Actividades cibernéticas y seguridad internacional: Hacia un régimen de normas de comportamiento estatal responsable y medidas de fomento de la confianza

Cyber activities and international security: towards a regime of norms of responsible state behaviour and confidence-building measures.

Por Laura Jamschon Mac Garry

Resumen: Este artículo tiene por fin analizar algunas cuestiones terminológicas en torno al estudio del uso malicioso de las tecnologías de la información y la comunicación (TIC) y su impacto en la seguridad y paz internacionales. En segundo lugar, abordará las características propias del ciberespacio y de las actividades cibernéticas para establecer puntos en común con otros dominios, así como particularidades que requieren un abordaje más original. Finalmente, hará una breve reseña respecto al trabajo que se viene desarrollando en las Naciones Unidas para abordar la seguridad internacional en el marco del uso de las TIC.
Palabras clave: ciberespacio; TIC; derecho internacional público; Naciones Unidas; multilateralismo

Abstract: The purpose of this article is to analyse some terminological issues surrounding the study of the malicious use of information and communication technologies (ICTs) and their impact on international security and peace. Secondly, it will address the characteristics of cyberspace and cyber activities in order to establish commonalities with other domains and particularities that require a more original approach. Finally, it will briefly review the work being developed at the United Nations to address international security in the context of the use of ICTs.
Keywords: Cyberspace; ICTs; public international law; United Nations; multilateralism

Fecha de recepción: 27/03/21

Fecha de aceptación: 13/05/21

Actividades cibernéticas y seguridad internacional: Hacia un régimen de normas de comportamiento estatal responsable y medidas de fomento de la confianza

Por Laura Jamschon Mac Garry[1]

I. Introducción

Las actividades cibernéticas maliciosas no son más una ficción o una preocupación para el futuro, sino que son una real y actual inquietud en el presente. Una intrusión cibernética puede llegar a comprometer derechos fundamentales de una persona humana, afectar intereses de una empresa o el funcionamiento de estructuras críticas, perturbar el bienestar de la sociedad toda y/o la seguridad y estabilidad de un Estado. Estas actividades maliciosas pueden ser conducidas por actores estatales o no estatales (criminales, terroristas e intermediarios del Estado).

Este artículo está dividido en tres partes: la primera abordará las cuestiones terminológicas que deben preceder cualquier análisis legal y político. A tal efecto, examinaremos una serie de conceptos que aún no cuentan con una definición universal, pero que son utilizados permanentemente en el tratamiento del tema. En segundo lugar, reseñaremos una serie de características propias del ciberespacio y de las actividades que se desarrollan en él. Finalmente, la tercera parte se focalizará en estudiar los avances que se han hecho en las Naciones Unidas respecto a tecnologías de la información

[1] Abogada (Universidad de Buenos Aires), diplomática de carrera (SEN), LL.M. (Universidad de Viena), Doctoranda (Sapienza Universidad de Roma). El presente trabajo es parte de una investigación de doctorado. Las opiniones vertidas son de carácter estrictamente personal y no reflejan posición de institución alguna a la cual la autora pueda estar vinculada. Correo electrónico: laura.jamschonmacgarry@uniroma1.it

y la comunicación (en adelante, "TIC") en el contexto de la seguridad internacional. El artículo concluye sosteniendo que es fundamental un acuerdo sobre la terminología a emplear y que es necesario homogeneizarla; que hay características en el ámbito cibernético que se verifican en otros dominios, lo que puede ser útil para establecer paralelismos regulatorios, y que el trabajo de las Naciones Unidas es un claro ejemplo de que el multilateralismo es el medio adecuado para reunir *expertise* técnico, legal y político.

II. Terminología

Cualquier jurista es consciente de que la precisión terminológica en derecho es de fundamental importancia. Es por ello que desde el inicio seleccionaremos una serie de conceptos, identificaremos algunas definiciones que la literatura o la práctica estatal ha dado hasta el momento y sugeriremos que es necesario acordar algunas definiciones para que cualquier iniciativa regulatoria sea clara y prometa una uniforme aplicación y un cumplimiento extendido.

II.1. El ciberespacio

El primero de los términos que hemos escogido es "ciberespacio". Si bien es una palabra incorporada al lenguaje cotidiano, requiere algunas precisiones. De esto se ha ocupado la Unión Internacional de Telecomunicaciones (UIT), que ha desarrollado una guía para que los Estados desarrollen sus estrategias cibernéticas. En la misma, la UIT utiliza el término "ciberespacio" para describir sistemas y servicios directa o indirectamente conectados con Internet, con las telecomunicaciones y con los sistemas informáticos (UIT, 2011).

Ya son varios los Estados que en sus documentos de política interna, en donde definen sus estrategias en materia de ciberseguridad, abordan este concepto. Las definiciones a nivel nacional varían en cuanto a la descripción del ciberespacio como un "dominio", como una "red de infraestructuras tecnológicas" o como un "ambiente" y en algunos casos se hace referencia al carácter estratégico de la información o de los sistemas que comprende. En otros se enfatiza que es un dominio global creado por el ser humano, lo que permite diferenciarlo de otros dominios globales naturales, como el espacio ultraterrestre, la Antártida o la alta mar. La Argentina, por ejemplo, definió este concepto del siguiente modo:

> "dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de la información y de telecomunicaciones, tiene entre otras, como características esenciales, su dimensión global y transfronteriza, su naturaleza dual, su masividad y su vertiginosa y constante evolución" (Argentina, 2019).

En el ámbito académico, en 2013 un grupo de expertos de distintos países redactó la primera versión del Manual de Tallin sobre Derecho Internacional Aplicable a la Guerra Cibernética (en adelante, "Manual de Tallin"). Dicha obra incluye un glosario al final, en el que se define el "ciberespacio" como el ambiente formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos usando redes informáticas (Schmitt, 2013).

II.2. "Ciberseguridad" y "seguridad de la información"

Probablemente, exista una mayor familiaridad con el prefijo "ciber" y con el término "ciberseguridad". Sin embargo, es importante resaltar que en el ámbito de las Naciones Unidas y, más precisamente, en el marco del trabajo de la Primera Comisión de la Asamblea General en el tema, la terminología utilizada fue variando a partir de la expresión inicial, que fue "seguridad de la información". En efecto, en sus orígenes en

1998, la propuesta de trabajo sobre el tema fue presentada por la Federación de Rusia empleando dicha expresión. Podemos verificar que "seguridad de la información" es el lenguaje que utiliza la Doctrina de Seguridad de la Federación de Rusia (Federación de Rusia, 2008) y también es la terminología utilizada en el Programa Nacional de medio y largo plazo para el Desarrollo de la Ciencia y la Tecnología (2006-2020) de China (China, 2006). Esta misma terminología fue empleada en la propuesta de un código internacional de conducta para la seguridad de la información, presentada por las delegaciones de China, la Federación de Rusia, Tayikistán y Uzbekistán (Naciones Unidas, 2011). Asimismo, esta es la expresión que utilizó el informe de 2010 del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (en adelante, "GEG").

La propuesta de trabajo sobre seguridad de la información se materializó posteriormente en una resolución de la Asamblea General que se adoptó sin votación (Asamblea General, 1998). Sin embargo, con el tiempo, algunos Estados presentaron reparos en torno a dicho lenguaje, por lo que su denominación fue mutando.

Cabe señalar que la discusión terminológica no es una mera cuestión de forma, sino de sustancia, y de ello nos dan cuenta los comentarios de algunos Estados en respuesta a la invitación de la Asamblea General a expresar opiniones sobre la temática. Por ejemplo, algunos Estados expresaron preferencia por el término "ciberseguridad" indicando que "seguridad de la información" es una expresión que algunos países y organizaciones utilizan como parte de una doctrina que considera a la información misma como una amenaza (Naciones Unidas, 2013; 2014; 2015b; 2016; 2017).

