la misma línea de lo establecido en los informes de los GEG, es decir, la aplicación de la Carta a los hechos derivados del ciberespacio.

El Consejo de Europa adoptó el primer Convenio sobre delitos cibernéticos (Conv. de Budapest) en 2001, cuyo objetivo es hacer frente a los delitos informáticos y delitos de internet, y en 2006 el Protocolo Adicional. Es el tratado líder que armoniza las normas nacionales y facilita la cooperación en la aplicación de la ley en delitos cibernéticos (Fidler, 2015, p. 11).

Como es de observar encontramos diversas iniciativas en la ONU y en otros órganos, pero no son más que declaraciones de intenciones, sin valor jurídico.

5. Reflexiones finales

El avance de la tecnología sin duda implica desarrollo, pero el uso de la misma ha creado nuevas situaciones a las que hacer frente. Es el caso del uso del ciberespacio para atacar y dañar infraestructura estatal y perjudicar a las empresas y personas.

[16] Elaborado por un Grupo de Expertos internacionales, compuesto por 20 académicos y juristas de reconocido prestigio, que vio la luz en 2012.

Ante ello, tanto los sujetos de DI como los actores nacionales e internacionales han adoptado medidas para proteger sus intereses, a través de la ciberseguridad.

Existen ciertos Estados que con frecuencia están involucrados en ataques cibernéticos, ya sea como presuntos autores o víctimas. La autoría en los ataques es difícil de determinar. Hay un común denominador en los ataques que han tenido mayor repercusión en el mundo, la influencia de la situación política en los mismos.

No hay tratados que regulen gran parte de los problemas ciber, pero sí consenso por parte de la doctrina y por parte del DI, sobre la aplicación del derecho existente al ciberespacio, es decir, la Carta de la ONU y otros instrumentos mencionados a lo largo del trabajo. No obstante, no resulta suficiente, es más, es inexistente e ineficiente en la práctica. No hay más que ver que la aplicación del capítulo VII está en manos de los cinco Estados que tienen derecho a veto y si uno de ellos está incurriendo en violación del DI, como sucede actualmente con Rusia, la Carta no se puede aplicar y por ende no se puede sancionar al violador, a pesar de estar infringiendo una norma de *ius cogens*.

Los ataques contra los sujetos de DI se incrementan, afectando a sus infraestructuras, a las empresas y a los ciudadanos. Generan inseguridad y peligro constante. Nadie escapa a ellos, la ONU fue víctima de estos ataques en julio del 2019. Estos ataques cibernéticos, que cada vez se perfeccionan más y son más sofisticados, son atribuidos a los Estados y/o grupos de cibercriminales organizados.

La ausencia de mecanismos legales hace que se incrementen los ataques y también la impunidad, porque no existen consecuencias jurídicas para los atacantes, sean éstas, personas físicas que actúen por su cuenta o con aquiescencia del Estado. Dado este contexto, la comunidad internacional tiene un reto difícil y dadas las circunstancias urge cada vez más, la regulación del régimen jurídico del ciberespacio.

La regulación del ciberespacio le corresponde al DI, pero esto pasa por la voluntad política de los Estados y su soberanía. Es necesaria una cooperación real y efectiva, con intercambio de información, para hacer frente a este problema.

Antes de la invasión de Rusia a Ucrania, los problemas ciber ya eran una prioridad, pero el incremento de su uso en esta guerra a través de los ataques cibernéticos hace que el reto que asume el Derecho internacional Público sea colosal, además de prioritario. A ello deben sumarse las campañas de sensibilización, tanto a nivel nacional como internacional, a fin de mostrar los riesgos reales a los ciudadanos.

Muchos de los Estados consideran suficiente la aplicación de las normas preexistentes que datan de mediados del S. XX. Probablemente sean adecuadas en un inicio, por la rapidez del desarrollo de la tecnología, pero no suficientes para enfrentar el problema de manera efectiva. A los hechos reales y actuales me remito.

Se requiere un tratado específico, que recoja un concepto de ciberespacio, sus alcances, límites, características, y demás aspectos. Es importante conocer taxativamente el papel de los Estados en este espacio. El desarrollo del DI del ciberespacio contribuirá también a determinar la responsabilidad internacional de los Estados por los ciberataques originados desde su territorio.