En el ámbito regional, tampoco existe un lenguaje uniforme: la Estrategia Interamericana Integral de Seguridad Cibernética (OEA, 2004) –como lo indica su nombre- utiliza el término "seguridad cibernética". La Unión Europea adoptó en 2013 la Estrategia de Ciberseguridad de la Unión Europea y en 2016 la Directiva para la Seguridad de las Redes y Sistemas de la Información (Directiva NIS, 2016), ambos con terminología diferente.

II.3. "Operaciones de la información" - "operaciones cibernéticas" y "ataques cibernéticos" - "ataques de la información"

Las actividades cibernéticas maliciosas abarcan un abanico con distintas gradaciones de daños, que pueden ir desde lo material a lo inmaterial, de lo inmediato a lo remoto, de lo directo a lo indirecto. En términos prácticos, podemos hablar de robo o destrucción de la información, de acceso no autorizado para espiar o para preparar otra actividad maliciosa posterior, de destrucción física o de disfuncionalidad. Respecto a las actividades maliciosas de baja intensidad se suele hablar de "incidentes"; cuando el objetivo es robar información, se suele hablar de "explotación" y en el caso de las de mayor intensidad (escala y efectos), la literatura suele denominarlas "ataques".

Si bien en el ámbito multilateral no se suele utilizar la expresión "operaciones de la información", la literatura que se nutre de la doctrina militar norteamericana sí utiliza ampliamente esta expresión. Se suele hacer referencia a la definición de una publicación conjunta de la Armada y la Marina norteamericanas, que las definió como el empleo integrado, durante las operaciones militares, de las capacidades relacionadas a lo informático en concierto con otras líneas de operación para influir, perturbar, corromper o usurpar la toma de decisiones de los adversarios y potenciales adversarios, al tiempo que se protege a los propios (Estados Unidos, 2012).

Si bien algunos autores han considerado que la expresión "operaciones de la información" abarca las actividades cibernéticas maliciosas, incluso si son llevadas a cabo en tiempos de paz (Schmitt, 2002), o si son desarrolladas por el sector privado o gubernamental más allá de un conflicto militar (Kuehl, 2002), lo cierto es que otra parte de la doctrina no distingue entre "operaciones de la información" y "guerra de la información". Dentro de esa segunda postura, autores como Hollis (2007) sostienen

que la información y los sistemas informáticos son considerados bajo esta denominación como herramienta y objetivo militar. En esa misma línea, Cox utiliza las expresiones "guerra de la información" y "operaciones de la información" indistintamente (Cox, 2005).

Por su parte, el Manual de Tallin define las "operaciones cibernéticas" como el empleo de capacidades cibernéticas con el fin primario de lograr objetivos en o a través del ciberespacio (Schmitt, 2013). Algunos autores han considerado que la diferencia entre "operaciones cibernéticas" y "operaciones de la información" es que las últimas son una categoría más amplia que incluye las operaciones cibernéticas, así como las capacidades electrónicas, militares y psicológicas (Roscini, 2014).

Cuando las definiciones se refieren a un conflicto subyacente, en donde hay adversarios, objetivos, capacidades y un marco operacional (ligado a lo militar), podemos concluir que dicho lenguaje desde un punto de vista textual restringe su aplicación a un determinado tipo de contexto que no es el de paz, sino el de conflicto armado.

Ahora veamos el concepto de "ataque cibernético" (o "ataque de la información"). Autores reconocidos en la materia han descripto estas actividades maliciosas como una categoría restringida aplicable a operaciones cibernéticas hostiles particularmente atroces que permiten la más enérgica de las respuestas del Estado (Schmitt y Vihul, 2014, p. 7). Característico de este grupo de actividades maliciosas es la gravedad de las consecuencias y no el acto en sí. Algunos autores como Lin le agregan un elemento intencional (es decir, que la actividad cibernética en cuestión sea deliberada) y otro temporal (en otras palabras, que tenga cierta duración) (Lin, 2010).

Los expertos de Tallin construyeron la definición de "ataque cibernético" a partir del art. 49(1) del Protocolo Adicional I a las Convenciones de Ginebra, que establece que los "ataques" son actos de violencia contra el adversario, ya sea de forma ofensiva o defensiva (Ginebra, 1977). A partir de dicha noción, la Regla 30 del Manual de Tallin

definió el "ataque cibernético" como una operación informática, ya sea ofensiva o defensiva, que se espera que razonablemente cause daño o muerte a personas o daño o destrucción de objetos (Schmitt, 2013).

Aquí vemos nuevamente no solo la utilización de lenguaje militar, sino la directa conexión con el concepto de "operación cibernética", lo que nuevamente limita su ámbito de aplicación. Es importante recordar que una actividad cibernética maliciosa puede activarse por medio de personal civil o militar; con fines económicos o políticos y no necesariamente siempre militares.

II.4. "guerra cibernética" - "guerra de la información" y "armas cibernéticas" - "armas de la información"

Una parte de la doctrina incluso utiliza un lenguaje militar aún más explícito. En dicho marco se incluyen términos como "guerra" y "armas". El término "guerra" es un tanto anacrónico ya que después de la Segunda Guerra Mundial se ha extendido la utilización de la expresión "conflicto armado".

El militar prusiano von Clausewitz describió a principios del siglo XIX la guerra como un acto de la política y como una pulsación de violencia (von Clausewitz, 2007, p. 28). Otra tradicional definición de "guerra" es la que ofreció Oppenheim a principios del siglo XX, al referirse a dicho término como la contienda entre dos o más Estados por medio de sus fuerzas armadas para dominar al otro e imponer las condiciones de paz que el vencedor desee (citado en Dinstein, 2003, p. 5). Y a principios del siglo XXI, otro autor que contribuyó a la definición de este concepto es Dinstein, quien lo describió como una interacción hostil entre dos o más Estados, ya sea en sentido técnico (con una declaración de guerra) o material (con el efectivo uso de la fuerza) (Dinstein, 2003, p. 15).

Por su parte, el Comentario de 1987 al Protocolo Adicional II a las Convenciones de Ginebra clarifica que el criterio material de un "conflicto armado" es la existencia

de hostilidades abiertas entre fuerzas armadas organizadas en mayor o menor grado (Ginebra, 1987).

En el ámbito más específico relativo al espacio cibernético, podemos afirmar que no hay una definición universalmente acordada de "guerra de la información" (Aldrich, 1996). Los autores que distinguen entre "operaciones de la información" y "guerra de la información" han considerado la última como un sub-grupo de las primeras (Schmitt, 2002) y cuya característica principal es que es una operación de la información llevada a cabo en tiempos de crisis o conflicto (Kuehl, 2002). En otras palabras, es lo mismo que una operación militar con medios convencionales, pero llevada a cabo por medios cibernéticos (Brenner, 2007).

Ahora, analicemos el concepto de "armas cibernéticas" (o "armas de la información"). El art. 36 del Protocolo Adicional I a las Convenciones de Ginebra implica la obligación de establecer procedimientos domésticos para determinar la legalidad de un arma; sin embargo, dicho instrumento no define ese concepto. Blake e Imburgia (2010) han explicado que cualquier *capacidad*, ofensiva o defensiva, contra un objetivo militar o combatiente enemigo puede ser considerada domésticamente como un arma; sin embargo, estos autores destacaron que los Estados puede evitar querer designar las capacidades cibernéticas como armas, para impedir que su uso quede comprendido bajo la calificación de "ataque armado" del art. 51 de la Carta de las Naciones Unidas. Cabe recordar que la Corte Internacional de Justicia enfatizó que las cláusulas del capítulo VII de la Carta de las Naciones Unidas se aplican a cualquier uso de la fuerza, sin importar el tipo de armas (Nuclear Weapons, 1996).

En ese marco, Dinstein (2002) admitió que una computadora puede ser un arma porque lo relevante no es el medio sino las consecuencias violentas que produce. El enfoque basado en los efectos es el que mayor adhesión tiene hoy en día en materia de guerra cibernética (Buchan, 2012). Así, también Boothby (2012) consideró que el uso de cualquier instrumento –incluso una computadora– que sea utilizado con fines destructivos o dañinos hacia la otra parte en un conflicto lo transforma en un arma o

un medio de guerra. En virtud de ello, Sharp (1999) argumentó que cualquier ataque a un sistema informático que intencionalmente cause cualquier efecto destructivo en otro Estado puede crear los efectos de un uso de la fuerza que dé lugar a la legítima defensa.

Ahora veamos cómo el grupo de expertos del Manual de Tallin ha definido el concepto "armas cibernéticas". El comentario a su Regla 41 nos brinda una respuesta: tales armas son medios de guerra que –ya sea por su diseño, uso efectivo o previsto– pueden lesionar o causar muertes humanas y/o daños o destrucción material; es decir, causan las consecuencias necesarias para considerar la operación cibernética un "ataque cibernético" de acuerdo a la Regla 30 (Schmitt, 2013).

En la literatura especializada abundan clasificaciones de armas cibernéticas. Por ejemplo, Brenner (2007) ha diferenciado tres clases: 1) armas de destrucción masiva, que son aquellas de efectos destructivos devastadores; 2) armas de distracción masiva, que son aquellas que generan pánico o confusión social generalizada y 3) armas de interrupción masiva, que derivan en un amplio descreimiento sobre la habilidad del gobierno de mantener el funcionamiento de los servicios esenciales.

Por su parte, Raboin (2011) distinguió cinco tipos de armas cibernéticas: 1) la denegación de servicio, que consiste en la coordinación y uso de numerosas computadoras pre-infectadas trabajando al unísono para inutilizar una red o servicio informático identificado como objetivo; 2) el software malicioso o malware, que consiste en un programa que interrumpe las funciones normales de la computadora; 3) las bombas lógicas, que consisten en una amenaza que permanece latente hasta que el operador decide activarla, 4) la suplantación de IP, que tiene por fin acceder al sistema con una identidad oculta y 5) los troyanos, que permiten el acceso remoto no autorizado a una computadora.

Otros autores reducen la lista de armas cibernéticas a virus, gusanos y bombas lógicas (Cox, 2005) o, por el contrario, la expanden hasta incluir *sniffers* (para robar

claves y credenciales de acceso a información estratégica), *spamming* (inundar un sistema bloqueando las comunicaciones genuinas), *video morphing* (para manipular la difusión de noticias del adversario), entre otras (Joyner y Lotrionte, 2001).

El análisis terminológico de esta sección nos permite demostrar la diversidad conceptual y concluir que cualquier abordaje futuro deberá aclarar ciertos términos a efectos de que el trabajo sobre normas de comportamiento estatal responsable y medidas de fomento de la confianza no sea vago o incierto. Es dable señalar que la ambigüedad del lenguaje solo contribuiría a una mayor dificultad en la aplicación de cualquier instrumento no vinculante porque –a diferencia de los tratados, cuya guía de interpretación es la Convención de Viena sobre el Derecho de los Tratados– las herramientas de *soft law* no cuentan con tal orientación para indagar su alcance (Beard, 2017).

III. Características del ámbito cibernético

Esta sección abordará las características del espacio cibernético, por un lado, y de las actividades cibernéticas, por el otro. Con esta tarea nos proponemos identificar las particularidades propias en este ámbito y las características que comparte con otros dominios, lo que permitirá trazar paralelismos que sirvan de guía para eventuales futuros marcos regulatorios.

III.1. El dominio cibernético como un espacio global común

En el ciberespacio no existe la conexión entre territorio y soberanía (Shackelford, 2009), por ello, no sólo parte de la literatura, sino que también algunos Estados describen el ciberespacio como un espacio común global.

Ya vimos que la Estrategia Nacional de Ciberseguridad de la Argentina definió el ciberespacio como un dominio global. El Departamento de Defensa norteamericano

ha descripto el ciberespacio como un espacio global (Estados Unidos, 2005). Por su parte, la alianza de comando de la Organización del Tratado del Atlántico Norte (OTAN) lo ha descripto como un espacio que no es de ningún Estado o entidad y que es potencialmente accesible a todos (OTAN, 2011).

Sin embargo, podemos reconocer en el léxico especializado que en algunos casos se habla de "soberanía en el ciberespacio". Por ejemplo, China incluyó esta expresión en su Estrategia de Cooperación en el Ciberespacio, definiéndola como el derecho de un Estado a elegir de forma independiente el camino de desarrollo cibernético, modelo de regulación del ciberespacio, la política pública sobre Internet, así como la capacidad de participar de forma igualitaria en la gobernanza del ciberespacio (China, 2017). Por su parte, la Federación de Rusia ha desarrollado un robusto andamiaje legal a nivel interno para asegurar la soberanía cibernética, que incluye la Ley de soberanía de Internet y la Ley Yarovaya (Tabachnik y Topor, 2020).

Shackelford (2009) ha presentado dos posibles modelos de regulación de este dominio: considerar el ciberespacio como un espacio en donde los Estados pueden ejercer su soberanía a través del principio de los efectos, es decir, ejercer jurisdicción donde las actividades cibernéticas impactan. El otro modelo, es considerarlo como un espacio global común sobre el cual no se puede afirmar ningún tipo de jurisdicción. En este último caso, explica, se aplicaría el concepto de patrimonio común de la humanidad, el cual implica –además de la no apropiación– la gestión común de los recursos, la distribución de los beneficios, la desmilitarización y desarme y su uso sostenible con el fin de preservarlo para futuras generaciones.

Podemos incluir la postura de Segura-Serrano (2006) dentro del segundo modelo, ya que dicho autor argumentó que la noción de patrimonio común de la humanidad es un concepto funcional más que territorial y que sería aplicable a Internet (cabe recordar que Internet es sólo un elemento del ciberespacio). Del mismo modo, D'Amato (2002) ha sostenido que Internet será considerada cada vez más como patrimonio común de la humanidad.

Sin embargo, la literatura especializada no es lineal en este punto tampoco. Woltag ha rechazado la dicotomía entre espacio global común y soberanía territorial. En esa línea, ha objetado que el ciberespacio sea calificado como un nuevo espacio bajo el derecho internacional, fuera de la autoridad y regulación del Estado, sino que ha propuesto calificarlo como una nueva especie de esfera social o pública (Woltag, 2011, p. 12).

De este análisis previo, parece claro que es necesaria una distinción entre, por un lado, soberanía y ejercicio de la jurisdicción estatal sobre un espacio y, por el otro, jurisdicción sobre las actividades en dicho espacio, o sobre las infraestructuras montadas en el mismo. Los informes de los GEG de 2013 y 2015 (ver sección IV) concluyen que la soberanía estatal y las normas internacionales que emanan de ella se aplican a la *conducta* estatal relativa a las TIC, y a su jurisdicción sobre la *infraestructura* en su territorio.

Por su parte, el Manual de Tallin comenta en su Regla 1 que un Estado no puede reclamar soberanía estatal sobre el ciberespacio como tal, pero sí tiene ciertas prerrogativas sobre las infraestructuras de las TIC y sobre las actividades relacionadas a ellas dentro de su territorio. Asimismo, aclara que el significado de soberanía en el contexto cibernético implica, entre otras cosas, restringir y proteger el acceso a Internet. Por otro lado, la Regla 2 expresa que los Estados tienen jurisdicción sobre las personas que desarrollan actividades cibernéticas dentro de su territorio, sobre las infraestructuras que se encuentran tendidas en su territorio y, extraterritorialmente, de acuerdo al derecho internacional.