El DI es dinámico y evoluciona conforme a las necesidades que van surgiendo en la sociedad internacional y en el caso materia de estudio, no tiene por qué ser de manera diferente; por ello, se espera que vaya a la par del desarrollo tecnológico, más

si se tiene en cuenta el incremento de las amenazas y ataques a través de este espacio.

Son muchos los que abogan por la aplicación del derecho preexistente al ciberespacio, pero también existen propuestas en el marco de la ONU sobre la necesidad de una regulación específica, aunque teniendo en cuenta los intereses de los Estados, que lamentablemente siempre priman sobre el interés general, y visto la evolución en los últimos diez años, no se avizora a corto ni mediano plazo ningún instrumento global que regule el ciberespacio de manera específica.

Bibliografía

A/HRC/RES/37/2, O. (2018). *Resolución Aprobada por el Consejo de Derechos Humanos.* ONU.

Agencia EFE. (5 de febrero, 2015). Estados Unidos, Reino Unido y España, los más atacados cibernéticamente. *Primera hora.* https://www.primerahora.com/noticias/mundo/notas/estados-unidos-reino-unido-y-espana-los-mas-atacados-ciberneticamente/

Albert Ferrero, J. (2013). La Ciberguerra. Génesis y evolución. *Revista General de Marina,* 264 (mes 1-2), 81-97.

BBC. (7 de enero, 2017) Qué dice el informe de inteligencia desclasificado que culpa a Rusia y a Putin de ordenar ciberataques para influir en las elecciones de Estados Unidos. *BBC*. (https://www.bbc.com/mundo/noticias-internacional-38545605).

BBC. (15 de mayo, 2017). Microsoft responsabiliza a la Agencia de Seguridad Nacional de Estados Unidos de propiciar el ciberataque masivo que afectó al menos a 150 países. *BBC.* https://www.bbc.com/mundo/noticias-internacional-39918517

Caro Bejarano, M. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Cuadernos de Estrategia,* (149), 48-82.

Centro Criptológico Nacional. (2015). *Guía de seguridad (CCN-STIC-401), Glosario y abreviaturas*. Ministerio de la Presidencia. https://www.ccn-cert.cni.es/es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file?format=html.

Chiappetta, A. (2019). The cybersecurity impacts on geopolitics. *FormaMenta,* XIV (1), 61-74.

Cocchine, A. (2020). ¿Es necesario un nuevo "jus ad bellum" frente al uso de la (ciber) fuerza y a los ciberataques (armados)? En M. Cervell Hortal, *Nuevas tecnologías en el uso de la fuerza: Drones, armas autónomas y ciberespacio* (págs. 249-277). Thomson Reuter Aranzadi.

Cocchine, A. (2021). Ciberseguridad debida: ¿una actualización necesaria para el Derecho Internacional del ciberespacio? *ARI Real Instituo Elcano,* (27), 1-6.

Cooperative Cyber Defence Centre of Excellence. (2017). Tallin Manual 2.0 on the international law applicable to ciberoperations. Cambridge University Press.

De Faramiñan, G. (2021). Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio [Recensión]. *Anuario Español de Derecho Internacional, 37*, 527-530.

Departamento de Seguridad Nacional. (14 de septiembre, 2020). 75º Aniversario de Naciones Unidas y la ciberseguridad mundial. *Departamento de Seguridad Nacional. Gabinete de la Presidencia del Gobierno*. https://www.dsn.gob.es/es/actualidad/sala-prensa/75%C2%BA-aniversario-naciones-unidas-ciberseguridad-mundial

DW. (5 de enero, 2019). Seis ataques cibernéticos que sacudieron el mundo. *DW.* https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

Fidler, D. (2015). Whither the web? International Law, Cybersecurity, and critical infrastructure protection. *Georgetown Journal of International Affairs,* 16, 8-20.

Fonfría, A., & Duch-Brown, N. (2020). Elementos para una política de ciberseguridad efectiva. *ARI Real Instituto Elcano* (127).

Fridman, O. (2018). *Russian 'Hybrid Warefare': Resurgence and Politicisation.* Oxford University Press.

Ganuza Artiles, N. (2011). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia,* (149), 165-214.