Si analizamos otros regímenes jurídicos, podemos ver esta suerte de disociación entre soberanía y jurisdicción. Por ejemplo, en el régimen jurídico del espacio ultraterrestre, tenemos por un lado la combinación de los arts. I y II del Tratado del Espacio (OST, 1967), que conforman la base legal para la consideración del espacio ultraterrestre como un dominio global común, ya que dichas cláusulas establecen la libertad

de uso y exploración del espacio ultraterrestre con fines pacíficos para todos los Estados y la no apropiación. Por el otro lado, el art. VIII del mismo tratado es el principal sustento legal del ejercicio de la jurisdicción y control estatales sobre los objetos espaciales. Si observamos el régimen del derecho del mar, podemos apreciar una combinación similar en los arts. 87 y 89 (libertad de la alta mar e ilegitimidad de las reivindicaciones de soberanía sobre ella) y del art. 92 (relativo a la jurisdicción sobre los buques) de la Convención del Mar (Convemar, 1982).

En el ámbito que nos ocupa, no existe aún un instrumento internacional específico que sirva de base legal para considerar el ciberespacio como un espacio global común. En las negociaciones que se vienen llevando a cabo en las Naciones Unidas hasta el momento de escribir el presente (ver sección IV), la aproximación más cercana a dar una idea en tal sentido fue en el informe de 2015, cuando el GEG subrayó "las aspiraciones de la comunidad internacional en el uso pacífico de las TIC para el bien común de la humanidad" (GEG, 2015, párr. 28).

III.2. Características de las actividades en el ciberespacio

Algunas de estas características han sido identificadas en los informes de los GEG, por ejemplo, el uso dual, el anonimato, la accesibilidad y la ubicuidad.

III.2.1. Uso dual

El ciberespacio es un dominio en el que se llevan a cabo actividades cibernéticas tanto de carácter civil como militar. Éstas utilizan la misma tecnología e infraestructura, pero difieren en la finalidad de su uso y el nivel de confidencialidad. Retomando nuestro ejercicio comparativo, es importante señalar que esta característica también es compartida por las actividades en el espacio ultraterrestre, donde coexisten actividades civiles –como la observación de la Tierra y la investigación científica– y los usos

militares, como la inteligencia y la operación de anti-satélites. Otro claro ejemplo de uso dual se encuentra en el ámbito nuclear, en el que la tecnología se puede utilizar, por ejemplo, con fines médicos o para desarrollar misiles.

Esta característica trae aparejada una serie de dificultades para controlar la proliferación de capacidades cibernéticas destructivas (Morth, 1998). Cuando dicho control resulta impracticable, la cooperación entre el gobierno y el sector privado se convierte en una necesidad crítica (Delibasis, 2006). El rol fundamental de la cooperación entre Estado y sector privado también ha sido señalado en los informes de los GEG de 2013 y 2015 (ver sección IV de este artículo).

Otra derivación de esta característica es el peligro de que el ciberespacio –al igual que sucede con el espacio ultraterrestre– se convierta en un escenario de conflicto armado; de hecho, la OTAN considera ambos espacios "dominios operacionales", junto con el mar, la tierra y el aire (OTAN, 2016; 2019).

En resumidas cuentas, esta característica de las actividades cibernéticas agrega tensiones entre los Estados, por lo que es fundamental crear una estructura de cooperación y de confianza mutua para alejar recelos y percepciones erróneas que puedan desencadenar malentendidos o conflictos.

III.2.2. Anonimato

Este es un aspecto que hace a las actividades cibernéticas maliciosas particularmente atractivas para criminales y terroristas. Consiste en la facilidad de esconder la identidad, lo que implica no solamente la dificultad de encontrar la computadora desde donde la actividad maliciosa proviene, sino también de descubrir quién está detrás de ella o de los dispositivos utilizados como trampolín para desorientar. Esta característica –junto con la posibilidad de activar varios niveles en un ataque cibernético

y la velocidad en la que se materializan las consecuencias nocivas–contribuye a la dificultad de atribuir a un sujeto una actividad cibernética y, consecuentemente, de establecer su responsabilidad (Tsagourias, 2012).

La dificultad para determinar si una actividad cibernética determinada fue intencional o inadvertida contribuye al problema de atribución (Williams, 2011). El anonimato permite reducir los costos de ser descubierto (Fidler, 2012) o de dañar el propio nombre (Cox, 2005). Por ello, podemos concluir que el anonimato y el problema de atribución son dos caras de la misma moneda.

Algunos Estados mantienen alianzas de cooperación para superar la dificultad que genera el anonimato en el proceso de atribución. Así surgió la alianza denominada Five Eyes, un grupo de Estados afines que incluye a los Estados Unidos, Canadá, Australia, Nueva Zelanda y el Reino Unido. La estrategia de esta alianza consiste en atribuir públicamente ataques cibernéticos (Comunicados, 2018). Si bien este método podría ser útil en términos políticos y como medio disuasivo para futuras actividades maliciosas, es difícil determinar cuándo dichas acusaciones están debidamente fundamentadas ya que en general se basan en información provista por servicios de inteligencia cuyas fuentes no se revelan.

Sin perjuicio de todo lo anterior, es necesario destacar que, en materia de derechos humanos, el anonimato y el cifrado permiten el ejercicio del derecho a la libertad de expresión y de opinión. Es por ello que la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos ha reconocido la importancia del discurso anónimo, ya que favorece la participación en el debate público de personas que, al resguardar su identidad, pueden evitar ser víctimas de represalias injustas por ejercer dichos derechos fundamentales (CIDH, 2013). Por su parte, en el ámbito universal, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión destacó en su informe de 2015 lo siguiente:

> "el cifrado y el anonimato brindan a los individuos y a los grupos una zona de vida privada en línea para sostener opiniones y ejercer la libertad de expresión sin injerencia o ataques arbitrarios o ilegales" (HRC, 2015, p.16).

En consecuencia, las restricciones en el cifrado y anonimato deben estrictamente limitarse de acuerdo a los principios de legalidad, necesidad, proporcionalidad y legitimidad del fin perseguido (HRC, 2015; 2018).

III.2.3. Ubicuidad

El ciberespacio elimina la necesidad de proximidad entre víctima y victimario y, con ello, amplía la distancia entre el punto de origen y el de los efectos de la actividad maliciosa. Más aún, las actividades maliciosas pueden ser segmentadas y presentadas fácilmente como proviniendo de un lugar determinado, sin que los dueños u operadores de las computadoras se hayan percatado de ello. La ubicuidad hace difícil determinar cuándo una actividad cibernética maliciosa empieza, cuán rápido desplegará sus efectos y en dónde.

III.2.4. Bajo costo y amplia accesibilidad

La literatura coincide en que otra característica de las actividades cibernéticas es que sus costos son relativamente económicos (Cox, 2005; Condron, 2007; Johnson, 2002). Tampoco se requiere mucho conocimiento para emplear esta tecnología y, de cualquier modo, es accesible a través de tutoriales disponibles en Internet. La amplia accesibilidad es una consecuencia derivada de la expansión de la digitalización y del surgimiento de la sociedad de la información, lo que se presenta como un desafío para los Estados, que deben encontrar un balance entre regulación y accesibilidad.

III.2.5. Asimetría de beneficios

Esta característica está relacionada con el anonimato y con la accesibilidad de las actividades cibernéticas; la asimetría contribuye a que tanto actores estatales como no estatales sin recursos económicos o militares utilicen la vía cibernética como medio de contienda (Segura-Serrano, 2006). Hathaway (2012, p. 842) se refirió a las herramientas cibernéticas como el "arma poderosa de los débiles". Asimismo, otra ventaja de las actividades cibernéticas es que brindan una estrategia menos coherente, tangible y predecible que la confrontación militar (Bowman, 1995, p. 1943).

Debido a esta característica, los Estados altamente dependientes de las TIC se enfrentan a la contradicción de querer establecer límites para aquellos que pueden poner sus infraestructuras críticas en jaque y, a la vez, mantener las capacidades cibernéticas propias disponibles para disuadir, defenderse y eventualmente atacar, de ser necesario.

III.2.6. Daño impredecible

La última característica que nos gustaría abordar aquí es la imprevisibilidad del daño. Ya hemos indicado que el daño abarca un amplio abanico de efectos, pero determinar qué nivel de daño la actividad maliciosa ha alcanzado y si ese es el último grado al que puede llegar, es difícil, al menos de forma inmediata.

En efecto, no es fácil distinguir entre un código malicioso que busca sólo explotar información y otro destinado a generar destrucción. Ello se debe a que el software puede permitir distintas acciones y cambiar de una a otra de manera muy veloz, causando en algunos casos daño instantáneamente. La falta de previsibilidad genera un problema serio en términos de respuesta estatal, ya que ésta debe cumplir con ciertos requisitos, como el principio de proporcionalidad, entre otros.

IV. Las TIC en el contexto de la seguridad internacional en la agenda de las Naciones Unidas

El tratamiento de las TIC en el contexto de la seguridad internacional está en la agenda de las Naciones Unidas desde hace dos décadas. Para una más fácil exposición, podemos dividir la línea temporal en tres segmentos:

IV.1. Los orígenes

En 1998, la Federación de Rusia presentó por primera vez un proyecto de resolución sobre seguridad de la información en la Primera Comisión de la Asamblea General, dando lugar a la adopción sin votación de la Resolución 53/70 de dicho órgano, intitulada "Los avances en la esfera de la informatización y las telecomunicaciones en el contexto de la seguridad internacional" (Asamblea General, 1999). Ya en uno de sus párrafos preambulares se introducía la preocupación de que las tecnologías pudieran utilizarse para fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales.

En los párrafos operativos, la resolución pide que se aborde la cuestión en un foro multilateral, lo que es un requerimiento fundamental para preservar el carácter inclusivo y la transparencia del debate. Adicionalmente, invita a los Estados a considerar la conveniencia de desarrollar principios internacionales que mejoren la seguridad de las TICs y, por último, decide incluir un punto en la agenda sobre el tema para el año subsiguiente.

En particular, esa resolución no hace referencia alguna a "armas informáticas" o a "guerras informáticas," expresiones incluidas en la carta que el Representante Permanente de la Federación de Rusia envió al Secretario General en septiembre de 1998 y en el proyecto de resolución adjunto (Naciones Unidas, 1998). Cabe recordar que dicho Estado también presentó propuestas de definición de "guerra en la esfera de la

información"[1] y de "arma informática"[2] (Naciones Unidas, 1999) en respuesta a la solicitud de opiniones efectuada por la Asamblea General en la ya mencionada Resolución 53/70.

Desde sus inicios, la Federación de Rusia ha tenido un enfoque preventivo[3] (Naciones Unidas, 1998). En esta línea, ha impulsado la creación de *lex specialis* para la seguridad de la información con iniciativas como el ya referido proyecto de resolución de 1998 (Naciones Unidas, 1998), los dos borradores de código internacional de conducta para la seguridad de la información (Naciones Unidas, 2011; 2015a) y la propuesta de una Convención Internacional sobre Seguridad de la Información (Proyecto, 2011).

IV.2. El trabajo de los GEG: los informes de 2010, 2013 y 2015

Podemos distinguir un segundo periodo a partir de fines de 2001, cuando la Asamblea General pidió al Secretario General que examinara junto con un GEG las amenazas existentes y potenciales en el ámbito de la seguridad de la información. Asimismo, le solicitó que realizara un estudio para definir ciertos conceptos relativos a la temática (Asamblea General, 2001). Reiteró el pedido en los años 2002 y 2003 (Asamblea General, 2002; 2003), hasta que en 2004 el Secretario General estableció un GEG en base al principio de distribución geográfica equitativa, el cual celebró su primera

[1]La definición propuesta de "guerra en la esfera de la información" reza: "enfrentamiento entre Estados en la esfera de la información con el objetivo de dañar los sistemas, procesos, recursos y estructuras vitales de la información y socavar los sistemas político y social de otro Estado, así como la manipulación sicológica de la población de un Estado y la desestabilización de la sociedad".

[2] La definición propuesta de "arma informática" reza: "medios y métodos empleados con el objetivo de dañar los recursos, procesos y sistemas de la información de otro Estado; la utilización de la información en detrimento de los sistemas vitales de defensa, administrativos, políticos, sociales, económicos o de otra índole de un Estado y la manipulación de la población de un Estado con el objetivo de desestabilizar la sociedad y el Estado."

[3] Extracto del documento presentado por dicho Estado: "En nuestra opinión ese peligro exige ya la adopción de medidas preventivas. No puede permitirse que surja en el escenario internacional un nuevo enfrentamiento de características esencialmente diferentes capaz de provocar otra espiral de la carrera de armamentos sobre la base de los avances de la revolución científico-tecnológica".

sesión del 12 al 16 de julio de 2004 y se reunió por segunda vez en 2005 sin llegar a un consenso.

El segundo GEG fue creado en 2009[4] y retomó los trabajos sobre los puntos referidos a petición de la Asamblea General en 2005, 2006, 2007 y 2008 (Asamblea General, 2005; 2006; 2007; 2008). El documento final de este grupo fue un informe publicado en julio de 2010 (GEG, 2010), que concluía con cinco recomendaciones en el ámbito de la "seguridad de la información": mayor diálogo para discutir normas para el uso de las TIC; medidas de fomento de la confianza; intercambio de información; formación de capacidades y elaboración de términos comunes y definiciones.

El tercer GEG[5] fue creado en 2012 a petición de la Asamblea General en 2010 y 2011 (Asamblea General, 2010; 2011). Redactó un informe consensuado en 2013, el que concluyó que el derecho internacional existente se aplica al entorno de las TIC y que deberá estudiarse con mayor detenimiento cómo es su aplicación. Otra de las conclusiones fue que las normas derivadas del derecho internacional existente deben aplicarse al comportamiento de los Estados, y que el uso de las TIC puede requerir desarrollar normas adicionales en el futuro (GEG, 2013). Se puede deducir que los miembros del GEG lograron un equilibrio entre las posiciones que reclamaban un nuevo conjunto de normas y las que consideraban que el derecho internacional existente era suficiente.

Una de las particularidades de este informe en comparación con el anterior tiene que ver con el lenguaje utilizado: en primer lugar ya no se habla de "seguridad de la información" sino de "seguridad de y en el uso de las TIC"[6]. En segundo lugar, este GEG adoptó un lenguaje mixto (asertivo, prescriptivo y recomendatorio) en el capítulo III dedicado a las normas, reglas y principios de comportamiento estatal responsable; y

[4]Compuesto por los siguientes Estados: Belarús, Brasil, China, Estonia, Francia, Alemania, India, Israel, Italia, Catar, República de Corea, la Federación de Rusia, Sudáfrica, el Reino Unido y los Estados Unidos.
[5] Compuesto por representantes de los siguientes Estados: Argentina, Australia, Belarús, Canadá, China, Egipto, Estonia, Francia, Alemania, India, Indonesia, Japón, la Federación de Rusia, el Reino Unido y los Estados Unidos.
[6] Ver documento en inglés que utiliza la expresión "security of and in the use of ICTs".

netamente recomendatorio en los capítulos IV (dedicado a medidas de fomento de la confianza) y V (dedicado a creación de capacidades). En el párrafo 18 del capítulo III, el GEG se limitó a "tomar nota" de la propuesta de un proyecto de código de conducta para la seguridad de la información, presentada por la Federación de Rusia, China, Tayikistán y Uzbekistán (Naciones Unidas, 2011).