Gutiérrez Espada, C. (2020). ¿Existe (ya) un derecho aplicable a las actividades en el ciberespacio? En M. Cervell Hortal, *Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberepacio* (págs. 225-248). Thomson Reuters Aranzadi.

Hoffman, F. (2009). Hybrid vs. Compound War. The Janus Choice of Modern War: Defining Today`s Multifaceted Conflict. *Armed Forces Journal, October*, 1-17.

ITU. (2018). *Guide to developing a national cibersecurity Strategy.* ITU.

ITU. (2020). *Global Cibersecurity Index 2020 Measuring commitment to cibersecurity.* ITU publications.

Kausch, K. (2017). Cheap Havoc: How Cyber-Geopolitics will destabilize the Middle East. *JSTOR*, 1-17.

Mars, A. (13 de mayo, 2021). Biden insta a Moscú a actuar contra el grupo responsable del ciberataque al oleoducto. *El País.* https://elpais.com/internacional/2021-05-13/biden-insta-a-moscu-a-actuar-contra-el-grupo-responsable-del-ciberataque-al-oleoducto.html#

McGuinness, D. (6 de mayo, 2017). Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. *BBC News.* https://www.bbc.com/mundo/noticias-39800133

Monge, Y. (28 de mayo, 2021). Un ciberataque de origen ruso vuelve a golpear al Gobierno de Estados Unidos. *El País.* https://elpais.com/internacional/2021-05-28/un-ciberataque-de-origen-ruso-vuelve-a-golpear-al-gobierno-de-estados-unidos.html

Morán Blanco, S. (2017). La ciberseguridad y el uso de las tecnologías de la información y la comunicación por el terrorismo. *Revista Española de Derecho Internacional,* 69 (2), 195-221.

Norris, M. (2013). The Law of Attacks in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace. *Inquiries Journal,* 5(10), 1-7.

ONU. (1970). La declaración relativa a los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas. *RESOLUCIÓN 2625 (XXV) de la Asamblea General de Naciones Unidas, de 24 de octubre de 1970* (pág. 11). ONU.

ONU. (2018). El derecho a la privacidad en la era digital (Resolución A/HRC/RES/37/2) Aprobada por el Consejo de Derechos Humanos). ONU.

ONU. (2020). *75º Aniversario de Naciones Unidas y la ciberseguridad mundial.* ONU. https://www.dsn.gob.es/es/actualidad/sala-prensa/75%C2%BA-aniversario-naciones-unidas-ciberseguridad-mundial

Pérez Cruz, C. (16 de abril, 2021). Biden tensa la cuerda y anuncia nuevas sanciones contra Rusia. *Ara.* https://es.ara.cat/internacional/biden-tensa-cuerda-anuncia-nuevas-sanciones-rusia_1_3949974.html.

Piernas López, J. (2020). *Ciberdiplomacia y Ciberdefensa en la Unión Europea.* Aranzadi.

Quispe Remón, F. (2012). Las normas de ius cogens: ausencia de catálogo. *Anuario Español de Derecho Internacional,* 28, 143-183.

Quispe Remón, F. (2021). El Derecho internacional y los ODS: la eficacia en su cumplimiento a seis años de su puesta en marcha. *Revista Iberoamericana De Estudios De Desarrollo,* 11 (2), 196–224. https://doi.org/10.26754/ojs_ried/ijds.690

Quispe Remón, F. (15 de marzo, 2022). El futuro de Putin ¿condena o impunidad? *Infolibre*, 1-9.

Roscini, M. (2010). World Wide Warfare-jus ad bellum at the Use of Cyber Force. *Max Planck Yearbook of United Nations Law,* 14, 85-130.

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

Serrano Segura, A. (2020). Ciberseguridad y normación en Derecho Interacional. *Fundación Euroarabe,* (5), 1-5.

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Ciber Incidents: legal considerations.* Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

Tsagourias, N. (2021). The legal status of cyberspace: sovereignty redux? En T. y. Buchan, *Research Handbook on International Law and Cyberspace* (págs. 9-31). Elgar.

Tsagourias, N., & Buchan, R. (2021). *Research Handbook on International Law and Cyberspace.* Elgar.

Voronkov, V. (26 de septiembre, 2019). Remarks by Mr. Vladimir Voronkov, [Discurso], Side-Event on Countering Terrorism with New and Emerging Technologies.