En ese informe, el GEG reconoció el deber de los Estados de abordar los desafíos de las TIC en consonancia con las obligaciones en materia de derechos humanos, confirmó la aplicación del derecho internacional (incluida la Carta de las Naciones Unidas) y los principios derivados de él, y recordó el deber de no permitir la utilización del propio territorio por parte de actores no estatales para acciones maliciosas. También reconoció el ejercicio de la jurisdicción estatal sobre las infraestructuras de las TIC ubicadas en el territorio nacional y la necesidad de involucrar al sector privado y a la sociedad civil en los mecanismos de cooperación estatal.

En 2013 se estableció otro GEG[7] a partir de una nueva petición de la Asamblea General (Asamblea General, 2013). El informe de consenso de 2015 (GEG, 2015) no adoptó un lenguaje uniforme, sino que entonces variaba entre "seguridad de las TIC", "seguridad en el uso de las TIC", "seguridad de y en el uso de las TIC", y "uso abierto, seguro, estable accesible y pacífico de las TIC". Una de las novedades de este informe es que el GEG estimó que el uso de las TIC en futuros conflictos será muy probable.

En el capítulo III, el GEG no aclaró qué entiende por "normas, reglas y principios de comportamiento estatal responsable", pero esta vez incorporó al mismo capítulo el tratamiento de "normas voluntarias y no vinculantes de comportamiento estatal responsable", respecto a las cuales explicó lo siguiente:

> "[…] no tratan de limitar ni prohibir acciones que, por lo demás, son compatibles con el derecho internacional. Las normas reflejan las expectativas de la

[7] Compuesto por representantes de los siguientes Estados: Belarús, Brasil, China, Colombia, Egipto, Estonia, Francia, Alemania, Ghana, Israel, Japón, Kenia, Malasia, México, Pakistán, República de Corea, Federación de Rusia, España, Reino Unido y Estados Unidos.

comunidad internacional, establecen criterios para un comportamiento responsable de los Estados y permiten que la comunidad internacional evalúe las actividades e intenciones de estos" (GEG, 2015, párr. 10).

Esta descripción fue el preludio de una serie de once recomendaciones de comportamiento estatal responsable (a diferencia del informe anterior, sólo empleó la fórmula recomendatoria "debería"), entre las que se incluyen: la cooperación internacional, no permitir que se utilice a sabiendas el territorio de un Estado para cometer actos ilícitos a nivel internacional que incluya el uso de TIC, el respeto de las resoluciones de la Asamblea General relativas al goce de los derechos humanos e Internet, derecho a la privacidad y libertad de expresión, la no utilización de las TIC para afectar intencionalmente infraestructuras críticas nacionales de otros Estados, proteger las propias, asistir a los Estados cuyas estructuras críticas se vean afectadas por actividades maliciosas y la protección de los equipos de respuesta a emergencias.

Además de los capítulos sobre medidas de fomento de la confianza (capítulo IV) y de cooperación para la seguridad y la creación de capacidades (V), este informe incluyó un capítulo sobre cómo se aplica el derecho internacional al uso de las TIC (capítulo VI). En este último, el GEG incluyó una lista no exhaustiva de opiniones expresadas con distinto lenguaje que oscila entre asertivo, prescriptivo y descriptivo, a saber:

- **Lenguaje asertivo:**

  Los Estados tienen jurisdicción sobre la infraestructura de las TIC en su territorio;

- **Lenguaje prescriptivo:**

  Los Estados deben observar los principios de soberanía nacional, respeto por los derechos humanos, resolución pacífica de controversias, no-intervención;

  Los Estados deben cumplir sus obligaciones relativas a los hechos internacionalmente ilícitos y no deben valerse de intermediarios para cometer hechos internacionalmente ilícitos;

• **Lenguaje descriptivo:**

El GEG tomó nota del derecho inherente a tomar medidas (legítima defensa), pero reconoció que ello requiere un mayor estudio;

El GEG tomó nota de los principios del derecho humanitario (proporcionalidad, distinción, necesidad y humanidad);

El GEG tomó nota de que las acusaciones relativas a los hechos internacionalmente ilícitos deberían estar fundamentadas.

El GEG señaló que era importante que un nuevo GEG estudiase cómo se aplica el derecho internacional al uso de las TIC y que siga trabajando en normas, reglas y principios de comportamiento estatal responsable, medidas de fomento de la confianza y la creación de capacidades. Al igual que en su informe anterior, el GEG tomó nota de un proyecto de código internacional de conducta sobre seguridad de la información (esta vez, refiriéndose a la versión revisada). Y al igual que el informe de 2010, retomó la recomendación de estudiar conceptos relacionados a la seguridad de las TIC.

El último hito en el desarrollo de esta etapa fue cuando la Asamblea General pidió al Secretario General que con asistencia de un GEG a establecerse en 2016 continuara examinando cómo se aplica el derecho internacional al uso de las TIC (Asamblea General, 2015). Lamentablemente, dicho GEG no pudo llegar a un consenso sobre un informe en 2017, lo que demuestra lo frágil y cuidadosamente elaborado que estaba cualquier acuerdo anterior (Tikk y Kerttunen, 2017, p. 15).

El saldo positivo que esta etapa dejó es la adopción en 2018 de una resolución de la Asamblea General por medio de la cual acogió con beneplácito trece normas de comportamiento estatal responsable, emanadas de las recomendaciones de los informes de 2013 y 2015 (Asamblea General, 2018a).

Desde los orígenes hasta el fin de esta etapa, algunos Estados consideraron que el marco jurídico existente, en particular el art. 51 de la Carta de las Naciones Unidas y el derecho internacional humanitario, se aplica al ciberespacio y que, por tanto, no

sería necesario un instrumento multilateral (Naciones Unidas, 2004a) (Naciones Unidas, 2004b), mientras que otros consideran necesario adoptar un instrumento internacional jurídicamente vinculante (Naciones Unidas, 2019). Esta divergencia de opiniones sigue siendo un escollo que la comunidad internacional deberá superar.

IV.3. El fin de una era y el inicio de otra

Tras la imposibilidad de acordar un informe en 2017, podemos decir que se ha iniciado un tercer periodo en las negociaciones. La Asamblea General adoptó dos resoluciones con mecanismos separados para seguir examinando la cuestión de las TIC en el contexto de la seguridad internacional:

- Un grupo de trabajo de composición abierta, a partir de una propuesta presentada por la Federación de Rusia y varios Estados del G77 y China (Naciones Unidas, 2018a). De acuerdo al esquema previsto, es de esperar que este año (2021) el grupo presente un informe reafirmando las recomendaciones de comportamiento estatal responsable de los anteriores informes y la aplicación del derecho internacional al uso de las TIC, y que impulse la continuación del estudio en la temática.
- Otro GEG[8] para asistir al Secretario General como en las anteriores oportunidades, propuesto por los Estados Unidos, Australia, Canadá, Japón, Israel y varios países europeos (Naciones Unidas, 2018b). Este GGE tuvo su primera reunión en diciembre de 2019 y su mandato se extiende hasta mayo del 2021, esperándose que este año emita un informe consensuado.

En definitiva, acaba de iniciarse una tercera etapa en los debates en torno a las TIC y la seguridad internacional y, así, se abren nuevas expectativas respecto a la negociación de normas de comportamiento estatal responsable y de medidas de fomento

[8] Compuesto por representantes de los siguientes Estados: Australia, Brasil, China, Estonia, Francia, Alemania, India, Indonesia, Japón, Jordania, Kazajstán, Kenia, Mauricio, México, Marruecos, Países Bajos, Noruega, Rumania, Federación de Rusia, Singapur, Sudáfrica, Suiza, Reino Unido, Estados Unidos y Uruguay.

de la confianza, así como de otros modelos regulatorios. Si bien los dos mecanismos creados reflejan posiciones polarizadas en algunos puntos, ambos pueden complementarse y enriquecer el trabajo de la Primera Comisión de la Asamblea General sobre una de las cuestiones más acuciantes y actuales en el ámbito de la paz y la seguridad internacionales.

Mientras que el grupo de composición abierta responde al deseo de participación universal de los miembros de la comunidad internacional, también proporcionaría un ámbito de discusión y negociación más político que técnico. Por ello, sus labores podrían implicar un "enfoque descendiente", es decir, primero lograr acordar los aspectos políticos para luego pasar a un acuerdo sobre las cuestiones de orden técnico. Por su parte, el grupo de expertos tiene como característica ser un grupo reducido de especialistas, por lo que se podría esperar que trabaje con un "enfoque ascendente", es decir, buscando acordar los aspectos técnicos para que el resultado sea luego endosado a nivel político. En dicho marco, es de esperar que el trabajo paralelo en ambos enfoques optimice el tiempo y esfuerzo dedicado a la materia.

V. Conclusiones

En primer lugar, este artículo ha tratado de demostrar que cualquier trabajo futuro sobre las TIC en el contexto de la seguridad internacional tiene que partir de un entendimiento común sobre el lenguaje a emplear, para lo cual, una recomendación es evitar estancarse en discusiones sobre terminología bélica que tiene la tendencia a polarizar posiciones y dificultar las negociaciones. En efecto, parte del mandato de los GEG ha sido definir conceptos relacionados con la temática. Sin embargo, aún queda mucho trabajo por hacer para homogeneizar el léxico en base a un acuerdo sobre su significado y, así, evitar lenguajes vagos y mutantes que no contribuyen a la correcta implementación de las normas de comportamiento estatal responsable y de las medidas de fomento de la confianza. Cualquiera sea la expresión que se decida utilizar, no

podrá desconocerse que cualquier esfuerzo regulatorio que se haga en la materia deberá prever suficiente salvaguarda a los derechos humanos y garantías fundamentales en una sociedad democrática.

La caracterización del ciberespacio y de las actividades cibernéticas demostró que hay aspectos comunes con otros dominios que son abordados por otras ramas del derecho, lo que permite establecer paralelismos y buscar orientación en otros regímenes en base a dichas similitudes. Por otro lado, quedó a la luz que las particularidades propias del mundo cibernético presentan desafíos respecto a los cuales habrá que buscar soluciones con algún grado de originalidad. Algunos de los desafíos reseñados se vinculan al control de la proliferación de tecnologías duales, el problema de atribución, la dificultad de respuesta ante la imprevisibilidad del daño, el dilema entre regulación de y accesibilidad a las TIC y la contradicción entre querer recortar capacidades cibernéticas ajenas a la vez que se quieren mantener las propias disponibles para disuasión, defensa y ataque.

Finalmente, la reseña del trabajo de las Naciones Unidas en la materia permite reafirmar la importancia del multilateralismo y del rol que éste tiene en la consecución de los objetivos de mantener la paz y seguridad internacionales. La actual combinación entre un acotado grupo de expertos con representación geográfica equitativa y un esquema abierto con representación universal parece transmitir que uno de los requerimientos de la regulación de los nuevos desafíos que presentan las TIC es que *expertise* técnico, legal y político van de la mano.

Bibliografía

Aldrich, Richard (1996) The international legal implications of information warfare. *Airpower Journal,* 10(3), 99-110.

Beard, Jack (2017) Soft law's failure on the horizon: the international code of conduct for outer space activities. *U. Pa.J. Int'L.,* 38(2), 335-424.

Blake, Dunkan e Imburgia, Joseph (2010)"Bloodless weapons"? The need to conduct legal review of certain capabilities and the implicationsof defining them as "weapons". *Air Force Law Review* (66), 159-200.

Boothby, William (2012) Some legal challenges posed by remote attack. *International Review of the Red Cross* (94), 579-595.

Bowman, M.E. "Spike" Eugene (1995) Is international law ready for the information age? *Fordham International Law Journal* (19), 1935-1946.

Brenner, Susan (2007) At light speed: attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law and Criminology*(97), 379-475.

Buchan, Russel (2012) Cyber attacks:unlawful uses of force or prohibited interventions? *Journal of Conflict and Security Law* (17), 212-227.

Condron, Sean (2007) Getting it right: protecting American critical infrastructure in cyberspace. *Harvard Journal of Law and Technology* (20), 402-422.

Cox, Stephen (2005) 'Confronting Threats Through Unconventional Means: Offensive Information Warfare as Covert Alternative to Preemptive War'. *Houston Law Review* (42), 881-910.

D'Amato, Anthony (2002) International law, cybernetics, and cyberspace. *International Law Studies*(76), 59-73.

Delibasis, Dimitrios (2006) State use of force in cyberspace for self-defence: a new challenge for a new century. *Peace Conflict and Development: an Interdisciplinary Journal*(8), 1-50.

Dinstein, Yoram (2002) Computer network attacks and self-defense. *International Law Studies* (76), 99-121.

Dinstein, Yoram (2003).*War, aggression and self-defense.* Cambridge: Cambridge University Press.

Fidler, David (2012) Tinker, Tailor, Soldier, Duqu: why cyberespionage is more dangerous than you think. *International Journal of Critical Infrastructure Protection* (5), 28-29.

Hathaway, Oona (2012) The law of cyberattack. *California Law Review* (100), 817-886.

Hollis, Duncan (2007) Why States need an international law for information operations. *Lewis and Clark Law Review* (11), 1023-1062.

Johnson, Phillip (2002) Is it time for a treaty on information warfare? *International Law Studies* (76), 439-531.

Joyner, Christopher y Lotrionte, Catherine (2001) Information warfare as international coercion: elements of a legal framework. *European Journal of International Law* (12), 825-865.

Kuehl, Daniel (2002) Information operations, information wafare, and computer network attack: their relationship to national security in the information age. *International Law Studies* (76), 35-58.

Lin, Herbert (2010) Offensive cyber operations and the use of force. *Journal of National Security Law and Policy* (4), 63-86.

Morth, Todd (1998) Considering our position: viewing information warfare as a use of force prohibited by article 2(4) of the UN Charter. *Case Western Reserve Journal of International Law* (30), 567-600.

Raboin, Bradly (2011) Corresponding evolution: international law and the emergence of cyber warfare. *Journal of the National Association of Administrative Law Judiciary* (31), 603-668.

Roscini, Marco (2014). *Cyber operations and the use of force international law.* Oxford: Oxford University Press.

Schmitt, Michael (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare .* Cambridge: Cambridge University Press.

Schmitt, Michael (2002) Wired warefare: Computer network attack and the jus in bello. *International Review of the Red Cross* (84), 365-398.

Schmitt, Michael y Vihul, Liis (2014). *The nature of international cyber norms.*Tallin: CCDCOE.

Segura-Serrano, Antonio (2006) Internet regulation and the role of international law. *Max Planck Yearbook of United Nations Law* (10), 191-272.

Shackelford, Scott (2009). From nuclear war to net war: analogizing cyber attacks in international law. *Berkeley Journal of International Law* (27), 192-251.

Sharp, Walter (1999). *Cyberspace and the use of force.* Falls Church: Aegis Research Corporation.

Tabachnik, Alexander y Topor, Lev. (2020). Russian cyber sovereignty: one step ahead. Russian International Affairs Council. Disponible en: https://bit.ly/2SeEaho

Tikk, Eneken y Kerttunen, Mika(2017)The alleged demise of the UN GGE: An autopsy and eulogy, Cyber Policy Institute, 1-46.

Tsagourias, Nicholas (2012) Cyber attacks, self-defence and the Problem of Attribution. *Journal of Conflict and Security Law* (17), 229-244.

Von Clausewitz, Carl (2007). *On war.* Oxford: Oxford University Press.

Williams, Robert (2011) Game change: cyber networks, intelligence collection, and covert action. *The George Washington Law Review* (79), 1162-1200.

Woltag, Johann-Cristoph (2011). Computer network operations below the level of armed force. *ESIL Conference Paper Series,* 1(1), 1-16.

Documentos Naciones Unidas

Asamblea General de las Naciones Unidas, Resolución 53/70, 4 de diciembre de 1998, A/RES/53/70.

Asamblea General de las Naciones Unidas, Resolución 54/49, 1 de diciembre de 1999, A/RES/54/49.

Asamblea General de las Naciones Unidas, Resolución 56/19, 29 de noviembre de 2001, A/RES/56/19.

Asamblea General de las Naciones Unidas, Resolución 57/53, 22 de noviembre de 2002, A/RES/57/53.

Asamblea General de las Naciones Unidas, Resolución 58/32, 8 de diciembre de 2003, A/RES/58/32.

Asamblea General de las Naciones Unidas, Resolución 6/45, 8 de diciembre de 2005, A/RES/60/45.

Asamblea General de las Naciones Unidas, Resolución 61/54, 6 de diciembre de 2006, A/RES/61/54.

Asamblea General de las Naciones Unidas, Resolución 62/17, 5 de diciembre de 2007, A/RES/62/17.

Asamblea General de las Naciones Unidas, Resolución 63/37, 2 de diciembre de 2008, A/RES/63/37.

Asamblea General de las Naciones Unidas, Resolución 65/41, 8 de diciembre de 2010, A/RES/65/41.

Asamblea General de las Naciones Unidas, Resolución 66/24, 2 de diciembre de 2011, A/RES/66/24.

Asamblea General de las Naciones Unidas, Resolución 68/243, 27 de diciembre de 2013, A/RES/68/243.

Asamblea General de Naciones Unidas, Resolución 70/237, 23 de diciembre de 2015, A/RES/70/237.

Asamblea General de las Naciones Unidas, Resolución 73/27, 5 de diciembre de 2018, A/RES/73/27.

Asamblea General de las Naciones Unidas, Resolución 73/266, 22 de diciembre de 2018, A/RES/73/266.

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/68/156, 16 de julio de 2013.

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/69/112/Add.1, 18 de septiembre de 2014.

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/70/172, 22 de julio de 2015.

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/71/172, 19 de Julio de 2016.

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/72/315, 11 de agosto de 2017.

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/C.1/73/L.27/Rev.1, 29 de octubre de 2018.

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/C.1/73/L.37, 18 de octubre de 2018.

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/74/120, 24 de junio de 2019.

Carta de fecha 23 de septiembre de 1998 dirigida al Secretario General por el Representante Permanente de la Federación de Rusia ante las Naciones Unidas, UN Doc. A/C.1/53/3, 30 de septiembre 1998.

Carta de fecha 12 de septiembre de 2011 dirigida al Secretario General por los Representantes Permanentes de China, la Federación de Rusia, Tayikistán y Uzbekistán ante las Naciones Unidas, UN Doc. A/66/359, 14 de septiembre de 2011.

Carta de fecha 9 de enero de 2015 dirigida al Secretario General por los Representantes Permanentes de China, la Federación de Rusia, Kazajstán, Kirguistán,

Tayikistán y Uzbekistán ante las Naciones Unidas, UN Doc. A/69/723, 13 de enero de 2015.

Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/65/201, 30 de julio de 2010.

Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, UN Doc. A/68/98, 24 de junio de 2013.

Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, A/70/174, 22 de julio de 2015.

Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/54/213, 10 de agosto 1999.

Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/59/116, 23 de junio de 2004.

Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, UN Doc. A/59/116/Add.1, 28 de diciembre de 2004.

Otras fuentes[9]

Argentina, Estrategia de Ciberseguridad, Secretaría de Gobierno de Modernización, Resolución 829/2019, publicada el 28 de mayo de 2019. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/323594/norma.htm

Asamblea General de la OEA, Resolución AG/RES. 2004 (XXXIV-O/04), 8 de junio de 2004.

China, International Strategy of Cooperation on Cyberspace (2017), versión en inglés disponible en: https://bit.ly/3zJZPPh

[9] Todos los enlaces fueron verificados el 5 de marzo de 2021.

China, Programa Nacional de medio y largo plazo para el Desarrollo de la Ciencia y la Tecnología (2006-2020), versión en inglés disponible en el repositorio de la UIT: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx/

CIDH, Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. OEA/Ser.L/V/II.149. Doc. 50. (Catalina Botero Marino), 31 de diciembre de 2013.

Comité Internacional de la Cruz Roja, Comentario de 1987 al Protocolo II a los Convenios de Ginebra del 12 de agosto de 1949, relativo a la protección de víctimas de conflicto armados no internacionales. Disponible en: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=AA0C5BCBAB5C4A85C12563CD002D6D09&action=openDocument/

Convención de las Naciones Unidas sobre el Derecho del Mar, adoptada el 10 de diciembre de 1982 y en vigor desde el 16 de noviembre de 1994, 1833 UNTS 3.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Encryption and Anonymity follow-up report, Research Paper 1/2018, Human Rights Council Special Procedures. Disponible en: https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

Estados Unidos, Joint publication 3-13, 27 de noviembre de 2012. Disponible en: https://web.archive.org/web/20150208100916/http:/www.fas.org/irp/dod-dir/dod/jp3_13.pdf

Estados Unidos, Strategy for Homeland Defense and Civil Support of the United States (2005). Disponible en: https://www.hsd.org/

Federación de Rusia, Information Security Doctrine of the Russian Federation (2008). Versión en inglés disponible en el repositorio de UIT: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx/

Gobierno de Canadá, Canada identifies malicious cyber-activity by Russia, 4 de octubre de 2018. Disponible en: https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html

Gobierno de los Estados Unidos, Departamento de Justicia, Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information, 20 de diciembre de 2018. Disponible en: https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

Gobierno de los Estados Unidos, Departamento de Justicia, U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations, 4 de octubre de 2018. Disponible en: https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

Gobierno de Nueva Zelanda, Oficina de Seguridad de las Comunicaciones, Malicious cyber activity attributed to Russia, 4 de octubre de 2018. Disponible en: https://www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/

Gobierno del Reino Unido, UK and allies reveal global scale of Chinese cyber campaign, 20 de diciembre de 2018. Disponible en: https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign

Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, A/HRC/29/32, 22 de mayo de 2015.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996.

OTAN, Assured access to the common globals, findings and recommendations, abril 2011. Disponible en: https://www.act.nato.int/images/stories/events/2010/gc/aagc_recommendations.pdf

OTAN, NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit (2016). Disponible en: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

OTAN, NATO'S approach to space, 23 de octubre de 2020. Disponible en: https://www.nato.int/cps/en/natohq/topics_175419.htm/

Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la Protección de las Víctimas de los Conflictos Armados Internacionales (Protocolo I), aprobado el 8 de junio de 1977 y en vigor desde el 7 de diciembre de 1978.

Proyecto de Convención sobre Seguridad de la información Internacional, 22 septiembre de 2011. Disponible en el sitio del Ministerio de Relaciones Exteriores de la Federación de Rusia: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666/

Tratado sobre los principios que deben regir las actividades de los Estados en la exploración y utilización del espacio ultraterrestre, incluso la Luna y otros cuerpos celestes, adoptado el 19 de diciembre de 1966 y en vigor desde el 10 de octubre de 1967, 610 UNTS 205.

Unión Internacional de Telecomunicaciones, Guide to Developing a National Cybersecurity Strategy. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx/