Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

TRABAJO FINAL DE MAESTRÍA

El Ciberataque como Afectación al Principio de la No Intervención y Causa Legal Suficiente para la Legítima Defensa Nacional

ALUMNO/A: ABOG. URIEL NATÁN BEKERMAN

DIRECTORES: MG. ABOG. NICOLÁS TATO Y ESP. ING. CARLOS AMAYA

SEPTIEMBRE, 2022

Esta página ha sido dejada en blanco intencionalmente.

i. Resumen

El presente trabajo final de maestría propone demostrar cómo diversas clases de ciberataques perpetrados por Estados pueden representar una violación al principio de no intervención establecido por la Carta de las Naciones Unidas, lo cual puede justificar, en ciertos casos, una legítima defensa armada por parte del Estado intervenido, siempre y cuando se logre cumplir con una serie de requisitos establecidos por el derecho internacional público.

ii. Abstract

This master's thesis proposes to demonstrate how various types of cyber-attacks perpetrated by States may represent a violation of the principle of non-intervention established by the United Nations Charter, which may justify, in certain cases, a legitimate armed defense by the attacked State, as long as a series of requirements established by public international law are met.

iv. Índice General

Esta página ha sido dejada en blanco intencionalmente.

Capítulo 1: Introducción

Descripción del tema

A lo largo de la historia se han visto un alto número enfrentamientos y combates entre Naciones a través de cuatro escenarios recurrentes: la tierra, el mar, el aire y el espacio. La integración de la tecnología en la cotidianeidad de las poblaciones, sumado a las inmensurables ventajas y beneficios que ha otorgado la innovación tecnológica al ámbito militar, estratégico y político, ha permitido la utilización del ciberespacio como un quinto escenario de combate que se suma a los cuatro antes mencionados.

El presente trabajo final de maestría propone demostrar cómo las diversas clases de operaciones cibernéticas pueden constituir una violación al principio de la no intervención en los asuntos internos de otros Estados, establecido por el artículo 2.7 de la Carta de las Naciones Unidas, que a su vez suele estar vinculado con la violación del principio de soberanía internacional. Esta contraposición al derecho internacional público, puede tener como consecuencia la aplicación de la legítima defensa, también incluida dentro del mismo instrumento internacional de Naciones Unidas.

El quinto dominio de combate implica nuevos desafíos a la hora de atribuir la responsabilidad de un hecho ilícito internacional, debido a grandes dificultades técnicas, políticas y estratégicas para la localización del responsable material del hecho, y además, para dilucidar si aquella persona ha sido la mente intelectual del hecho. La dificultad de la ciber atribución es ampliamente explotada por quienes perpetran los ataques a través de ataques híbridos, quienes se sirven de guerrillas, rebeliones internas y terroristas para el acaecimiento de sus objetivos.

Si bien estas operaciones cibernéticas hacia un Estado suelen implicar las violaciones al derecho internacional público antes mencionadas, no todas las operaciones dan acceso a una defensa legítima armada, lo cual únicamente debe tener lugar en caso de que el ataque cuente con determinadas características que se deriven del propio hecho ilícito internacional, las cuales deberán justificar que la respuesta armada sea la única vía eficiente para repeler el ataque. A la fecha actual existen múltiples formas de operar en el ciberespacio con fines militares y estratégicos sobre otro Estado, sea a través de ciberataques tradicionales cuyo blanco son las infraestructuras críticas de un Estado, como a través de herramientas como la ciber influencia, el ciber lavado de activos, el ciberterrorismo, entre otras, cuyo objetivo es la desestabilización de un gobierno mediante la afectación de su estructura interna.

Justificación

La situación geopolítica actual, considerando especialmente los conflictos bélicos que están sucediendo en Europa del este a la fecha de elaboración del presente trabajo, dan noción de la relevancia que conlleva un detallado análisis acerca de las consecuencias jurídicas que puede tener un ciberataque a la luz del derecho internacional de las Naciones Unidas. En esta línea, los conceptos de no intervención, legítima defensa y atribución de la responsabilidad, cobran una esencia trascendental para la evolución de un conflicto entre naciones.

Un entendimiento equivocado de alguna de estas definiciones puede derivar en una guerra entre naciones, incluyendo la posibilidad de que esta exceda del mismo escenario del ataque como campo de batalla, produciéndose un conflicto en múltiples dominios que ponga en peligro la vida de civiles.

Objetivos del presente trabajo

El presente trabajo propone identificar cómo determinadas actividades desarrolladas en el ciberespacio pueden ser consideradas operaciones militares y estratégicas con gravedad equiparable al ataque armado, y de qué manera estas pueden tener graves impactos en la estructura interna de un Estado, a tal punto de ser consideradas intervenciones a la luz del derecho de las Naciones Unidas. Además, se propone categorizar un determinado grupo de ciberataques destinados a la afectación psicológica y social en la población de un Estado a través de la ciber influencia y el ciber terrorismo, los cuales pueden derivar en consecuencias tan graves como lo es un ciberataque a una infraestructura crítica.

Al analizar el estado actual de las definiciones que hacen a la ciberguerra y a las relaciones diplomáticas en el marco de operaciones de esta índole, se pretende definir cuáles son los entendimientos del orden jurídico internacional sobre las nociones de “ciberataque”, “operaciones cibernéticas”, “ataque armado”, “agresión”, “intervención en los asuntos internos de otro Estado”, “soberanía nacional”, “responsabilidad del hecho ilícito internacional”, “atribución de la responsabilidad” y “legítima defensa”. Por otro lado, se buscará determinar cuáles son las características que deberá tener el hecho ilícito internacional para concluir en que la legítima defensa armada es la vía más eficiente para repeler dicho acto.

La investigación y el desarrollo de la Tesis buscará concluir finalmente con el entendimiento de cuáles son los ciberataques que pueden ser considerados ataques armados a la luz del derecho internacional público, y en qué circunstancias se habilita la vía de la legítima defensa armada por parte del Estado atacado.

Hipótesis

Hipótesis principales

Un ciberataque puede constituir una violación al principio de la no intervención garantizado por la Carta de las Naciones Unidas.

Un ciberataque puede dar lugar a la legítima defensa armada por parte del Estado atacado.

Hipótesis secundarias

Un ciberataque puede representar una vulnerabilidad a la soberanía nacional del Estado atacado.

Un ciberataque desarrollado en el marco de una operación militar puede estar comprendido dentro de la figura del ataque armado.

Un ciberataque puede representar un crimen de agresión.

Los Estados suelen utilizar vías indirectas de ataque a través de metodologías de guerra híbrida, esto es, a través de agentes no estatales, los cuales dispersan la responsabilidad de los ciberataques y ocultan al verdadero responsable intelectual del hecho internacionalmente ilícito.

Metodología de investigación

Con el objeto de llevar adelante una investigación destinada a concluir con los objetivos mencionados anteriormente, la presente Tesis llevará adelante una metodología de análisis cualitativo de información, lo cual refiere al estudio de un tema en virtud de descripciones, investigaciones e interpretaciones de diversas personas y organizaciones (Aspers y Corte, 2019), así como aquellas que se desprenden de normativas, sentencias judiciales, guías, manuales, opiniones y declaraciones de entidades con reconocida experiencia en el ámbito específico que hace al presente trabajo.

Al invocar información que ha sido expresada en diversos materiales doctrinarios y jurisprudenciales del ámbito del derecho internacional público aplicado a la ciberguerra, el método cualitativo utilizado permitirá aprovechar el contenido de cada fuente basándose en la comparación, contraste, diversificación y la profundización del qué se dijo y el cómo se expresó dicha idea, que remiten a aspectos conversacionales que ayudan a la interpretación de las ideas (Jackson et al., 2007).

Debido a que el mundo suele carecer de ideas universales o convencionales, las interpretaciones y significados suelen estar configurados de acuerdo con la experiencia propia de cada persona, lo cual suele llevar a cada una de ellas construir su propia realidad. En esta linea, el método cualitativo permite observar el conjunto de realidades interpretadas por otros, enriqueciendo de esta manera el debate e incrementando el alcance del punto de vista personal a través de la colección y análisis de la información (Merriam, 2002).

Con el objeto de dar credibilidad científica a las conclusiones que derivarán del presente trabajo, se tomarán consideraciones de la Carta de las Naciones Unidas, Resoluciones y opiniones de la Asamblea Genereal de las Naciones Unidas, la Convención de Ginebra, sentencias de la Corte Internacional de Justicia y de la Corte Penal Internacional, el Manual de Tallin 1.0 y 2.0, opiniones de entidades gubernamentales dedicadas al cibercrimen y a la ciberguerra, así como a autores especialistas en la materia de investigación.

Estructura de la tesis

Luego del presente texto introductorio al trabajo de investigación, el segundo capítulo de la tesis evalúa el marco teórico actual de las nociones y teorías que se desarrollarán a lo largo del trabajo de investigación, así como los alcances y las discrepancias actuales entorno a determinadas figuras legales, conceptuales y jurisprudenciales en el marco del derecho internacional público.

El tercer capítulo define cuáles son los cuatro escenarios tradicionales de combate donde han tenido lugar la mayoría de los enfrentamientos bélicos a lo largo de la historia, frente a la aparición del ciberespacio como un nuevo dominio de batalla.

El cuarto capítulo expresa cuáles son los ciberataques que pueden tener lugar en las operaciones cibernéticas militares y estratégicas perpetradas entre Estados, así como cuáles pueden ser las consecuencias de estos y de qué manera pueden ser considerados una intervención a la luz de la Carta de las Naciones Unidas.

El quinto capítulo introduce la dificultad de los Estados de atribuir con exactitud la responsabilidad de un hecho ilícito internacional, antes de proseguir a activar una defensa contra un presunto culpable. En este análisis se brindan detalles de las dificultades a las que se enfrentan los departamentos de inteligencia de cada Estado a la hora de definir la ciber atribución, debido a la multiplicidad y dispersidad de actores que pueden perpetrar el acto, ocultando al responsable intelectual del hecho.

En el sexto capítulo se analizan cuáles son los requisitos que debe cumplir un hecho ilícito internacional para habilitar la vía de la legítima defensa armada, la cual debe resultar más eficiente que las otras formas de defensa existentes.

Por último, en el séptimo capítulo se encuentran las conclusiones de lo analizado a través de todo el trabajo de investigación, resumiendo los principales aspectos comprendidos así como definiendo nuevas opciones de investigación para futuros proyectos académicos.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo 2: Estado del Arte

Definiciones y alcances

La intersección entre la tecnología y la mayoría de los ámbitos de las sociedades modernas, fruto de las inmensurables innovaciones que han tenido protagonismo en las últimas décadas e impulsadas principalmente por las integraciones en la nube, la robótica y el Internet de las cosas –referente a la posibilidad de conectar cualquier objeto y/o dispositivo a Internet a través de protocolos creados para ello (K. Patel y S. Patel, 2016)-, ha generado un desafiante cambio en la vida de los participantes de este nuevo mundo hiperconectado (Plunkett y Gasser, 2016). Las sociedades de la información, término que no refiere a priori a comunidades hiperconectadas a través de Internet sino a aquellas que se desarrollan a partir del conocimiento como capital y recurso principal, así como una guía para el desarrollo económico y evolutivo de estas (Castelfranchi, 2007), tienen como foco principal la educación y entrenamiento de cada uno de los integrantes de dicha sociedad con el objetivo de obtener una posterior contribución de ellos en el conocimiento de la comunidad, viendo a las personas como talentos y generadores innatos de conocimiento (Lauwers, 2019).

La innovación tecnológica del siglo XXI ha sido una llave a un nuevo mercado de oportunidades laborales, sociales y culturales, que han tenido un gran impacto en la sociedad. El autor Zang (2021) analiza las diversas formas en las cuáles la innovación tecnológica tiene efectos en la población, y concluye en que a veces el interés público de la sociedad es afectado por el uso de las nuevas tecnologías, pero no siempre es considerado a la hora de desarrollarlas. En esta línea, a lo largo de la historia los diversos inventos revolucionarios han tenido grandes impactos en las poblaciones, y que han ido amoldándose con el paso del tiempo con la finalidad de que sus consecuencias ayuden a más gente que a las que perjudican por su nueva existencia. Por ello, la innovación es considerada un conjunto de desarrollos llevados adelante para la mejora de procesos, que difieren significativamente de sus antecesores (OCDE, 2018).

Especialmente, Naciones Unidas (2018) reporta además un claro avance en el desarrollo de tecnología sustentable en los últimos años, a través de la inteligencia artificial y big data, la impresión 3D, la biotecnología e innovación en materia de salud, los avances materiales de nanotecnología, las tecnologías de energía renovable, los satélites, los drones y la tecnología Blockchain.

Sin perjuicio de que la hiperconexión de las sociedades de la información no hacen a su denominación sino su apuesta e inversión por el desarrollo del conocimiento, la tecnología que desarrollan las sociedades que conecta el conocimiento y la información generada tanto interna como externamente, tiene un protagonismo crucial a la hora de medir la evolución y el crecimiento de un país (Perepelkin, Perepelkina

y Morozova, 2016). En la actualidad, la mayoría de los ámbitos de rubros de una sociedad que hacen al desarrollo económico, como la educación, las industrias de servicios profesionales, el entretenimiento, la salud, el transporte, entre otros, se apoyan cotidiana y masivamente en las tecnologías de la información (Berisha-Shaqiri y Berisha-Naman, 2015).

Esta dependencia tecnológica tiene una sustancial parte positiva, que deriva de los avances en todos los ámbitos mencionados que se sirven constantemente de los beneficios del Internet y otras tecnologías, que dan pie a un intercambio inmediato de información, pero por el otro, tiene el efecto negativo de excluir a un determinado porcentaje de la población mundial que carece de conectividad y por ende acceso a los servicios conectados a la Red (ECLAC, 2021). Un ejemplo concreto de los beneficios de la innovación tecnológica son los avances en materia de salud y medicinas, donde los descrubrimientos de científicos, ingenieros y tecnólogos salvan la vida de millones de personas con sus inventos (Laal, 2012). En la parte negativa de una tan intensa dependencia sobre la tecnología, se encuentran los inmensos riesgos a los que se exponen todos los ámbitos interconectados por el simple hecho de servirse de su conexión (Strupczewski, 2021).

El ciberespacio, considerado un mundo virtual multidimensional y artificial creado por máquinas, redes e información (Haig, 2021), se convierte en el principal ámbito que interconecta la industria del conocimiento, el cual resulta necesario para ella. Esto resulta innovador ya que en la también llamada economía del conocimiento, el principal recurso potenciador no tiene relación con factores materiales, como ocurría en tiempos anteriores, sino que en este caso el principal poder de producción se encuentra en el cerebro (Berisha-Namani y Badivuku-Pantina, 2009), por lo que tanto el conocimiento humano como el ciberespacio, no están anexados a elementos materiales o físicos. El Ciberespacio conecta el mundo con su existencia, y permite que la información generada en un país pueda transmitirse inmediatamente a otro, achicando las distancias físicas y permitiendo un aprendizaje de las experiencias de otras personas, lo cual recae nuevamente en cómo la tecnología está focalizada en el aumento de conocimiento (Ali, B. Kwame, Nam, Svetlik y Zhong, 2019). Hoy se considera al conocimiento como un contribuidor clave en el avance de las economías (OCDE, 2013).

La existencia de un ciberespacio de uso masivo para las sociedades de la información, que apuestan principalmente al conocimiento y al intercambio de información a través de este espacio, da lugar a un nuevo tipo de riesgos, el cibernético. Strupczewski (2021) los define de la siguiente manera:

> Cyber risk is an operational risk associated with performance of activities in the cyberspace, threatening information assets, ICT resources

> and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term ’cyber risk’ also includes physical threats to the ICT resources within organisation. [El riesgo cibernético es un riesgo operativo asociado a la realización de actividades en el ciberespacio, que amenaza los activos de información, los recursos de TIC y los activos tecnológicos, y que puede causar daños materiales a los activos tangibles e intangibles de una organización, la interrupción de la actividad o el daño a la reputación. El término "riesgo cibernético" también incluye las amenazas físicas a los recursos TIC de la organización] (p.2).

En línea con la existencia de riesgos cibernéticos, existen diversos rubros que cuentan con una mayor sensibilidad por la posibilidad de ser vulnerados a través de la Red, cuya causa es la cantidad de personas que dependen de su servicio. En concreto, El Parlamento Europeo y el Consejo de Europa (2019) señalan que:

> La intensificación de la digitalización y de la conectividad trae consigo un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resulta más vulnerable a las ciberamenazas y se exacerban los peligros a que se enfrentan las personas, incluidas las personas vulnerables como los niños (cons. 3).

Por un lado, el Estado argentino ha definido (2019) a las infraestructuras críticas como:

> Aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente (Punto I, primer párrafo).

Por el otro, consideró a las infraestructuras críticas de información como “las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas” (Punto I, segundo párrafo).

Las infraestructuras críticas son operadores esenciales o instituciones de grande relevancia, debido a que cumplen una función esencial para una sociedad, y, en caso de interrupir sus servicios debido a fallas accidentales o causadas intencionalmente, perjudicarían a un gran porcentaje de personas, por lo que el Estado se vería también perjudicado por tener que solucionar dicho problema para reanudar el ofrecimiento del servicio interrumpido. Además, las infraestructuras críticas de una sociedad tienen como objetivo no sólo el ofrecimiento de determinados bienes y servicios, sino también el de promover el desarrollo económico, social, político, cultural y hasta el bienestar de la población, por lo que una grave afectación a una infraestructura crítica podría culminar en un grave golpe para la estabilidad de un gobierno (CISA, 2019).

Cualquier actividad cuya finalidad es socavar, atacar o desestabilizar un activo cibernético o red de computadoras, sea con finalidades de delincuencia, política, inteligencia, ataque o defensa militar, u otras, es denominado un ciberataque (Hathaway et al., 2012). Otra definición, un tanto más amplia refiere al ciberataque como toda operación cibernética que pueda razonablemente generar daños a personas u objetos (Manual de Tallin, 2013). Los ciberataques son realizados de manera constante y masiva en la actualidad, y son una de las principales formas de delincuencia en el mundo y con mayor crecimiento en los últimos años (Interpol, 2021).

Debido al enorme incremento de la delincuencia informática en los últimos años, y la gran exposición de las infraestructuras críticas a los riesgos que existen por el hecho de estar conectados y transferir importante cantidad de información a través del ciberespacio, la seguridad en el uso masivo de los sistemas de tecnología de la información se han convertido en un factor clave dentro de las agendas de trabajo de los gobiernos (ECLAC, 2021).

Una de las características principales de los ciberataques es la posibilidad de contar con una gran asimetría entre su causa y consecuencia (Reséndiz, 2019), lo cual refiere, ejemplificativamente y en otras palabras, a que una persona puede perjudicar a millones, o que la ejecución de un código puede resultar devastador para todo un sistema electrónico de miles de ellos. En la actividad de ciberatacar, si bien puede medirse en las cantidad de personas inmersas en un plan, o en el presupuesto contado para financiar la actividad criminal o bélica, uno de los grandes diferenciales que puede darse en el éxito del ciberataque se da a través de la estrategia e inteligencia empleada en él, por lo que una vez más, el conocimiento resulta un recurso indispensable.

Cuando las actividades cibernéticas –o ciberactividades-, consideradas estas actividades similares a las que tienen las personas en el mundo físico (Olasunkanmi Oluga, 2014), y donde existen aquellas ilegales

que hoy tienen gran protagonismo asechando a las empresas del sector privado y a la población (Li, 2017), se utilizan coordinadamente mediante herramientas técnicas cuya finalidad es alcanzar objetivos militares o de inteligencia sobre otro Estado, a través del acceso a los sistemas, la intercepción de sus comunicaciones, entre otras formas de ataques nacionales direccionados, estas quedan inmersas dentro de lo que se conoce como operaciones cibernéticas –también conocidas como ciberoperaciones u operaciones de ciberguerra- (Haig, 2021).

En esta línea discursiva, no todas las actividades cibernéticas ilegales son ciberataques; no todos los ciberataques son operaciones cibernéticas con objetivos militares o de inteligencia; y no todas las operaciones son ciberataques. Existe cierta independencia entre los términos, aunque en la práctica suelen confundirse y utilizarse como sinónimos.

Sin embargo, en este punto resulta menester aclarar que los ciberataques que hacen a la ciberguerra no deben corresponderse únicamente con un ataque tradicional a infraestructuras tecnológicas (Bendovschi, 2015), sino que pueden tener además objetivos que directa o indirectamente afecten activos valiosos para un gobierno, cuyo ataque produzca o pretenda producir una leve o grave desestabilización de este sin que el Estado víctima, aún descubriendo el hecho ilegal, tenga la facultad de detectar con claridad quién es el responsable de dicho ataque, lo que se conoce como la problemática de la ciber atribución (Goldstein, 2013).

En esta línea, al analizar cómo un ciberataque a un Estado puede resultar en efectos desestabilizadores para el gobierno y su población, López de Turiso y Sanchez (2012) define que:

> ...un ciberataque bien organizado, coordinado y dirigido a la línea de flotación de un país puede dejar inutilizado sus sistemas de comunicación, sus infraestructuras críticas o su capacidad de mando y control, tanto civil como militar. Esto puede hacer que se desestabilice su centro de gravedad y le produzca graves consecuencias políticas, económicas o sociales (p.143).

Como ejemplo de ciberataques no tradicionales, un Estado que permite el ciber lavado o fuga de activos de un Estado hacia el suyo, podría ser considerado también un acto de ciberguerra, por contar con la posibilidad de desestabilizar la economía del Estado víctima de dicho lavado (Uzal, Riesco, Montejano, Agüero y Baieli, 2015).

Por lo tanto, para considerar el impacto que puede tener un ciberataque sobre un Estado, debe partirse desde la consideración de los tipos de daños que pueden ser alcanzados a través de la vía cibernética, para lograr dimensionar las consecuencias de ellos y no tan sólo categorizarlos por su causa. Agrafiotis, Nurse, Goldsmith, Creese y Upton (2018) definieron las clases de daños que puede tener un ataque sobre un Estado de la siguiente manera:

> The main harm types we include are:
>
> - Physical or Digital harm (i.e. harm describing a physical or digital negative effect on someone or something).
> - Economic harm (i.e. harm that relates to negative financial or economic consequences).
> - Psychological harm (i.e. harm which focuses on an individual and their mental well-being and psyche).
> - Reputational harm (i.e. harm pertaining to the general opinion held about an entity).
> - Social and Societal harm (i.e. a capture of harms that may result in a social context or society more broadly).
>
> [Los principales tipos de daños que incluimos son:
>
> - Daño físico o digital (es decir, el daño que describe un efecto negativo físico o digital sobre alguien o algo).
> - Daño económico (es decir, daño relacionado con consecuencias financieras o económicas negativas).
> - Daño psicológico (es decir, el daño que se centra en un individuo y en su bienestar mental y psíquico).
> - Daño reputacional (es decir, el que se refiere a la opinión general que se tiene de una entidad).

- Daño social y societario (es decir, un conjunto de daños que pueden producirse en un contexto social o en la sociedad en general)] (p.7).

Algunos antecedentes de ciberguerra

En las últimas décadas han habido diversos casos que han sido catalogados como actos de ciberguerra. La década de 1990 fue caracterizada por un enorme incremento del uso de Internet en el sector privado, sumado a la cantidad de infraestructuras críticas que comenzaron a utilizar el ciberespacio por sus ventajas en el ofrecimiento de servicios, lo que resultó en un detonante de que el ciberespacio podía ser una eficiente vía de ataque para desestabilizar a un país, sea cual fuera la gravedad del acto a perpetrar. Además, comenzaron a verse ataques realizados por atacantes individuales que buscaban probar las consecuencias de sus conocimientos informáticos, sin que ello sea buscado con fines bélicos (Kozlowski, 2014).

El primero de los ciberataques entre Estados ha sido perpetrado en Estonia en el año 2007, siendo considerado uno de los casos más populares y reconocidos de actividades realizadas en el marco de operaciones de ciberguerra. Sin embargo, dicho caso no fue tratado en su origen como un ataque armado, debido, entre otras cosas, a las consecuencias geopolíticas que podía acarrear el involucramiento de la Organización del Tratado del Atlántico Norte, conocida popularmente como la OTAN, en defensa de un ataque armado perpetrado a uno de sus Estados miembros (Hayward, 2017).

El ciberataque a Estonia, del cual se acusa al gobierno de Rusia como responsable sin aún contarse con la totalidad de evidencia que así lo confirme, consistió en un conjunto masivo de ataques de denegación de servicios que dejaron indisponibles a los servicios estatales estonios por el lapso de tres días. Este ataque, perpetrado luego de una tensión política entre el país báltico y Rusia, fue una de las causas que llevaron luego a Estonia a convertirse en uno de los países líderes en materia de ciberseguridad, contando con metodologías de denfesa cibernéticas que son tomadas como referencia en el resto de los países del mundo, por sus elevadas habilidades de resiliencia ante ataques externos (Egtan, 2018).

El segundo caso de ataques cibernéticos considerados actos de ciberguerra, fue el sufrido por Georgia en el año 2008. Este ciberataque, del cual también se acusa a Rusia como responsable, tuvo la característica de haber sido una herramienta más de combate en el marco de una batalla en múltiples escenarios bélicos. Es decir, el ciberespacio fue una vía que se agregó al aire, la tierra y el mar como espacios de batalla. De similar manera al ataque estonio, nuevamente se trataron de ataques de denegación de servicios contra páginas georgias, considerando a su vez que las redes locales contaban con peores infraestructuras que las estonias y resultaban más vulnerables a los ataques perpetrados. (Kozlowski, 2014).

En el ciberataque del cual Georgia fue víctima, la metodología implementada por el Estado ruso tuvo dos estrategias diferenciadas. La primera de ellas constitió en una estrategia para socavar los comandos de control y armamento georgio, mientras que la segunda se concentró en utilizar el ciberataque como forma de desestabilización psicológica dentro de la población georgia, a través del ataque de los medios de comunicación social y las telecomunicaciones (Blank, 2017). En referencia de ambas clases de ciberataques, al poco tiempo de iniciado este accionar la mayoría de los sitios web del gobierno georgio estaban caídos, el gobierno tenía indisponibilidad de comunicaciones a través de Internet, los bancos no podían operar y la población no podía utilizar sus dispositivos celulares por falta de señal (Kozlowski, 2014).

Si bien Kirguistán hoy ha demostrado un gran desarrollo económico en base a su resiliencia cibernética y apuesta por las nuevas tecnologías y su mejora constante (Karazhanova y Dyakonova, 2021), podría decirse que su actual desempeño resulta un aprendizaje de lo sucedido en el año 2009, donde el Estado sufrió un ataque ruso de denegación de servicios a dos servidores web que hicieron caer diversos sitios web así como servicios de correo electrónico dentro del país, ataque que fue relacionado con conflictos políticos entre Kirguistán y Rusia, de la misma manera que en los casos de Estonia y Georgia (Ashmore, 2009).

Otro de los casos resonantes relacionados a ciberataques que pueden ser considerados dentro del marco de operaciones de ciberguerra, es el de Stuxnet, en el año 2010. Sin embargo, este caso resultó ser un antes y un después para la ciberguerra a nivel internacional, debido a que fue la primera vez que el ciberespacio fue utilizado como escenario de combate, donde el ciberataque fue utilizado como un arma, y ya no solo como un ataque de denegación de servicios web (Wirtz, 2015).

El ciberataque de Stuxnet tuvo como víctima al Estado iraní, quien en 2010 sufrió la infección de un aproximado de 60 mil computadoras, así como las de una planta nuclear dedicada al enriquecimiento de uranio, en la localidad de Natanz. La consecuencia esperada de dicho ataque fue la inutilización parcial de dicha planta (Maskun, Irwansyah, Yunus, Safira y Nurhalima Lubis, 2021). El ataque de Stuxnet contenía características técnicas avanzadas, lo que comenzó a despertar el interés por los Estados para desarrollar mayores herramientas estratégicas de ataque y defensa dentro de este nuevo escenario: el ciberespacio, como ámbito de operaciones bélicas (Farwell y Rohozinski, 2011).

Nociones de derecho y jurisprudencia internacional

Con los antecedentes de la primera y segunda guerra mundial, y con la creación de la Liga de las Naciones en 1919, diversas grandes potencias comenzaron a desear a principios de la década de 1940 la creación de una organización internacional que ponga fín al sufrimiento generado por los conflictos bélicos

alrededor del mundo (Santa Cruz, 1995). El 1° de enero de 1942, 26 Estados soberanos celebraron un instrumento internacional denominado como la Declaración de las Naciones Unidas, estableciendo cooperación mutua entre los signatarios y a favor de la promoción de la paz mundial (Naciones Unidas, 1947).

En el año 1945 se celebró la Carta de las Naciones Unidas, instrumento internacional que dio origen formal a la Organización de las Naciones Unidas (ONU), y que fue realizado en la Conferencia de San Francisco, una convención de delegados de naciones aliadas durante la Segunda Guerra Mundial. El texto de la Carta respondió, según Campos Salazar (2019): "*a la presión de ciertos movimientos políticos derivados de las guerras, los cuales se apegaron a los derechos naturales y a las libertades humanas que desde 1948 s denominaron 'derechos humanos'*" (p.119).

El primer artículo de la Carta se encarga de establecer cuáles son los propósitos de las Naciones Unidas:

> Los propósitos de las Naciones Unidas son:
>
> Mantener la paz y la seguridad internacionales, y con tal fin: tomar medidas colectivas eficaces para prevenir y eliminar amenazas a la paz, y para suprimir actos de agresión u otros quebrantamientos de la paz; y lograr por medios pacíficos, y de conformidad con los principios de la justicia y del derecho internacional, el ajuste o arreglo de controversias o situaciones internacionales susceptibles de conducir a quebrantamientos de la paz;
>
> Fomentar entre las naciones relaciones de amistad basadas en el respeto al principio de la igualdad de derechos y al de la libre determinación de los pueblos, y tomar otros medidas adecuadas para fortalecer la paz universal;
>
> Realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión; y
>
> Servir de centro que armonice los esfuerzos de las naciones por alcanzar estos propósitos comunes. (Art. 1°).

La Carta, conformada por 111 artículos, representa una guía para las relaciones diplomáticas internacionales y ha ayudado en múltiples oportunidades a determinar la legalidad de los actos que los Estados miembros de la Organización de las Naciones Unidas incurre diariamente, con el principal objetivo de traer paz al mundo luego de tanto conflicto bélico.

Cuando en materia de relaciones internacionales se refiere al derecho internacional público, lo que se busca es enmarcar el conjunto de actos dentro de la legislación internacional pública, esto es, de los organismos, tratados, leyes, normas y jurisprudencia internacional, y que los Estados deben observar para mantener vínculos pacíficos con sus pares soberanos (Alqamoudi, 2021). En esta línea, la Carta de la ONU, así como todo el conjunto de opiniones y material jurídico creado posteriormente, sirven de fuente indiscutible para el desarrollo y consolidación del derecho internacional público (Schrijver, 2006).

La ONU es la organización internacional que en la actualidad reúne la mayor cantidad de Estados soberanos del mundo, y está estructurada a través de una Asamblea General, un Consejo de Seguridad, un Consejo Económico y Social, un Consejo de Administración Fiduciaria, la Secretaría de Naciones Unidas y la Corte Internacional de Justicia, cuya sede se encuentra en La Haya, Países Bajos, y cuyo Estatuto forma parte integrante de la Carta.

El segundo artículo de la Carta se encarga de delinear una serie de principios básicos y generales a los cuáles todos los Estados miembros deben seguir atentamente, ya que la totalidad de artículos que prosiguen a él están alineados a los mencionados principios. El primero de los principios establece la igualdad soberana entre todos los Estados miembros, y representa uno de los grandes pilares de la Carta. Este principio refiere a que, bajo la órbita del derecho internacional público que surja de las disposiciones tanto de la Carta como de cualquier otro instrumento internacional, todos los países deberán cumplirlos y ser juzgados de igual forma y condición, con independencia y sin preferencias o desventajas para alguna de las partes (Ramírez Bulla, 2008).

El cuarto principio del artículo 2, establece prohibición general de utilizar el uso de la fuerza, al expresar que:

> Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas (artículo 2, párr. 4°).

El principio de la no intervención, establecido por el artículo 2, párrafo 7° de la Carta, es el principio más importante e indispensable para la línea de compresión del presente trabajo de investigación.

> Ninguna disposición de esta Carta autorizará a las Naciones Unidas a intervenir en los asuntos que son esencialmente de la jurisdicción interna de los Estados, ni obligará; a los Miembros a someter dichos asuntos a procedimientos de arreglo conforme a la presente Carta; pero este principio no se opone a la aplicación de las medidas coercitivas prescritas en el Capítulo VII (Art. 2°, párr. 7).

La Resolución 2131 de la Asamblea de las Naciones Unidas, del año 1965, trató una posible aclaración al principio de la no intervención, y estableció lo siguiente:

> No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned [Ningún Estado tiene derecho a intervenir, directa o indirectamente, por cualquier motivo, en los asuntos internos o externos de otro Estado. En consecuencia, se condenan la intervención armada y todas las demás formas de injerencia o de tentativa de amenaza contra la personalidad del Estado o contra sus elementos políticos, económicos y culturales] (Párr. 1).

En 1970 la Asamblea volvió a expedirse sobre este tema, analizando el alcance del concepto de intervención en virtud del principio de la Carta, y lo ha hecho de la siguiente forma:

> Ningún Estado o grupo de Estados tiene derecho a intervenir directa o indirectamente, y sea cual fuere el motivo, en los asuntos internos o externos de ningún otro. Por lo tanto, no solo la intervención armada, sino también cualquier otra forma de injerencia o de amenaza atentatoria de la personalidad del Estado, o de los elementos políticos, económicos y culturales que lo constituyen, son violaciones del derecho internacional.

> 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 ejecicio de sus derechos soberanos y obtener de él ventajas de cualquier orden. Todos los Estados deberán también 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 las luchas interiores de otro Estado (punto 1, párr. 24-25).

Nuevamente, se da pie a la existencia de formas de intervención que exceden de aquella realizada mediante el uso de la fuerza, la cual se produce a través de diversas formas de injerencia contra la soberanía de un Estado.

Y como una violación al principio de la no intervención podría requerir medidas urgentes para detener un acto de graves consecuencias, tal como se desprende de las últimas palabras del artículo de la Carta, el mencionado no se opone a la toma de medidas establecidas en el Capítulo séptimo de la Carta, donde se encuentran las disposiciones dedicadas a las acciones a tomar por parte de los Estados miembros y la Organización en caso de amenazas a la paz y/o actos de agresión. Esto significa que, en caso de que un Estado ponga o pueda poner en peligro la paz internacional, el Consejo de Seguridad y, en algunos casos, el Estado víctima de dicha intervención, estará facultada para intervenir en los asuntos internos del Estado culpable de dicho acto, lo cual podrá tener forma de medidas tanto con o sin uso de la fuerza.

Existen dos categorías de acciones que puede tomar la Organización de las Naciones Unidas, a través del Consejo de Seguridad, en casos de amenazas a la paz internacional por parte de un Estado miembro. La primera de ellas se encuentra expresa en el artículo 41 del instrumento:

> El Consejo de Seguridad podrá decidir qué medidas que no impliquen el uso de la fuerza armada han de emplearse para hacer efectivas sus decisiones, y podrá instar a los Miembros de las Naciones Unidas a que apliquen dichas medidas, que podrán comprender la interrupción total o parcial de las relaciones económicas y de las comunicaciones ferroviarias, marítimas, aéreas, postales, telegráficas, radioeléctricas, y otros medios de comunicación, así como la ruptura de relaciones diplomáticas (art. 41°).

En otras palabras, la primera categoría de medidas por parte del Consejo de Seguridad refiere a aquellas que no implican el uso de la fuerza armada, y que tienen como objetivo perjudicar la estabilidad económica, política y social del Estado causador del daño, buscando persuadir a los gobernantes de dicho Estado para que cesen con el curso de sus actividades ilegales.

El segundo grupo de medidas se encuentran en el artículo 42 de la Carta, y refieren a aquellas que sí consisten en el uso legítimo de la fuerza armada por parte de la Organización.

> Si el Consejo de Seguridad estimare que las medidas de que trata el Artículo 41 pueden ser inadecuadas o han demostrado serlo, podrá ejercer, por medio de fuerzas aéreas, navales o terrestres, la acción que sea necesaria para mantener o restablecer la paz y la seguridad internacionales. Tal acción podrá comprender demostraciones, bloqueos y otras operaciones ejecutadas por fuerzas aéreas, navales o terrestres de Miembros de las Naciones Unidas (Art. 42°).

Al establecer el principio de la no intervención una excepción de cumplimiento con respecto a las medidas establecidas en el Capítulo séptimo de la Carta, estas medidas exceptuadas no se limitan únicamente a aquellas –con o sin uso de la fuerza- llevadas adelante por el Consejo de Seguridad, sino que existe un supuesto en el cual los mismos Estados miembros, individualmente y por fuera de una solicitud del Consejo de Seguridad, pueden utilizar el uso de medidas que representen una intervención en los asuntos internos de otro Estado, sin violar el artículo 2° de la Carta. Este caso, es el de la legítima defensa establecido por el artículo 51 del mismo instrumento:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales (Art. 51°).

En otras palabras, en caso de que un Estado miembro sufra una intervención por parte de otro Estado, el primero podrá hacer uso de la legítima defensa, únicamente cuando la intervención se haya producido a través de un ataque que sea considerado armado, para lo cual el Estado deberá informar de manera inmediata al Consejo sobre sus medidas defensivas tomadas, mientras espera las acciones que tomará el Consejo de Seguridad como parte de sus paquetes de medidas de los artículos 40 y siguientes de la Carta.

La Corte Internacional de Justicia (ICJ) se ocupó de definir y analizar algunos de estos conceptos en su sentencia del año 1986, para el caso de Nicaragua contra Estados Unidos de América, referido a las actividades militares y paramilitares en Nicaragua y contra Nicaragua. En este fallo, estableció que:

> Whtsther self-defence be individual or collective, it can only be exercised in response to an "armed attack". In the view of the Court, this is to be understood as meaning not merely action by regular armed forces across an international border, but also the sending by a State of armed bands on to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack had it been carried out by regular rumed forces. [Ya fuera individual o colectiva, la legítima defensa sólo podía ejercerse como reacción a un "ataque armado". A juicio de la Corte, podía entenderse que eso significaba no sólo acciones emprendidas por fuerzas armadas regulares a través de una frontera internacional, sino también el envío por un Estado de bandas armadas al territorio de otro Estado, si esa operación, por su escala y efectos, se hubiera clasificado como un ataque armado en caso de ser realizada por fuerzas armadas regulares] (p.165).

Por otro lado, la Corte analizó también el prinicipio de la no intervención, y dispuso que:

> ...a prohibited intervention must be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely (for example the choice of a political, economic, social and cultural system, and formulation of foreign policy). Intervention is wrongful when it uses, in regard to such choices, methods of coercion, particularly force, either in the diit form of military action or in the indirect form of support for subversive activities in another State. [...una intervención prohibida debe ser aquella que incide en cuestiones en las que cada

> Estado está autorizado, en virtud del principio de soberanía estatal, a decidir libremente (por ejemplo, la elección de un sistema político, económico, social y cultural, y la formulación de la política exterior). La intervención es ilícita cuando utiliza, en relación con tales elecciones, métodos de coacción, en particular la fuerza, ya sea en forma de acción militar o en forma indirecta de apoyo a actividades subversivas en otro Estado.] (p.165)

Además, la Asamblea General de las Naciones Unidas (1974) también se expidió sobre este tema y otros relacionados, lo cual fue consecuencia del trabajo de una Comisión Especial creada por la Resolución 688 para el tratamiento de estos conceptos (Marqués Rueda, 2009), y cuyo texto, ha sido también utilizado por la CIJ en el caso de Nicaragua v. Estados Unidos de América, y ha establecido que:

> Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. [Agresión es el uso de la fuerza armada por parte de 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 las Naciones Unidas, como se establece en esta Definición] (Artículo 3°).

La Convención de Ginebra de 1949 estableció en su artículo 2° que tendría jurisdicción ante casos de guerra declarada o de cualquier otro conflicto armado que pueda surgir entre Estados, pero no se ocupó de definir qué clases de actos podrían quedar inmersos en dicha categoría de conflictos. Luego, el primer protocolo adicional a dicho Convenio (1977) agregó algunas concepciones más a este término, refiriendo a que los conflictos armados son aquellos:

> ...en que los pueblos luchan contra la dominación colonial y la ocupación extranjera y contra los regímenes racistas, en el ejercicio del derecho de los pueblos a la libre determinación, consagrado en la Carta de las Naciones Unidas y en la Declaración sobre 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 (artículo 1°, párrafo 4).

Sin embargo, continuaba una falta de claridad en cuanto a la definición del conflicto armado. Ante esta situación, el Tribunal Penal Internacional para la Antigua Yugoslavia (ICTY), creado por el Consejo de Seguridad mediante la Resolución 808 de 1993 para juzgar los crímenes de guerra en la ex-Yugoslavia, se ocupó de tratar este tema en el caso Tadic (1995), donde expresó:

> ...we find that an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State. [...consideramos que existe un conflicto armado siempre que se recurra a la fuerza armada entre Estados o a la violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados o entre dichos grupos dentro de un Estado] (Párr.70).

La definición del crimen de agresión ha representado diversos desafíos a lo largo del tiempo, y vale destacar que la definición de la Resolución de 1974 no había sido incorporada a ningún tratado, lo cual puede reflejarse en el Estatuto de Roma de la Corte Penal Internacional (CPI), el cual estableció en su artículo quinto que la Corte tendría jurisdicción sobre esta clase de crimen únicamente cuando se haya definido dicha categoría de crimen (Vallarta Marrón, 2011).

Durante la Conferencia de Revisión del Estatuto de Roma de 2010, donde se celebraron las conocidas enmiendas de Kampala mediante la Resolución N°6, relativas exclusivamente al crimen de agresión, se estableció una definición para este crimen, al disponer lo siguiente:

> 1. A los efectos del presente Estatuto, una persona comete un "crimen de agresión" cuando, estando en condiciones de controlar o dirigir efectivamente la acción política o militar de un Estado, dicha persona planifica, prepara, inicia o realiza un acto de agresión que por sus características, gravedad y escala constituya una violación manifiesta de la Carta de las Naciones Unidas.
>
> 2. A los efectos del párrafo 1, por "acto de agresión" se entenderá el uso de la fuerza armada 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 las Naciones Unidas. De conformidad con la resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1974, cualquiera de los actos siguientes,

> independientemente de que haya o no declaración de guerra, se caracterizará como acto de agresión:
>
> a) La invasión o el ataque por las fuerzas armadas de un Estado del territorio de otro Estado, o toda ocupación militar, aún temporal, que resulte de dicha invasión o ataque, o toda anexión, mediante el uso de la fuerza, del territorio de otro Estado o de parte de él;
>
> b) El bombardeo, por las fuerzas armadas de un Estado, del territorio de otro Estado, o el empleo de cualesquiera armas por un Estado contra el territorio de otro Estado;
>
> c) El bloqueo de los puertos o de las costas de un Estado por las fuerzas armadas de otro Estado;
>
> d) El ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres, navales o aéreas de otro Estado, o contra su flota mercante o aérea;
>
> e) La utilización de fuerzas armadas de un Estado, que se encuentran en el territorio de otro Estado con el acuerdo del Estado receptor, en violación de las condiciones establecidas en el acuerdo o toda prolongación de su presencia en dicho territorio después de terminado el acuerdo;
>
> f) La acción de un Estado que permite que su territorio, que ha puesto a disposición de otro Estado, sea utilizado por ese otro Estado para perpetrar un acto de agresión contra un tercer Estado;
>
> g) El envío por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación en dichos actos (artículo 8 bis).

Por lo expuesto, existe una cierta sintonía entre los entendimientos del derecho internacional con respecto al conflicto o ataque armado y la agresión de un Estado hacia otro, lo cual puede verse reflejado entre los Convenios de Ginerbra, el fallo de Nicaragua de la CIJ y el caso Tadic de la ICTY (Pinto, 2003).

Como conclusión de lo narrado anteriormente, un acto Estatal que interviene en los asuntos internos de un tercer Estado, viola el artículo 2, párrafo 7° de la Carta, y por ende deja a dicho Estado en una situación de incumplimiento ante la Carta de las Naciones Unidas. Sin embargo, para que dicho acto que viola el derecho internacional, de lugar a una legítima defensa en virtud del artículo 51 del mismo instrumento, por parte del Estado víctima de la intervención, debería analizarse previamente a la defensa si dicho acto ha sido un ataque armado a la luz de la ley, doctrina y jurisprudencia internacional, para que el accionar defensivo sea legítimo.

Según lo dispuesto por la Asamblea General de las Naciones Unidas y la CPI, un ataque armado es aquel que involucra a las fuerzas armadas de un Estado, y que implica una agresión hacia otro Estado, lo cual puede implicar una violación a su soberanía, integridad, independencia, e incluso, cualquier otra violación a los principios de la Carta. Este último supuesto que se encuentra en la definición de agresión, que contempla la posibilidad de que se produzca esta ante una violación a los principios, podría fundar la idea de que una violación al principío de la no intervención, independientemente de la vía por la cual se produzca, podría ser considerada un ataque armado y por lo tanto, dar lugar a la legítima defensa, también armada, por parte del Estado vícitma, en virtud del artículo 51 de la Carta.

El Manual de Tallin

En el año 2013, luego de 3 años de trabajo por un Grupo Internacional de Expertos multidisciplinarios y por invitación del Centro de Excelencia en Defensa Cibernética Cooperativa (CCDCOE) de la Organización del Tratado del Atlántico Norte (OTAN), se aprobó el Manual de Tallin sobre el derecho internacional aplicable a la guerra cibernética, el cual consiste en una serie de reglas y comentarios, y no tiene la misma forma jurídica vinculante que sí poseen los tratados internacionales, pero cuenta con un gran valor académico que es utilizado regularmente para evaluar las conductas cibernéticas de los Estados y analizarlas de acuerdo a ciertos parámetros (Schmitt, 2012).

La falta de efectos vinculantes del Manual se desprende de la misma introducción del documento original (2013), el cual describe:

> Like its predecessors, the Manual on the International Law Applicable to Cyber Warfare, or ‘Tallinn Manual’, results from an expert-driven process designed to produce a non-binding document applying existing law to cyber warfare. [Al igual que sus predecesores, el Manual sobre el Derecho Internacional Aplicable a la Ciberguerra, o "Manual de Tallin", es el resultado de un proceso impulsado por expertos con el fin de

> elaborar un documento no vinculante que aplique el derecho existente a la ciberguerra] (p.1).

Sin perjuicio de la falta de efectos vinculantes, el Manual representa un medio de interpretación complementario de la Carta de las Naciones Unidas y otros instrumentos internacionales, lo cual podría enmarcarse perfectamente dentro del artículo 32 de la Convención de Viena sobre el derecho de los tratados (1969), el cual dispuso que:

> …Se podrán acudir a medios de interpretación complementarios, en particular a los trabajos preparatorios del tratado y a las circunstancias de su celebración, para confirmar el sentido resultante de la aplicación del artículo 31, o para determinar el sentido cuando la interpretación dada de conformidad con el artículo 31: a) deje ambiguo u oscuro el sentido; o b) conduzca a un resultado manifiestamente absurdo o irrazonable (artículo 32).

Como el Manual de Tallin original se especializó en el tratamiento de aquellos actos cibernéticos aplicables a conflictos armados, en el año 2017 se aprobó una extensión del Manual, conocida como la versión 2.0, la cual amplió su alcance a operaciones cibernéticas en tiempos de paz, que puedan no ser consideradas parte de un conflicto armado y no sean asociadas al uso de la fuerza armada; nuevamente, destacando que no se trata de una guía de buenas prácticas o una ley con efectos vinculantes (Jensen, 2017).

El Manual aporta diversas nociones de cómo debe aplicarse a las actividades realizadas a través del ciberespacio, una de ellas es la idea de la soberanía de los Estados extendida al ámbito cibernético, lo cual podría aplicarse también al principio de la Carta de las Naciones Unidas con respecto a la soberanía. En el Manual se dispone en su primera regla que: "*States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure*" [*Los Estados gozan de soberanía sobre cualquier infraestructura cibernética situada en su territorio y sobre las actividades asociadas a ella*] (Manual de Tallin 2.0, 2017, Regla 1). Sin perjuicio de ello, el Manual de Tallin 1.0 había ya definido a las infraestructuras cibernéticas como aquellas comunicaciones, almacenamientos y recursos computacionales que operan a través de sistemas de información (Manual de Tallin 1.0, 2013, p.15).

Además, la soberanía de Tallin también debe interpretarse como extensiva, además de las infraestructuras cibernéticas y actividades asociadas, a las personas, por lo que una operación cibernética que impacte no a infraestructuras gubernamentales pero sí a la población civil, podría quedar enmarcada dentro de una violación a este principio (Manual de Tallin 2.0, 2017, Regla 2).

Si bien el ciberespacio es comúnmente asociado con la falta de presencia física, el grupo de expertos deja en claro que las actividades cibernéticas suelen tener consecuencias en los territorios y los elementos físicos que forman parte de ellos, donde se ejerce la soberanía regularmente; esta concepción es apuntada como la capa física del ciberespacio (Manual de Tallin 2.0, 2017, regla 2.4).

El Manual 1.0 (2013) estableció que: "*if such cyber operations are intended to coerce the government (and are not otherwise permitted under international law), the operation may constitute a prohibited "intervention" or a prohibited "use of force"*" [*si dichas operaciones cibernéticas tienen por objeto coaccionar al gobierno (y no están permitidas por el derecho internacional), la operación puede constituir una "intervención" prohibida o un "uso de la fuerza" prohibido*] (Regla 1.7).

Una de las nociones que más impacto posee a la hora de analizar las consecuencias legales que puede acarrear una actividad cibernética perpatrada por un Estado hacia otro, en linea con la ya desarrollada violación a la soberanía internacional, se da cuando el Manual establece, aclarando que lo hace en sintonía con el fallo de la Corte Internacional de Justicia en el caso Nicaragua contra Estados Unidos de América, que una operación cibernética constituye un uso de la fuerza cuando su escala y efectos son comparables a los de las operaciones no cibernéticas que alcanzan el nivel de uso de la fuerza, lo cual debe analizarse contemplando ciertos parámetros establecidos por el mismo instrumento: La severidad, inmediatez, causalidad, el carácter invasivo, las consecuencias, el involucramiento militar y del Estado, y la legalidad del acto (Manual de Tallin 2.0, 2017, Regla 69).

Frente a la idea de que una operación cibernética, definida por al Manual de Tallin como aquella por la cual se emplean recursos informáticos ofensivos para la consecución de objetivos (Schmitt y Vihul, 2017), pueda ser considerada –lo cual no ocurre en todos los casos- como un ataque armado por parte de un Estado, el Manual da lugar a que el Estado que sufre dicho acto se defienda mediante una legítima defensa (Manual de Tallin 2.0, 2017, Regla 71). Esta legítima defensa, deberá limitarse a los principios de necesidad y proporcionalidad. La necesidad refiere a que la únicamente deberá utilizarse el uso de la fuerza como defensa cuando esta sea la acción que repele de manera más eficiente el ataque, mientras que la proporcionalidad refiere a cuál será el límite de uso de la fuerza que se admitirá para que dicha defensa sea legítima, lo cual sea determinará en comparación con la severidad del ataque en sí (Manual de Tallin 2.0, 2017, Regla 72).

Por otro lado, para que una defensa sea legítima, además de contemplarse los requisitos de necesidad y proporcionalidad de esta acción defensiva, el Manual establece que debe considerarse la inminencia e inmediatez del ataque, lo cual refiere a casos en los cuales el ataque ya haya ocurrido, sin permitir defensas

anticipatorias ni la posibilidad de que el Estado víctima pueda buscar una solución alternativa (regla 15 párr.3 1.0 y 73 2.0).

Una de las principales consecuencias que refleja el análisis del grupo de expertos, al desarrollar ambas versiones del Manual de Tallin, se da al aplicar de manera continua y sin excepción los principios del derecho internacional público a las actividades ocurridas en el ciberespacio (Pipyros et al., 2018).

En los próximos capítulos del presente trabajo se profundizan los términos mencionados anteriormente.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo 3: El Quinto Dominio de Combate

Los cuatro escenarios tradicionales

Históricamente, la noción de la guerra se ha forjado como una actividad violenta que tenía como objetivo continuar de manera forzada una postura política, obligando a determinadas personas o comunidades a adoptar una determinada ética prevaleciente, que coincidía con los intereses de quien perpetraba tal acto (Keegan, 1993). Los problemas que pueden llevar a conflictos internos y externos entre Estados, pueden variar tanto como varían las culturas y culturas en el mundo, tal como lo establece Thauby García (1996):

> ...tendencias desestabilizadoras como el crecimiento poblacional y la inmigración; lacreciente brecha entre los países que t ienen riqu eza, tecnologí y conocimiento y los que no los tienen; el co lapso económico de los países mal administrados o con gobiernos corruptos; el odio racial, religioso o nacionalista, y la influencia desestabilizadora d organizaciones no gubernamentales que promueven causas o intereses de grupos reducidos, pero económica o políticamente poderosos, tienden a conformar un panorama confuso en el cual pueden preverse conflictos armados internos, interestatales y mixtos, de naturalezas muy variadas (p.374).

Nuño Luco (2003) brinda una introducción a la noción histórica de la guerra de la siguiente manera:

> La guerra es un fenómeno social y como tal se asocia inevitablemente a la historia de la especie humana sobre la faz del planeta. Siendo así, se sujetó en sus orígenes sólo a la ley del más fuerte, el que con frecuencia se conducía en la más absoluta barbarie y sin compasión alguna por los vencidos. Sin embargo, producto de su constante evolución, la protección del hombre contra los males causados por la guerra no es una idea nueva, y ya en la antigüedad fueron varios los pensadores que condenaron los métodos bárbaros de hacerla. Más aún, desde los ya lejanos inicios del Derecho Internacional encontramos que el tema de la guerra y de los estragos que ésta causa aparece como un elemento de fundamental importancia para los precursores de esta nueva rama del Derecho (p.201).

A lo largo de los años se han forjado un alto número de enfrentamientos entre Naciones, los cuales han tenido lugar a través de determinados escenarios de combate. Suele hablarse de escenario o dominio, en términos de conflictos bélicos, al espacio físico donde ocurre la confrontación. En esta línea de definción, la tierra es uno de los escenarios o dominios tradicionales de batalla, y ofrece la oportunidad de ocupar terreno físico del adversario y excluirlo de él, así como controlar a las poblaciones del Estado atacado (Johnson, 2018).

A través del terreno, las fuerzas adversarias logran avanzar sobre el campo enemigo tomando espacio, lo cual es a su vez visible para la población del Estado invadido, con importantes consecuencias psicológicas en dichas personas, quienes son atacadas indirectamente a través del terror y la desesperación, al ver los destrozos de cerca, y a través de la búsqueda desaforada por huir de la situación. Estos ataques de desesperación, que podrían ser considerados parte de una "guerra psicológica", pueden ser cruciales en un enfrentamiento bélico y hasta ser más efectivos que otros tipos de ataque (Sameen, 2019).

El segundo dominio tradicional de combate es el marítimo o naval, a través del cual las fuerzas de un Estado conducen sus operaciones a través del agua, caracterizándose estas por tener mayor despliegue pero menor velocidad de avance. (Callender, 2018). Considerando que el planeta Tierra cuenta con un porcentaje dominante de agua, la cual representa una fuente inmensurable de recursos comerciales y estratégicos en múltiples sentidos que tienen como consecuencia grandes beneficios para los Estados (US Army, 2020), resulta fácil entender por qué las naciones no solo utilizan las vías marítimas como campo de batalla sino que también se esmeran por contar con fuerzas navales que puedan proteger estos espacios y dar continuidad a dichos beneficios.

El tercer dominio de combate es el aéreo, que refiere a la utilización del aire como vía para el acaecimiento de operaciones ofensivas y defensivas, que a su vez los Estados se encargan de controlarlo no solo en tiempos de conflicto, sino también en tiempos de paz a través de la vigilancia y el control sobre la circulación de aeronaves (Muñoz Castresana, 1996). Con el aprendizaje de la Primera Guerra Mundial, el uso de aeronaves otorgó una alternativa para evitar parcialmente el combate cuerpo a cuerpo, y de esta manera reducir la cantidad de bajas en la población civil, y permitiendo alcanzar objetivos precisos del Estado rival (Krause, 2015).

El cuarto escenario de combate es el espacial, que suele ser conocido como aquel donde se ejercen las operaciones nucleares. Surgidas desde finales de la Segunda Guerra Mundial, y con una capacidad de destrucción inmensa, las armas nucleares otorgan no solo una ventaja evidente en el plano de combate sino que además brinda al Estado poseedor de estas una posición dominante frente a sus adversarios, lo cual a

su vez ha tenido un desencadenado desarrollo militar, político y económico entorno a estas (de Salazar Serantes, 2004). La amenaza del uso del dominio espacial a través de las armas nucleares, suele tener como principal funcionalidad la coerción contra otro Estado. De esta manera, Ven Bruusgaard (2021) analiza el uso de este dominio por parte de las fuerzas rusas y explica lo siguiente:

> A nuclear threat could be used to manipulate the adversary, as the risk of a horrific nuclear war would influence its behaviour, given the unprecedented 'threat value' of nuclear weapons. Nuclear weapons offered novel tools for deterring conventional aggression and for influencing the course of war. [Una amenaza nuclear podría utilizarse para manipular al adversario, ya que el riesgo de una horrible guerra nuclear influiría en su comportamiento, dado el "valor de amenaza" sin precedentes de las armas nucleares. Las armas nucleares ofrecían nuevas herramientas para disuadir la agresión convencional y para influir en el curso de la guerra] (p.8).

El quinto dominio

De igual manera que la inteligencia artificial se ha mostrado en múltiples oportunidades como vencedora de humanos para la realización de actividades que son parte de la cotidianeidad, esta tecnología se ha extendido también al plano militar, sea a través tanto de sistemas autónomos que tienen correlatividad con el campo físico de combate, como desde sistemas tecnológicos de inteligencia (CCDCOE, 2021). A esto, se le suma la alta cantidad de actividades sociales, políticas, económicas y militares que dependen del ciberespacio, sea a través del Internet u otras tecnologías, lo cual da lugar a una gran puerta de acceso para la ocasión de daños a las capacidades de un Estado (Anderson, 2016).

Al analizar las nuevas innovaciones en materia tecnológica, y, especialmente, acerca de la velocidad de propagación de la información en la actualidad, Deptula (2015) establece:

> Cada día aparecen avances importantes en telecomunicaciones, sensores, almacenamiento de datos y potencia de procesamiento. Como resultado, el ciclo de selección de blancos ha pasado desde meses hasta semanas, días, y minutos; y desde múltiples aviones, especializados y separados asignados a comandantes separados, hasta "encontrar, fijar y terminar" desde una aeronave en minutos (p.55).

Estos avances tecnológicos que generan una nueva vía de ataque no son utilizados de igual manera por los Estados enfrentados, sea por falta de conocimiento, recursos o mismo por diferencias en la estrategia de ataque. Esto hace que no exista una igualdad de condiciones tecnológicas para las partes que se enfrentan en un combate, lo cual resulta semejante a los enfrentamientos en otros escenarios: Existen Estados con ventaja técnica. Por otro lado, la aparición de nuevas herramientas de combate, como son los drones, generan nuevos desafíos operacionales que implican a las Fuerzas militares el uso de una mente abierta y flexible (Pérez Aquino, 2017).

Kasapoğlu (2015) analiza las posibilidades que otorga la tecnología a este plano militar considerando a este nuevo dominio como una revolución:

> Within this framework, it could be argued that cyber warfare should be considered as the next – or the current – Revolution in Military Affairs. In this regard, operating advanced battle networks to detect, identify, and track targets and managing intelligence-surveillance reconnaissance (ISR) systems necessitate access to orbital and cyber dimensions of the global commons. As a result, the cyber arms race has already brought these dimensions to the forefront through counter-network attacks, anti-satellite systems, and directed-energy weapons systems. [Dentro de este marco, podría afirmarse que la ciberguerra debería considerarse como la próxima -o la actual- revolución en los asuntos militares. En este sentido, el funcionamiento de las redes de combate avanzadas para detectar, identificar y rastrear objetivos y la gestión de los sistemas de inteligencia, vigilancia y reconocimiento (ISR) requieren el acceso a las dimensiones orbitales y cibernéticas del patrimonio mundial. En consecuencia, la carrera armamentística cibernética ya ha puesto en primer plano estas dimensiones mediante ataques contra la red, sistemas antisatélites y sistemas de armas de energía dirigida] (p.4).

Por lo expuesto, hoy el ámbito cibernético da lugar a un nuevo campo de operaciones militares, lo que en otras palabras se conoce como un quinto dominio de combate (Eissa et al., 2012). Contemplando la cantidad de operaciones cibernéticas que tienen protagonismo hoy en los ámbitos militares de las naciones, a través de una integración de los sistemas tecnológicos a los de combate tradicional –tierra, aire, mar y espacio-, los Estados se ven ante la necesidad de desarrollar nuevas formas de incoporar técnicas ofensivas y defensivas de combate a través del uso de la tecnología (Dougherty, 2021).

Otra de las situaciones presentes en este discurso, se da frente a la posibilidad de ataques a través de más de un escenario de comate, lo que las fuerzas armadas de Estados Unidos han denominado como “operaciones de multidominio”, y que refiere a la optimización de los campos de combate a través de diversas técnicas que son capaces de integrar todos los dominios posibles (De Leon, 2021). Estas actividades desarrolladas, en conflictos bélicos y que implican más de un dominio de combate, no es algo novedoso, y ha resultado relevador durante la Segunda Guerra Mundial, donde los ataques simultaneos a través de diversos escenarios integrados han sido algo regular (Carafano, 2018).

Los acontecimientos de las últimas décadas, entre las que se encuentran las operaciones en Estonia, Georgia, Kyrguistan, Irán, ya mencionadas, así como la anexión de Krimea, entre otras, ponen de manifiesto que resulta indispensable contar con fuerzas militares dedicadas a responder frente a ataques de multidominios, debido a un mundo avanzado donde los ataques pueden provenir también de actores no estatales, y con grandes capacidades de combate (Jones y Diaz de Leon, 2020). Además, las Fuerzas de cada uno de los Estados debe contar con un entrenamiento integrador, equilibrado y distribuido que permita a este lograr capacidades de respuesta frente a ataques originados en todos los escenarios de combate, focalizándose en la posibilidad que tiene la tecnología de generar una integración entre los dominios y producir ataques evolucionados (Benitez, 2016).

Como conclusión de lo narrado en el presente capítulo, en la actualidad se encuentra instalado un quinto dominio de combate, que se extiende a los ya existentes tierra, mar, aire y espacio. Este quinto escenario, el ciberespacio, posibilita la integración y mejora de los ya existentes, así como crea nuevas vías de ataque que son facilitadas por la extrema dependencia que cuenta la población mundial actual en las nuevas tecnologías, las que pueden ser vulneradas por un enemigo, o mismo utilizar estas para el acaecimiento de diversos perjuicios. En esta línea, los Estados buscan la manera de reducir el impacto de los ciberataques los sistemas tecnológicos de su país, sea en los sistemas militares o que hacen al bienestar de la población, asumiendo que ocurrirán debido al alto porcentaje de probabilidad de ocurrencia de estos.

Por otro lado, la utilización de la tecnología en los ya existentes escenarios tradicionales de combate, ha brindado grandes innovaciones que se traducen en un superior aprovechamiento de las armas existentes, que presupone además la integración entre los diversos escenarios de combate generando la posibilidad de originar ataques de multidominio, esto es, producidos a través de varios escenarios en simultáneo. Esto tiene como consecuencia la necesidad de las Fuerzas Estatales de mejorar sus capacidades de inteligencia militar, entrenando a sus soldados para un desempeño que permita la integración de la tecnología a sus actividades, y contando con estrategias que contemplen un ataque integral mediante la conjunción de dominios.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo 4: La Intervención Cibernética

Violación al principio de las Naciones Unidas

Tal como se desprende de de una interpretación armónica entre la Carta de las Naciones Unidas y la Convención de Ginebra, en conjunto con las Resoluciones de la Asamblea General, la jurisprudencia de la Corte Internacional de Justicia y de la Corte Penal Internacional, así como de otros medios de interpretación complementarios como lo es el Manual de Tallin, una intervención en los asuntos internos de un Estado, que cumpla con ciertos parámetros de severidad, representaría una agresión y, por ende, una violación a la soberanía de otro Estado a través del uso de la fuerza, lo cual podría justificar una legítima defensa armada por parte del Estado víctima de dicha intervención.

Una vez contemplada la posibilidad de una legítima defensa ante una intervención que viole el principio de soberanía de un Estado sobre sus asuntos internos, cabe dilucidar ahora qué clases de actividades desarrolladas en el ciberespacio podrían influir efectivamente en los asuntos de otro Estado, por lo tanto ser consideradas intervenciones a la luz de la Carta de las Naciones Unidas.

Considerando que la intervención, según la mencionada Resolución 2131 de la Asamblea General de las Naciones Unidas, existe ante cualquier injerencia o amenaza contra los elementos políticos, económicos y culturales de un Estado, cualquier actividad cibernética que perjudique o altere el curso natural de dichos elementos, independientemente que se haya realizado mediante el uso de la fuerza por parte de otro Estado, sería considerada una intervención (Shamsi et al., 2016).

En esta línea, resulta menester la aclaración de que no toda intervención conlleva la posibilidad de una legítima defensa armada por parte del Estado atacado, sin perjuicio de la existencia de una violación al derecho internacional público, debido a que el mero hecho de una violación legal no amerita que el uso de la fuerza armada sea la vía necesaria y proporcional para repeler dicho ataque, y por lo tanto, la legitimidad de una defensa armada sería una cuestión que luego se analizará en el Capítulo 6 del presente trabajo.

Al contar hoy en día con un alto traslado del mundo físico al virtual o cibernético, donde la mayoría de las actividades cotidianas se realizan a través de Internet y donde la mayoría de los Estados ejercen sus actividades gubernamentales y proveen los servicios a la población a través de tecnologías de la información, existe una multiplicidad de formas que pueden tener las intervenciones cibernéticas (Buchan, 2012), por lo que cada caso deberá analizarse particularmente a la luz de las consecuencias que puedan tener estas actividades en las capacidades soberanas de un Estado.

Si bien el ciberespacio ha dado lugar a una vía para el acaecimiento de ataques dirigidos contra determinados sistemas, que podrían provocar daños físicos y concretos a gran escala, el objetivo del presente Capítulo es analizar cuáles son las diversas formas de operaciones cibernéticas o ciberataques que pueden darse en el marco de una intervención, cuáles podrían ser las consecuencias de dichos actos en el Estado que es víctima de ellos, y cuáles de estos no producen efectos de manera tradicional y directa –como podría ser un ciberataque que produzca un accidente aéreo con víctimas fatales-, sino que afectan a la estabilidad de un país desde sus raíces estructurales.

Sobre la posibilidad de generar daños concretos a través de armas cibernéticas, el Grupo de Expertos de la OTAN (2013) brindó una defínción sobre la idea de ciber armas:

> For the purposes of this Manual, cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack (Rule 30). The term means of cyber warfare encompasses both cyber weapons and cyber weapon systems. A weapon is generally understood as that aspect of the system used to cause damage or destruction to objects or injury or death to persons. Cyber means of warfare therefore include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack (Rule 30).
>
> [A los efectos del presente Manual, las ciberarmas son medios cibernéticos de guerra que, por su diseño, uso o intención de uso, son capaces de causar (i) lesiones o muerte a personas; o (ii) daños o destrucción de objetos, es decir, causar las consecuencias requeridas para calificar una operación cibernética como un ataque (Regla 30). El término medios de guerra cibernética abarca tanto las ciberarmas como los sistemas de armas cibernéticas. Un arma se entiende generalmente como el aspecto del sistema utilizado para causar daños o destrucción a objetos o lesiones o muerte a personas. Los medios de guerra cibernéticos incluyen, por tanto, cualquier dispositivo, material, instrumento, mecanismo, equipo o software cibernético utilizado, diseñado o

> destinado a ser utilizado para llevar a cabo un ciberataque (Regla 30).]
> (p. 141-142).

Como contraposición a las ciberarmas pero aún dentro de la categoría de operaciones cibernéticas, existen ataques cibernéticos que se dan a través de la influencia masiva, el lavado de activos, la creación de falsas noticias y otros campos de acción, que si bien no producen daños físicos a las infraestructuras de un Estado y pueden quedar excluidas de la categoría de ciberarmas, tienen la capacidad de desestabilizar tanto a un gobierno como al bienestar de la población a través del poder y la intimidación (Duić et al., 2017).

Clases de intervenciones cibernéticas

Para la categorización y discriminación de las operaciones cibernéticas que podrían enmarcarse como una intervención sobre los asuntos internos de otro Estado, podría utilizarse como punto de partida los posibles y diversos ámbitos en los que se puede dañar o afectar directa o indirectamente a un Estado -los cuales han sido desarrolladas anteriormente en el Capítulo 2 del presente trabajo como tipos de daño-: El ámbito físico, económico, psicológico, reputacional y social (Agrafiotis et al., 2018).

Si bien al estar configurada la intervención a los fines del artículo 2.7 de la Carta de las Naciones Unidas ya se lograría acreditar un daño al derecho internacional público propio del Estado atacado, vinculado directamente a la soberanía de aquel sobre sus asuntos internos, en los siguientes párrafos se profundizará las diferentes herramientas que pueden ser utilizadas para realizar la operación cibernética original que da lugar a dicha intervención, las cuales se diferenciarán de acuerdo a sus objetivos, consecuencias y daños.

La intervención cibernética con consecuencias físicas

Las operaciones cibernéticas que tienen como objetivo un daño dentro del plano físico, representan un argumento sólido para la consideración de que existe un correlato real entre el ciberespacio y el mundo físico, que a priori parecían ser mundos completamente ajenos el uno del otro y con el paso del tiempo se ha demostrado que no. Este primer grupo de daños refieren generalmente a aquellos ciberataques tradicionales que suelen afectar los sistemas tecnológicos de un adversario.

Al utilizarse el ciberespacio como vía para alcanzar su objetivo, los ciberataques con daños físicos suelen buscar impactar en el correcto funcionamiento de un sistema informático determinado, lo cual puede a su vez tener tan diversas como graves consecuencias en los objetos controlados por los sistemas afectados. Por ejemplo, un ciberataque al comando de control de un aeropuerto, puede tener como consecuencia el accidente de un avión produciendo víctimas fatales. La avanzada integración de la tecnología a la industria de la aviación, sumado a la gravedad de las consecuencias que puede tener un incidente cibernético en sus

sistemas, ha llevado a que durante los últimos años se lleven adelante nuevas herramientas de ciberseguridad dentro del rubro (Ukwandu et al., 2022).

De esta manera, la afectación cibernética se traslada a consecuencias físicas y concretas. Otro ejemplos, con menor o mayor gravedad, pueden ser: La afectación de semáforos que produce un alto número de accidentes viales y genera un alto tráfico en todas las avenidas principales de un país (Özarp et al., 2021); el corte de servicios estatales como el agua, la electricidad, el gas, entre otros, dejando a millones de personas con ausencia de estos (Choraś et al. 2016); la caída de páginas y servidores web con funcionalidades gubernamentales y privadas; la explosión de máquinas o dispositivos de manera provocada; la alteración del curso ordinario de vehículos inteligentes (Guan et al., 2022); entre un sinfín de otros casos en los cuales el ciberatacante puede intervenir y modificar estos sistemas, provocando daños muy diversos y que algunos pueden evaluarse con pérdidas económicas, mientras que otros derivan en víctimas fatales (Casson Moreno et al., 2018).

En estos últimos casos, donde el impacto tiene consecuencias físicas sobre las infraestructuras de un Estado particular, debe analizarse la presencia de infraestructuras críticas, o en otras palabras, operadores esenciales, afectados por el ciberataque perpetrado. Ya habiendo definido el significado de estas, un ataque que perjudica la normal operación de una entidad de semejantes características, perjudica gravemente al Estado por no poder dar continuidad a un servicio que resulta de vital importancia para la población, por lo que suele significar una herramienta de desestabilización por excelencia (UNOCT y CTED, 2018).

En caso de que un Estado provoque un daño fìsico grave sobre otro Estado, podría este acto inmiscuirse dentro de la categoría de agresión según el derecho internacional público, y, por ende, ser considerada una intervención sobre los asuntos internos de un Estado, donde la vía de la legítima defensa armada estará abierta si es posible considerar a dicho ataque uno armado, sea por su severidad u otros elementos que se mencionan en los Capítulos 2 y 6.

La intervención cibernética con consecuencias económicas

Para entender la segunda forma de intervención, resulta esencial considerar la importancia de la economía sobre la estructura y estabilidad de un Estado. En este punto, Tansini et al. (2003) define:

> La economía es la ciencia que se ocupa del estudio sistemático de las actitudes humanas orientadas a administrar los recursos, que son escasos, con el objetivo de producir bienes y servicios y distribuirlos de forma tal

> que se satisfagan las necesidades de los individuos, las que son ilimitadas (p.13).

En este orden de ideas, la economía, al buscar la satisfacción de necesidades a través de la producción y distribución de bienes y servicios, hace al bienestar de cada habitante y ello lleva a un bienestar social de la población (Diaz T., 2008). Sin perjuicio de ello, para considerar la importancia de la economía en virtud de los daños que pueden generarse a través de ella, se destaca también las estructuras del sistema impositivo o tributario, y del sistema bancario y financiero de un país. El primero remite a la competencia tributaria de un Estado, en otras palabras, a la facultad estatal de cobrar tributos a sus habitantes con el objeto de equilibrar las finanzas públicas, mantener la estructura del Estado e invertir dichos ingresos para el bienestar de la población (Altavilla, 2009).

Por otro lado, el sistema financiero es definido por Faure (2013) como:

> The financial system is a set of arrangements / conventions embracing the lending and borrowing of funds by non-financial economic units and the intermediation of this function by financial intermediaries in order to facilitate the transfer of funds, to create additional money when required, and to create markets in debt and equity instruments (and their derivates) so that the price and allocation of funds are determined efficiently. [El sistema financiero es un conjunto de acuerdos/convenios que abarcan el préstamo y el endeudamiento de fondos por parte de las unidades económicas no financieras y la intermediación de esta función por parte de los intermediarios financieros con el fin de facilitar la transferencia de fondos, crear dinero adicional cuando sea necesario y crear mercados de instrumentos de deuda y de acciones (y sus derivados) para que el precio y la asignación de los fondos se determinen de forma eficiente.] (p.8).

En correlación directa con el sistema financiero, el sistema bancario, ejercido a través de entidades legales autorizadas para ello, promueve el funcionamiento económico de un Estado, al proporcionar herramientas a los ciudadanos para utilizar su riqueza y facilitar el comercio, permitiendo una interacción entre el sector público y privado, y entre el sector privado de uso doméstico y el comercial, representando una pieza clave para el desarrollo y crecimiento de la economía (Douglas, 2008).

El Estado, como institución que regula la figura de los bancos, sus requisitos, derechos y obligaciones, y por ende, al sistema financiero y bancario en su integridad, tiene como objetivo controlar la actividad

bancaria para evitar potenciales crisis y actividades que puedan desestabilizar la continuidad del sistema y el bienestar de la población por todo lo mencionado anteriormente, lo cual realiza a través del desarrollo de políticas y normativas de diversos carácteres legales (Heimler, 2006).

En el caso de que un ciberataque perpetrado por un Estado hacia otro altere el normal funcionamiento del sistema económico de otro, a través de la afectación de los sistemas financieros o bancarios de este, se estaría interviniendo en sus asuntos internos y violando su soberanía. Un ejemplo claro de cómo podría afectarse este ámbito es el del ciber lavado de activos, en otras palabras, el blanqueo ilícito de capitales que circula a través del ciberespacio.

En virtud de lo dispuesto por la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2001), se tipifica de la siguiente manera el delito del blanqueo de capitales que sean producto de un delito:

> Artículo 6. Penalización del blanqueo del producto del delito
>
> 1. Cada Estado Parte adoptará, de conformidad con los principios fundamentales de su derecho interno, las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan intencionalmente:
>
> a) i) La conversión o la transferencia de bienes, a sabiendas de que esos bienes son producto del delito, con el propósito de ocultar o disimular el origen ilícito de los bienes o ayudar a cualquier persona involucrada en la comisión del delito determinante a eludir las consecuencias jurídicas de sus actos;
>
> ii) La ocultación o disimulación de la verdadera naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes o del legítimo derecho a éstos, a sabiendas de que dichos bienes son producto del delito;
>
> b) Con sujeción a los conceptos básicos de su ordenamiento jurídico:
>
> i) La adquisición, posesión o utilización de bienes, a sabiendas, en el momento de su recepción, de que son producto del delito;

ii) La participación en la comisión de cualesquiera de los delitos tipificados con arreglo al presente artículo, así como la asociación y la confabulación para cometerlos, el intento de cometerlos, y la ayuda, la incitación, la facilitación y el asesoramiento en aras de su comisión.

2. Para los fines de la aplicación o puesta en práctica del párrafo 1 del presente artículo:

a) Cada Estado Parte velará por aplicar el párrafo 1 del presente artículo a la gama más amplia posible de delitos determinantes;

b) Cada Estado Parte incluirá como delitos determinantes todos los delitos graves definidos en el artículo 2 de la presente Convención y los delitos tipificados con arreglo a los artículos 5, 8 y 23 de la presente Convención. Los Estados Parte cuya legislación establezca una lista de delitos determinantes incluirán entre éstos, como mínimo, una amplia gama de delitos relacionados con grupos delictivos organizados;

c) A los efectos del apartado b), los delitos determinantes incluirán los delitos cometidos tanto dentro como fuera de la jurisdicción del Estado Parte interesado. No obstante, los delitos cometidos fuera de la jurisdicción de un Estado Parte constituirán delito determinante siempre y cuando el acto correspondiente sea delito con arreglo al derecho interno del Estado en que se haya cometido y constituyese asimismo delito con arreglo al derecho interno del Estado Parte que aplique o ponga en práctica el presente artículo si el delito se hubiese cometido allí;

d) Cada Estado Parte proporcionará al Secretario General de las Naciones Unidas una copia de sus leyes destinadas a dar aplicación al presente artículo y de cualquier enmienda ulterior que se haga a tales leyes o una descripción de ésta;

e) Si así lo requieren los principios fundamentales del derecho interno de un Estado Parte, podrá disponerse que los delitos tipificados en el párrafo 1 del presente artículo no se aplicarán a las personas que hayan cometido el delito determinante;

> f) El conocimiento, la intención o la finalidad que se requieren como elemento de un delito tipificado en el párrafo 1 del presente artículo podrán inferirse de circunstancias fácticas objetivas (artículo 6).

El lavado de activos a través del ciberespacio, o ciber lavado, refiere al delito de blanqueo de capitales tradicional con la variante de que este es facilitado a través de este ya analizado quinto dominio, el cual permite nuevas metodologías de lavado de activos como lo son los pagos electrónicos y los sistemas de apuestas en línea (Uzal, 2013). El hecho de que la tecnología actual permite el intercambio de información de manera inmediata entre casi todos los Estados del mundo, especialmente otorgando la posibilidad de transferir dinero y otros activos fungibles a través de las plataformas digitales, ha dado lugar al uso constante de convenciones internacionales respecto de cómo debe interpretarse a la luz de la ley, hechos que involucran más de un Estado interviniente, y que, por ende, se tornan actividades transnacionales, lo cual, ya teniendo complicaciones cuando se encuentran dentro del marco de la ley, se convierten en una pesadilla al involucrar al lavado de activos (Filipkowski, 2008).

Una forma muy común en la que el lavado de activos tiene lugar, de manera recurrente y en el espacio cibernético, es a través de las páginas de apuestas en línea. El blanqueo de dinero obtenido a través del azar resulta una posibilidad concreta para los delincuentes, quienes logran ingresar al sistema bancario grandes sumas de dinero que, si no fuese por el argumento del azar, no hubieran podido justificar dichos montos. Las organizaciones de crimen transnacional organizado que se dedican a enmascarar estructuras de lavado de activos a través de estos sistemas de apuestas en línea, cobran un interés por circular el dinero a través de sus mecanismos de flujo de dinero, quienes generalmente a su vez se encuentran establecidas en Estados con baja o nula regulación financiera o bancaria.

Si bien el ciberespacio otorga mayor posibilidad de rastreo del dinero que las apuestas presenciales clandestinas con efectivo, estas organizaciones delictivas se encargan de falsificar el ingreso de dinero irreal a su plataforma a través de usuarios falsos que pierden su dinero en su plataforma. De esa manera, el casino en línea incrementa exponencialmente sus ingresos debido a un falso éxito, el cual se traduce en paralelo al ingreso de dinero ilegal que resulta producto de un delito. Una vez que la compañía logra acreditar una gran suma de dinero por parte de las ganancias de los usuarios falsos, ya cuenta con suficiente capital para que, quien pretende blanquear el capital, gane un juego de apuestas y obtenga una suma blanca de dinero, la cual se ingresa a su cuenta de manera legal.

La cuestión a dilucidar, luego de definir el crimen del lavado cibernético de capitales, es el de cómo puede un Estado intervenir en los asuntos económicos de otro a través de esta figura delictiva.

Como se mencionó anteriormente, los Estados son los encargados de regular el sistema bancario y financiero interno de cada uno de ellos, a través de la generación de leyes, resoluciones, reglamentos, así como cualquier otra especie de normativa o regla que tienda a normalizar la existencia y el ejercicio de las entidades u operaciones bancarias, siendo estas auditadas y controladas con el fin de observar, predecir, evitar y/o castigar cualquier intento de actividad ilícita, así como también evitando fraudes, crisis financieras u otras consecuencias que puedan derivar en perjuicios para los usuarios finales, la población en general e incluso para el propio gobierno.

Una de las vías por las cuales hoy las entidades de apuestas en línea logran lavar grandes cantidades de dinero y evadir diversos tipos de inspecciones, es a través de una cooperación estatal omisiva, que se da a través de la falta de observación en su sospechosa estructura ilícita. Por otro lado, la falta de regulación puede ser interpretada como una omisión dolosa, debido a los avanzados conocimientos que se cuentan hoy en día sobre estas nuevas formas de ciberdelincuencia.

Por lo tanto, en caso de que un Estado no cuente con regulación bancaria, financiera o sobre las organizaciones de apuestas en línea dentro de su propia jurisdicción, y que esta permita el blanqueo de capitales afectando a la estabilidad económica de otro Estado, sea por daños al sistema impositivo como al financiero y bancario, podría darse el caso de que esta situación constituya una agresión, intervención y violación a la soberanía internacional.

La intervención cibernética con consecuencias psicológicas, reputacionales y sociales

La siguiente clase de intervenciones, en este caso agrupadas por estar estrechamente relacionadas, reúne a aquellas que tienen consecuencias sobre aspectos psicológicos, reputacionales y sociales de la población del Estado atacado, lo que ocurre cuando un ciberataque, que puede tener diversas formas de presentación, impacta y logra tener consecuencias en la mente de los ciudadanos a través de la influencia, provocando cambios en su comportamiento y afectando su forma de pensar y/o ver algo. Esta situación, si bien a priori podría no significar una violación a la soberanía de un Estado, ya que lo que afecta es la mentalidad de los ciudadanos, sí deriva en afectaciones a la soberanía en cuanto a que suele estar conectada con fines desestabilizadores del gobierno, por ejemplo, a través de la publicación de documentos que dejan en evidencia una situación gubernamental que deja mal parado al Presidente de un país.

Un elemento que puede hacer al ataque psicológico o influenciador uno que supere en eficiencia a los que tienen consecuencias en el plano físico, es el del terror. El ciberataque que produce como principal consecuencia terror en una población civil, actividad conocida como ciberterrorismo, está prohibida por la Regla 36 de la Primera Versión y por la 98 de la Segunda del Manual de Tallin. Biller (2013) presenta una

amplia definición para entender el alcance del ciberterrorismo, incorporando la idea de ansiedad en la población, y asumiendo motivos políticos por parte del grupo que perpetra el acto:

> Premeditated, politically motivated computer network attacks perpetrated against noncombatant targets by subnational groups, designed to cause fear or anxiety in a civilian populance either by: a) inflicting, falsely appearing to inflict, or threatening to inflict, widespread damage to critical physical or informational infrastructure, national security related information systems, or critical economic systems; or b) causing, appearing to cause, or threatening to cause any type of severe physical damage or human casualties. [Ataques premeditados a redes informáticas con motivación política perpetrados contra objetivos no combatientes por grupos subnacionales, diseñados para causar miedo o ansiedad en una población civil, ya sea: a) infligiendo, aparentando falsamente infligir, o amenazando con infligir, daños generalizados a infraestructuras físicas o informáticas críticas, sistemas de información relacionados con la seguridad nacional, o sistemas económicos críticos; o b) causando, aparentando causar, o amenazando con causar cualquier tipo de daño físico grave o víctimas humanas.] (p.292).

Otro caso ejemplificador de la intervención psicológica, la cual se ve cotidianamente, es la que se da mediante la circulación masiva de falsas noticias, conocidas como fake news, las cuales tienden a generar una posición errónea sobre un tema particular, siendo estas diseñadas y creadas especialmente para afectar y hacer creer a los ciudadanos situaciones inexistentes. Si bien en la antiguedad la circulación de noticias era una actividad exclusiva para periodistas y medios de comunicación, en la actualidad existe una puerta abierta para que todo aquel que desee escribir una noticia, sea verdadera o falsa, pueda hacerlo, alcanzando grandes cantidades de lectores de manera inmediata, lo cual da lugar a una nueva amenaza, por un lado, y una gran oportunidad desestabilizadora, por el otro (Quintanilha et al., 2019).

En la actualidad existen Estados que apuestan a la elaboración de falsas noticias para desestabilizar a un gobierno adversario, a través de la búsqueda de reducción de imagen positiva de una determinada figura política, lo cual ha llevado a considerar estados de “desinformación” debido a que en determinados momentos de conflicto posiblemente la mayor cantidad de información que circula es falsa.

Otro ejemplo de influencia se dio a través de la afectación electoral, lo cual ha sucedido en el caso de Cambridge Analytica (Vercelli, 2018):

> Las investigaciones revelaron al público que Cambridge Analytica ofrecía a sus clientes el armado de campañas electorales sucias y el uso de datos personales de millones de usuarios de Facebook Inc. para diseñar campañas psicográficas. En particular, se denunciaba que Cambridge Analytica había utilizado estas herramientas en las elecciones norteamericanas de 2016 (a favor de Donald Trump) y que, en el mismo año, también las habían usado en el Reino Unido para apoyar el Brexit (p.2).

Como conclusión del presente Capítulo, existen diversas clases de operaciones cibernéticas que pueden generar daños en diferentes ámbitos de un Estado y ser considerados intervenciones a la luz de la Carta de las Naciones Unidas, así como también una agresión en virtud de las Resoluciones de la Asamblea General y la jurisprudencia de la Corte Internacional de Justicia, por representar una violación a la soberanía de un determinado Estado atacado.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo 5: El Problema de la Ciber Atribución

El principio de inocencia internacional

Luego de determinar qué tipos de actividades cibernéticas podrían ser catalogadas como una intervención, e incluso si esta intervención es considerada una agresión por su severidad y por violar la soberanía internacional, debe analizarse cuidadosamente que dicho ataque sea atribuido a los verdaderos responsables de este, así como considerar los riesgos existentes en caso de que dicha atribución se realice de manera incorrecta, y un Estado se defienda armadamente contra un Estado que no había iniciado el ataque.

En el derecho internacional público se conoce como "principio de inocencia" a aquel por el cual toda persona es inocente hasta que se demuestre lo contrario. Esto puede verse reflejado en el texto de la Declaración Universal de los Derechos Humanos (1948):

> Toda persona acusada de delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad, conforme a la ley y en juicio público en el que se le hayan asegurado todas las garantías necesarias para su defensa (artículo 11, primer párrafo).

Si bien este principio es aplicado a las personas humanas, quienes son poseedoras de los derechos humanos y, como contra cara del mismo tema, son los Estados quienes deben garantizar el cumplimiento de estos, los Estados cuentan con un principio de inocencia similar en el derecho internacional público, debiendo probarse la responsabilidad o culpabilidad de un Estado ante la presunción de cualquier acto ilícito perpetrado por este, previo a la asignación de una pena. A esta búsqueda de nexo causal entre un sujeto –sea una persona humana o un Estado- y el origen de un hecho específico, se lo conoce como atribución de la responsabilidad (Fincham y Jaspars, 1980).

Este principio de inocencia debe ser aplicado antes de la activación de la legítima defensa del artículo 51 de la Carta de las Naciones Unidas, donde un Estado debe tener la seguridad absoluta de que un determinado Estado lo ha atacado -y no otro- para luego defenderse proporcionalmente. En caso de que un Estado se defienda contraatacando a un Estado inocente del presunto ataque inicial, el Estado que presume la legítima defensa se convertirá en un violador de la normativa internacional, atacando a un Estado inocente, quien a su vez podrá activar la legítima defensa frente a dicho ataque.

Responsabilidad por hechos internacionalmente ilícitos

La Asamblea de las Naciones Unidas (2001) expidió una Resolución destinada al tratamiento de la responsabilidad del estado por hechos internacionalmente ilícitos, y estableció en ella que:

> 1. Se considerará hecho del Estado según el derecho internacional el comportamiento de todo órgano del Estado, ya sea que ejerza funciones legislativas, ejecutivas, judiciales o de otra índole, cualquiera que sea su posición en la organización del Estado y tanto si pertenece al gobierno central como a una división territorial del Estado.
>
> 2. Se entenderá que órgano incluye toda persona o entidad que tenga esa condición según el derecho interno del Estado (Artículo 4).

En el caso judicial internacional de Bosnia y Herzegovina contra Serbia y Montenegro del año 2007, relativo a la aplicación de la Convención para la Prevención y Sanción del Castigo del Crimen de Genocidio, la Corte Internacional de Justicia estableció que:

> Genocide will be considered as attributable to a State if and to the extent that the physical acts constitutive of genocide that have been committed by organs or persons other than the State's own agents were carried out, wholly or in part, on the instructions or directions of the State, or under its effective control. [Se considerará que el genocidio es atribuible a un Estado si, y en la medida en que, los actos físicos constitutivos de genocidio que hayan sido cometidos por órganos o personas distintas de los propios agentes del Estado se hayan llevado a cabo, total o parcialmente, siguiendo las instrucciones o direcciones del Estado, o bajo su control efectivo.] (párr.401).

Como se arroja del mencionado fallo, y contemplando el mencionado artículo 4 de la Resolución de Naciones Unidas del 2002, la atribución de la responsabilidad internacional a un Estado debe analizarse entorno a que los actos perpetrados sean direccionados por un órgano estatal, lo que podría darse, por ejemplo, mediante una orden del Presidente o el Parlamento, dentro del marco del control efectivo del Estado sobre dichos órganos.

A esto se le suma la posibilidad de que un hecho particular, al cual se le pretendrá atribuir la responsabilidad de un Estado, pueda ser originado tanto mediante la comisión de una acción, como por la omisión de esta. En esta línea, Milanovic (2020) define ambas clases de acciones de la siguiente manera:

> ...an inquiry into special rules of attribution of con-duct must be rigorous in defining the conduct being attributed. That conduct can consist either of action (commission) or inaction (omission). An action is capable of breaching a negative obligation, that is, one that requires a State to refrain from a certain action. An omission can breach a positive obliga-tion, that is, one that requires a State to perform a certain action. This is a fairly elementary point, but international case law is replete with examples of courts and other institutions not clearly distinguishing between positive and negative obligations, and consequentially between the attributions of omis-sions or actions. [...una investigación sobre las normas especiales de atribución de conductas debe ser rigurosa en la definición de la conducta que se atribuye. Esa conducta puede consistir en una acción (comisión) o en una inacción (omisión). Una acción puede infringir una obligación negativa, es decir, una que exige que un Estado se abstenga de realizar una determinada acción. Una omisión puede violar una obligación positiva, es decir, la que requiere que un Estado realice una determinada acción. Se trata de un punto bastante elemental, pero la jurisprudencia internacional está repleta de ejemplos de tribunales y otras instituciones que no distinguen claramente entre obligaciones positivas y negativas y, en consecuencia, entre la atribución de omisiones o acciones.] (p.315).

Por otro lado, resulta menester la aclaración de que los daños que perpetra un Estado a otro pueden, sin perjuicio de ser realizados tanto mediante una comisión como mediante una omisión, ser realizados tanto mediante un accionar lícito como uno ilícito. En otras palabras, Los Estados operan diariamente tomando decisiones que pueden afectar a otros Estados, lo cual no por dicha razón los convierte en violadores del derecho internacional público. Por ende, no por el hecho de existir daño, existe un hecho ilícito que lo provoca. Sin embargo, todo hecho ilícito debe penarse, sin perjuicio del análisis posterior de los daños cometidos por este (Aizenstatd Leistenschneider, 2012).

En este mismo orden de ideas, la Comisión de Derecho Internacional de las Naciones Unidas (2001) se expresó sobre la posibilidad de que un hecho lícito puede generar daños en otro Estado:

> Pueden existir casos en que los Estados incurran en obligaciones de indemnizar por las consecuencias perjudiciales de un comportamiento que no está prohibido, y que incluso puede estar expresamente permitido, por el derecho internacional (por ejemplo, la indemnización por bienes debidamente expropiados con fines de utilidad pública). También puede haber casos en que un Estado esté obligado a restablecer el statu quo ante después de que se ha llevado a cabo alguna actividad lícita. Estos requisitos de indemnización o de restauración pueden entrañar obligaciones primarias: lo que entrañaría la responsabilidad internacional del Estado de que se trate sería no haber pagado la indemnización o no haber restablecido el statu quo. En consecuencia, a los efectos de los presentes artículos, la responsabilidad internacional resulta exclusivamente de un hecho ilícito contrario al derecho internacional (p.32).

La dificultad de atribuir responsabilidad en el ciberespacio

Al buscar determinar la atribución de la responsabilidad de un Estado sobre un hecho que tiene lugar en el ciberespacio, se realiza una tarea conocida como ciber atribución, a través de la cual los Estados deben considerar varios aspectos informáticos, políticos y legales de la operación cibernética cuya responsabilidad se pretende atribuir, la cual representa grandes desafíos de inteligencia técnica y estratégica (Derian-Toth et al., 2021), considerando especialmente que las confrontaciones en el ciberespacio suelen implicar anonimato por parte de la parte atacante (Feliu Ortega, 2012).

Sobre esta dificultad, el Grupo de Expertos de la OTAN (2013) brindó una herramienta legal para determinar si un ataque cibernético perpetrado por las infraestructuras tecnológicas de un Estado, son suficientes o no para dilucidar la responsabilidad del Estado atacante:

> The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State, but is an indication that the State in question is associated with the operation.

> [Regla 7 - Ciberoperaciones lanzadas desde una ciberinfraestructura gubernamental
>
> El mero hecho de que una operación cibernética haya sido lanzada o se origine de otro modo a partir de una ciberinfraestructura gubernamental no es prueba suficiente para atribuir la operación a ese Estado, pero es un indicio de que el Estado en cuestión está asociado a la operación.] (Regla 7).

La Asamblea de las Naciones Unidas (2015) fomentó la utilización de recursos y esfuerzos destinados para descifrar el verdadero origen del hecho:

> ...en el caso de incidentes relacionados con las TIC, los Estados deberían tener en cuenta toda la información pertinente, incluido el contexto más amplio en el que se haya producido el hecho, los problemas que plantea la atribución en el entorno de estas tecnologías, así como la naturaleza y el alcance de las consecuencias (párr.13.b).

Como los Estados deben ejercitar sus fuerzas cibernéticas para mitigar o repeler cualquier intento de ataque a través de este quinto dominio de combate, independientemente de su origen y causa, es menester resaltar que los ataques pueden producirse además por actores no estatales, es decir, por atacantes individuales o grupos organizados motivados por el daño o perjuicio al Estado que atacan. Sobre esta noción, Eg Tan (2018) menciona:

> The cyber realm is organised differently; other than bringing concerns to both military and civilian populations, it is accessed by many users on different platforms, and most importantly, there is the presence of non-state actors. Cyberspace deterrence is thus not limited to relationships between states, but has expanded to incorporate the malicious activity of non-state actors as well. With the proliferation of computers and computing knowledge, cyberattacks can be undertaken by almost anyone or any group, with or without state affiliation. [El ciberespacio está organizado de forma diferente; además de preocupar a la población militar y civil, a él acceden muchos usuarios en diferentes plataformas y, lo que es más importante, existe la presencia de actores no estatales. Por tanto, la disuasión en el ciberespacio no se limita a las relaciones entre

> Estados, sino que se ha ampliado para incorporar también la actividad maliciosa de actores no estatales. Con la proliferación de ordenadores y conocimientos informáticos, los ciberataques pueden ser realizados por casi cualquier persona o grupo, con o sin afiliación estatal.] (p.1).

Frente a esta posibilidad de los Estados de recibir ataques provenientes de una multiplicidad de atacantes, la atribución de responsabilidad se dificulta aún más. Esta situación, considerada como "guerra híbrida", refiere a la posibilidad de atacar a un Estado tanto mediante el uso de fuerzas convencionales de combate como de otras irregulares, entre las que se encuentran las guerrillas, rebeliones contra la autoridad y los terroristas (Wither, 2020). Los ataques pertenecientes al entorno híbrido mencionado, suelen estar caracterizados por estar coordinados para afectar y desastabilizar a un Estado conociendo sus vulnerabilidades internas, usando una alta gama de herramientas para obtener sus objetivos y dificultando la detección de los responsables verdaderos (Terrados, 2019).

La responsabilidad de los ciberataques deben atribuirse con altos grados de exactitud antes de responder mediante la figura de la legítima defensa de las Naciones Unidas, y aquí se encuentra uno de los mayores desafíos de la acción defensiva en el marco de la ley. Para poder demostrar que una defensa es legítima, debe poder demostrarse sin duda alguna que el ciberataque que ha violado el principio de la no intervención, ha sido originado por otro Estado. Sumado a la dificultad de la atribución de la responsabilidad en contextos de combate tradicional, junto con la posibilidad de que se produzcan ataques de guerra híbrida con mayor dificultad de atribución del principal responsable, Anderson (2016) brinda una diferenciación sobre cuán difícil es atribuir la responsabilidad de un ataque proveniente de un escenario tradicional, frente a uno del quinto dominio:

> Enforcing cyberspace policy is not the same as enforcing rules in the other four domains—land, air, sea, and space. For example, when an unauthorized ship enters a sovereign nation's waters, it is detected, the responsible agency takes action, and attribution is quickly determined. The same actions can occur in air and space. The same is not necessarily true for cyberspace, at least not today. [Aplicar la política del ciberespacio no es lo mismo que aplicar las normas en los otros cuatro dominios: tierra, aire, mar y espacio. Por ejemplo, cuando un barco no autorizado entra en aguas de una nación soberana, se detecta, el organismo responsable toma medidas y se determina rápidamente la atribución. Las mismas acciones pueden ocurrir en el aire y el espacio.

> Lo mismo no es necesariamente cierto para el ciberespacio, al menos no hoy] (p.72).

La manera en la cual fue construido el ciberespacio pareciera favorecer la dificultad de la atribución de la responsabilidad de quien perpetra el ciberataque, ya que el Estado atacado debe ubicar la locación del potencial agresor, lo cual generalmente suele ser el primer desafío ante el que se enfrenta el Estado atacado. Por otro lado, existe una asimetría de recursos entre los daños que pueden generarse y la defensa necesaria para evitarlo o atribuir dicha responsabilidad, y las herramientas destinadas a causarlo, ya que en la actualidad los dispositivos tecnológicos utilizados para estos fines ilícitos son baratos (Kozlowski, 2014).

En virtud de lo expuesto, los ataques informáticos que desestabilizan a un Estado pueden ser generados por una multiplicidad de actores, y a su vez, tomar una multiplicidad de formas y vías para lograr sus objetivos. Los Estados deben atribuir correctamente la responsabilidad del hecho ilícito antes de dar lugar a la legítima defensa del artículo 51 de la Carta de las Naciones Unidas, lo cual implica grandes desafíos de diversas índoles para el Estado atacado.

En caso de que un Estado se defienda contraatacando a un Estado inocente, por presumir erroneamente que este había originado un ataque, dicha defensa será considerada un hecho ilícito a la luz del derecho internacional público y permitirá al Estado atacado injustamente una defensa legítima para repeler dicho ataque. Un mal entendimiento de la normativa internacional de la legítima defensa puede tornar culpable a un Estado que en principio había sido atacado, y por lo tanto, la acción defensiva del último Estado atacado se convertirá en una acción legal respaldada por las Naciones Unidas.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo 6: El Problema de la Legítima Defensa Armada

La intervención cibernética como ataque armado

La legítima defensa es aquella por la cual el derecho internacional público perimte a un Estado defenderse frente a un inminente ataque o nuevas amenazas (Bethlehem, 2012). Si bien la defensa legítima frente a un hecho internacionalmente ilícito, proviene del derecho consuetudinario histórico, en el presente Capítulo se analizará el tema de acuerdo con lo dispuesto por la Carta de las Naciones Unidas, la cual representa una expresa excepción a la prohibición del uso de la fuerza:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales [...] (artículo 51).

El primer criterio que debe tenerse en cuenta a la hora de dilucidar si un hecho internacionalmente ilícito puede abrir la vía de una legítima defensa por parte del Estado atacado, a la luz de la Carta de las Naciones Unidas, se da a través de la definición de "ataque armado", el cual, ya descripto en el Capítulo 2 del presente trabajo, se encuentra expreso en el artículo 51 de la Carta y resulta la figura esencial en este asunto.

Al deber interpretar el ataque como uno "armado", ya se ha analizado la vinculación entre este concepto y el de "agresión", los cuales refieren al control efectivo sobre la acción política o militar de un Estado a través de fuerzas militares o grupos enviados para ello, y cuando su gravedad y escala constituya una violación a la Carta de las Naciones Unidas. Por otro lado, si bien el uso de la fuerza armada resulta en una vía esencial para que se produzcan dichas figuras legales, las enmiendas de Kampala (2010) han establecido que estos actos pueden tener otra naturaleza, siempre y cuando se contemple una manifiesta incompatibilidad con la Carta de las Naciones Unidas.

Mediante la Opinión Consultiva de 1996 relativa a la legalidad de la amenaza del uso de armas nucleares, la Corte Internacional de Justicia (1996) se expresó estableciendo que tanto la violación del uso de la fuerza como su legítima defensa armada, no cuentan con vinculación a algun tipo de arma en particular:

> ...This prohibition of the use of force is to be considered in the light of other relevant provisions of the Charter. In Article 51, the Charter recognizes the inherent right of individual or collective self-defence if an

> armed attack occurs. A further lawful use of force is envisaged in Article 42, whereby the Security Council may take military enforcement measures in conformity with Chapter VI1 of the Charter.
>
> 39. These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter.
>
> [...Esta prohibición del uso de la fuerza debe considerarse a la luz de otras disposiciones pertinentes de la Carta. En el artículo 51, la Carta reconoce el derecho inherente de legítima defensa individual o colectiva en caso de ataque armado. Otro uso legítimo de la fuerza se contempla en el artículo 42, según el cual el Consejo de Seguridad puede adoptar medidas militares coercitivas de conformidad con el capítulo VI1 de la Carta.
>
> 39. Estas disposiciones no se refieren a armas específicas. Se aplican a cualquier uso de la fuerza, independientemente de las armas empleadas. La Carta no prohíbe ni permite expresamente el uso de ningún arma específica, incluidas las armas nucleares. Un arma que ya es ilícita per se, ya sea por tratado o por costumbre, no se convierte en lícita por el hecho de que se utilice para un fin legítimo en virtud de la Carta.] (párr. 38-39).

Sumado a esto, el Grupo de Expertos de la OTAN adhirió a la posición de la Corte Internacional de Justicia en el caso mencionado, estableciendo que las operaciones cibernéticas constituyen un ataque armado de acuerdo con la Carta de las Naciones Unidas, brindando ejemplos para su mayor entendimiento, y aclarando que no todo uso de la fuerza significa un ataque armado, sino que deberá evaluarse la escala de severidad y los efectos de dicho ataque, ideas que surgen del fallo de Nicaragua contra Estados Unidos (Manual de Tallin 1.0, 2013).

Respecto al ataque perpetrado por agentes no estatales, en el caso Tadic (1995) el Tribunal Penal Internacional para la Antigua Yugoslavia consolidó la idea de que dichas agresiones, propias del conflicto

armado, pueden ser realizadas por grupos organizados enviados para ello, donde allí se encuentran fundadas las ideas expresadas en este trabajo relacionadas a la guerra híbrida.

A través de la realización de alguna de las operaciones cibernéticas mencionadas en el Capítulo anterior, se ha concluido en que las consecuencias que traen aparejadas dichas intervenciones pueden afectar y desestabilizar el control que tiene un Estado sobre sus asuntos internos, y por ende, ser constitutivo de una violación al principio de no intervención y de soberanía internacional. Sin embargo, no todo ataque perpetrado a través del ciberespacio cuenta con las mismas características, y debe analizarse cada caso de manera aislada contemplando el alcance, la duración y la intensidad de cada operación, dependiendo de las consecuencias que pueda traer consigo el hecho cibernético ilícito originario del conflicto armado (Sharp, 1999).

En este orden de ideas, una intervención cibernética en los asuntos internos de un Estado, viola la soberanía de dicho Estado y puede ser interpretada como un ataque armado, una agresión, y una vía habilitadora de la legítima defensa, de acuerdo con la interpretación de los elementos propios del ataque y de la jurisprudencia internacional. Sin embargo, a pesar de que técnicamente pueda justificarse una defensa contra dicha violación internacional, debe analizarse si la defensa “armada” es la vía más eficiente para repeler dicho ataque, e incluso los límites de su ejecución.

Proporcionalidad y necesidad de la defensa ante una intervención cibernética

Jensen (2002) brinda una descripción de cuáles son los requisitos principales para legitimar una acción de defensa:

> Two principles limit the doctrine of self-defense: necessity and proportionality. Necessity is the imminent danger of an armed attack; proportionality "is the degree of force, that is reasonable in terms of intensity, duration and magnitude, required to decisively counter the hostile act or demonstration of hostile intent that constitutes the necessity part of the equation-but no more than that." Any act of self-defense must therefore be out of necessity and must be proportional to the threat against which it defends. [Dos principios limitan la doctrina de la legítima defensa: necesidad y proporcionalidad. La necesidad es el peligro inminente de un ataque armado; la proporcionalidad "es el grado de fuerza, razonable en términos de intensidad, duración y magnitud, que se requiere para contrarrestar decisivamente el acto hostil o la demostración

> de intención hostil que constituye la parte de la ecuación correspondiente a la necesidad, pero no más que eso". Por lo tanto, todo acto de legítima defensa debe ser por necesidad y debe ser proporcional a la amenaza de la que se defiende.] (p.218).

Por otro lado, el uso de la fuerza como vía defensiva debe a su vez considerar que la acción original esté enmarcada dentro de la definición de ataque armado, sumado a la atribución de la responsabilidad antes mencionada –aspecto que hoy resulta de gran dificultad al tratarse de operaciones realizadas en el ciberespacio-, y que esta cumpla los requisitos de necesidad y proporcionalidad (Hadji-Janev y Aleksoski 2013).

El autor Novak Talavera (2002) se ha expedido, de manera similar, acerca de cuáles son los requisitos para que un Estado pueda hacer uso de la legítima defensa en virtud del artículo citado:

> ...para que un Estado, víctima de un ataque armado, pueda hacer un uso lícito de la legítima defensa requiere cumplir con ciertos requisitos, algunos de ellos exigidos por el derecho consuetudinario (necesidad, proporcionalidad e inmediatez) (p.24).

Si bien el primero de los requisitos puede ya acreditarse a través del argumento de la violación al principio de la soberanía internacional y por encontrarse esta situación en manifiesta incompatibilidad con la Carta de las Naciones Unidas, resulta menester que debe analizarse en detalle si la figura de la defensa armada resulta esencial para repeler dicho ataque, en virtud de determinados requisitos. Como se mencionó en los párrafos anteriores, la proporcionalidad y la necesidad son parte de los elementos que deben reunirse para que dicha defensa quede enmarcada en el derecho internacional público.

Por otro lado, no debe olvidarse de que la defensa será legítima siempre y cuando tenga un carácter supletorio del Consejo de Seguridad de las Naciones Unidas, debido a que el mismo artículo se encarga de establecer que la acción permitirá defenderse legítimamente "*hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales*" (artículo 51). En esta linea discursiva, la supletoriedad de la legítima defensa es considerada como otro de los requisitos fundamentales para esta vía (Torres, 2002).

Respecto de la noción de proporcionalidad a la luz del derecho internacional público, en el caso de Nicaragua contra Estados Unidos (1986) la Corte Internacional de Justicia criticó la falta de aclaración en

la Carta de las Naciones Unidas sobre la proporcionalidad de la legítima defensa, lo cual a su criterio ya existe desde el derecho consuetudinario:

> 176. As regards the suggestion that the areas cover'ed by the two sources of law are identical, the Court observes that the United Nations Charter, the convention to which most of the United States argument is directed, by no rneans covers the whole area of the regulation of the use of force in international relations. [...] Moreover the Charter, having itself recognized the existence of this right, does not go on to regulate directly al1 aspects of its content. For exarnple, it does not contain any specific rule whereby self-defence would warrant only rneasures which are proportional to the arrned attack and necessary to respond to it, a rule well established in custornary international law. [176. En cuanto a la sugerencia de que los ámbitos cubiertos por las dos fuentes de derecho son idénticos, el Tribunal observa que la Carta de las Naciones Unidas, la convención a la que se dirige la mayor parte de la argumentación de los Estados Unidos, no cubre en absoluto todo el ámbito de la regulación del uso de la fuerza en las relaciones internacionales [...] Además, la Carta, habiendo reconocido ella misma la existencia de este derecho, no pasa a regular directamente todos los aspectos de su contenido. Por ejemplo, no contiene ninguna norma específica según la cual la legítima defensa sólo justificaría las medidas proporcionales a la agresión sufrida y necesarias para responder a ella, una norma bien establecida en el derecho internacional consuetudinario.] (párr. 176).

Una vez que se ha probado que un ciberataque ha sido originado por un Estado, y que ha violado el principio de la no intervención de las Naciones Unidas a través del "ataque armado", debe analizarse qué tipo de defensa es proporcional al ataque perpetrado. Mientras que una escuela propone que la respuesta debe ser "ojo por ojo", en términos de equivalencia al ataque original –sea por vía de ocurrencia como en magnitud de daños ocasionados-, existe otra escuela que establece que la defensa debe tener como objetivo detener o repeler el ataque, sin perjuicio de más o menos grave que el ataque original (Pert, 2017). En esta línea, la vía elegida para la defensa legítima puede diferir tanto en naturaleza como en escala frente al ataque armado inicial, siempre y cuando la proporcionalidad logre atarse a los fines perseguidos mediante dicha acción defensiva (Kretzmer, 2013).

Por otro lado, el principio de proporcionalidad resulta un límite para el Estado que pretende defenderse, cuyo objetivo es evitar que se utilice al ataque original como argumento para perpetrar un ataque de ilimitado alcance generando daños desproporcionales e incluso contemplando la posibilidad de derivar en víctimas fatales (Gardam, 1993).

Con respecto a la necesidad como requisito para la toma de determinadas medidas, el mismo artículo 51 da una pista de dicho requisito, al establecer que esta acción defensiva será legítima "*hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales*" (artículo 51), por lo tanto, el Consejo de Seguridad será quien deberá tomar medidas necesarias para reestablecer el orden internacional. Ante la falta de esta toma de medidas, podrá ser el Estado atacado quien supla al Consejo de Seguridad, adoptando según su criterio, las que considere necesarias para ello.

Sin embargo, la tarea de considerar que una legítima defensa resulta una acción necesaria, no es para nada una tarea fácil. En esta línea, Lin (1963) establece:

> Not every illegal resort to force or act of aggression constitutes an armed attack and justifies the victim State to resort to force in self-defence. Resort to force in self-defence will be allowed only in case of absolute necessity. It is, therefore, necessary to consider under what degree of danger and urgency should the victim State of an illegal resort to force be entitled to resort to force in self-defence in accordance with Article 51. [No todo recurso ilegal a la fuerza o acto de agresión constituye un ataque armado y justifica que el Estado víctima recurra a la fuerza en defensa propia. El recurso a la fuerza en legítima defensa sólo se permitirá en caso de absoluta necesidad. Por lo tanto, es necesario considerar en qué grado de peligro y urgencia debe el Estado víctima de un recurso ilegal a la fuerza tener derecho a recurrir a la fuerza en legítima defensa de conformidad con el artículo 51.] (p.46-47).

La idea de peligro y urgencia que se desprenden de la necesidad de defenderse frente a un ataque armado, han seguido de otras nociones vinculadas. Una de ellas, es la conocida como "doctrina de Bush", y tiende a establecer la posibilidad legal de defenderse frente a un hecho ilícito que todavía no ocurrió, otorgando a esta acción defensiva una propiedad anticipatoria en caso de que la necesidad lo justifique (Himes y Kim, 2021). Al establecerse que la necesidad de defenderse está vinculada con el peligro inminente de ser atacado

(Jensen, 2002), la doctrina bush puede quedar enmarcada dentro de lo autorizado por la Carta de las Naciones Unidas siempre y cuando se logre atribuir la responsabilidad al Estado que resulte responsable intelectual del acto, especialmente cuando se trata de actores no estatales propios de la guerra híbrida, los cuales representan nuevos desafíos y retos para la práctica internacional (Pozo Serrano, 2018).

Otro de los aspectos que hacen a la necesidad de la legítima defensa, en línea con las ideas de urgencia, inminencia, peligro y subsidiariedad de la toma de medidas por parte del Consejo de Seguridad de las Naciones Unidas, es el argumento de la inmediatez de la acción defensiva, debido a la gravedad del ataque que no permite la toma de medidas pacíficas y consensuadas con el Órgano de Naciones Unidas, sino una vez tomadas las medidas urgentes para repeler el ataque (Rodriguez Rodriguez, 2019). Sin embargo, en la práctica, la noción de inmediatez suele estar un tanto ampliada y diluida frente a las acciones tomadas por los Estados (Vallarta Marrón, 2009).

La Cámara de Apelaciones de la Organización Mundial del Comercio, en el caso de *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef* (2000) estableció que el término de necesidad debe analizarse en virtud de varios factores equilibrados, entre los que se encuentra la posibilidad de hacer cumplir una norma de manera forzosa que no se estaba cumpliendo –reestableciendo el orden internacional- así como analizando los intereses en juego de ambas partes. Por otro lado, aclaró que no debe confundirse el término “necesario” con el de “indispensable”, ya que no siempre la medida necesaria será indispensable, pero podrá ser la opción elegida en determinados casos (Cottier et al., 2012).

Por otro lado, la Corte Internacional de Justicia (2003) se expresó sobre este asunto en el caso *Oil Platforms* (República Islámica de Irán contra Estados Unidos de América):

> ...in the present case a question of whether certain action is "necessary" arises both as an element of international law relating to self-defence and on the basis of the actual terms of Article XX, paragraph 1 (d), of the 1955 Treaty, already quoted, whereby the Treaty does "not preclude . . . measures . . . necessary to protect [the] essential security interests" of either party. In this latter respect, the United States claims that it considered in good faith that the attacks on the platforms were necessary to protect its essential security interests, and suggests that "A measure of discretion should be afforded to a party's good faith application of measures to protect its essential security interests”. [...en el presente caso se plantea la cuestión de si cierta acción es "necesaria"

> tanto como elemento del derecho internacional relativo a la legítima defensa como sobre la base de los propios términos del Artículo XX, párrafo 1 (d), del Tratado de 1955, ya citado, según el cual el Tratado "no excluye... las medidas... necesarias para proteger [los] intereses esenciales de seguridad" de cualquiera de las partes. . necesarias para proteger [los] intereses esenciales de seguridad" de cualquiera de las partes. A este último respecto, Estados Unidos alega que consideró de buena fe que los ataques a las plataformas eran necesarios para proteger sus intereses esenciales de seguridad, y sugiere que "debe concederse cierta discrecionalidad a la aplicación de buena fe de las medidas de una parte para proteger sus intereses esenciales de seguridad".] (párr.73).

Además, puede existir la posibilidad de que existan acciones defensivas menos dañinas para repeler el ataque, las cuales deben tomarse en cuenta previo a la toma de la acción. En caso de que un Estado se defienda mediante el uso de la fuerza armada existiendo vías alternativas pacíficas, probablemente incurra en una violación al derecho internacional público por no haber interpretado correctamente la esencia de la Carta de las Naciones Unidas, esto es, el objetivo de la organización internacional mediante la adopción del instrumento. A esta postura, la cual busca inmiscuirse en la mente del legislador constituyente, se la conoce como la interpretación subjetiva del legislador, y es a través de esta que se pretende poner el foco no en la norma como fín sino como un medio para la obtención de un objetivo (Cavino, 2009).

En linea con lo descripto anteriormente, una vez definidos los requisitos de proporcionalidad y necesidad para legitimar la vía defensiva por parte del Estado atacado, resta dilicudar qué vías de defensa pueden cumplir con estos requisitos al tratarse de ataques perpetrados a través del ciberespacio. Sin embargo, la postura que se toma en el presente trabajo de investigación no sigue la del “ojo por ojo” (Kretzmer, 2013), es decir, que debe tomarse como vía o acción defensiva la misma que permitió el acaecimiento del hecho internacionalmente ilícito –en este caso el ciberataque-, sino que podrían tomarse medidas defensivas mediante cualquiera de los otros cuatro escenarios de combate –tierra, mar, aire y espacio- siempre y cuando la acción cumpla con los requisitos de proporcionalidad y necesidad antes mencionados.

Un ejemplo concreto de cómo un ciberataque podría ser defendido mediante el uso de la fuerza armada a través de otros dominios de combate, se da con el siguiente caso: Una central de cómputos de un Estado interviene en un comando de control del aeropuerto de otro Estado, lo cual genera el inminente y severo peligro de que se ocasione un accidente de aviación con víctimas fatales. El Estado cuyo aeropuerto se encuentra intervenido, atribuye con exactitud la responsabilidad del Estado atacante, y envía un misil hacia

la central de cómputos que perpetra la intervención, como medida proporcional y necesaria para repeler de manera inmediata dicho ataque, subsidiariamente hasta que el Consejo de Seguridad tome conocimiento del asunto y resuelva cuáles serán las medidas ulteriores a tomar para el reestablecimiento del orden internacional.

El problema de determinar la proporcionalidad y necesidad de una legítima defensa, nacional y armada, frente a ataques de intervención cibernética resulta una díficíl de tarea de argumentación de acuerdo al cumplimiento de los requisitos profundizados en el presente trabajo. Si bien las intervenciones con consecuencias físicas, incluso aquellas desarrolladas a través de "ciberarmas" –término utilizado en el Manual de Tallin-, pueden facilitar la noción de los daños susceptibles de ser producidos, no ocurre la misma situación frente a aquellas con consecuencias económicas, psicológicas y sociales, las cuales requerirán que los Estados que pretendan defenderse armadamente deban pensar dos veces cómo demostrarán luego al Consejo de Seguridad el análisis previo.

Concluyendo con el presente Capítulo, una respuesta armada que busque enmarcarse dentro de la legítima defensa del artículo 51 de la Carta de las Naciones Unidas, deberá poder justificar sus aspectos de proporcionalidad y necesidad al ataque inicial, que a su vez contemplan las ideas de subsidiariedad, inminencia y anticipatoriedad, y por ende, deben tene como objetivo reestablecer el orden internacional a través de la no intervención sobre sus asuntos internos.

Al tratarse de operaciones cibernéticas que el Estado atacado propone identificar y categorizar como ataques armados, se deberán analizar todos los aspectos mencionados de manera particular en virtud de cada contexto, especialmente para argumentar que el hecho ilícito inminente cuenta con severidad suficiente para justificar que una defensa armada resulta proporcional para repeler dicho ataque (Schmitt, 1999). Sin perjuicio de lo desarrollado, aún prevalecen grandes discrepancias entre la doctrina y la jurisprudencia internacional por falta de clara regulación aplicable a la ciberguerra, lo cual lleva a dejar a manos de cada Estado la interpretación acerca de cuál es la vía más eficiente para repeler un ataque armado llevado adelante a través del ciberespacio (Hadji-Janev y Aleksoski 2013).

Esta página ha sido dejada en blanco intencionalmente.

Capítulo 7: Conclusiones

A raíz de lo analizado a través de metodologías cualitativas a lo largo del presente trabajo de investigación, puede concluirse que un ciberataque puede constituir una violación al principio de la no intervención garantizado por la Carta de las Naciones Unidas, y por ende, representar una vulnerabilidad a la soberanía nacional del Estado atacado, por lo cual se han logrado demostrar las hipótesis planteadas al comienzo del presente trabajo de investigación.

Gracias a los aportes de la Carta de las Naciones Unidas, la Convención de Ginebra, la jurisprudencia de la Corte Internacional de Justicia y la Corte Penal Internacional, sumado a las Resoluciones de la Asamblea de las Naciones Unidas y medios de interpretación complementarios como lo es el Manual de Talin, puede concluirse que un ciberataque desarrollado en el marco de una operación militar puede estar comprendido dentro de la figura del ataque armado y por ende representar un crimen de agresión. Sin perjuicio de ello, la Carta de las Naciones Unidas no establece diferencia alguna acerca de qué tipos de armas violan la prohibición del uso de la fuerza, lo cual nada lleva a la interpretación de que los ciberataques queden excluidos de la mencionada postura.

Una vez comprobado el hecho ilícito internacional, el estado debe investigar cuidadosamente el origen del ataque para atribuir la responsabilidad intelectual del acto, lo cual suele representar grandes desafíos de diversas índoles para los departamentos de inteligencia, seguridad y defensa nacional. Debido a la problemática técnica que representa el ciberespacio para la ciber atribución, se suma el complemento de que los Estados suelen utilizar vías indirectas de ataque a través de metodologías de guerra híbrida, esto es, a través de agentes no estatales, como lo son las guerrillas, las rebeliones y los grupos terroristas, los cuales dispersan la responsabilidad y ocultan al verdadero responsable intelectual del hecho.

En caso de que un Estado se defienda contraatacando a un Estado inocente, por presumir erroneamente que este había originado el ataque, dicha defensa representaría una violación al derecho internacional público por uso de la fuerza ilícito, lo cual daría lugar al Estado atacado injustamente a defenderse mediante la herramienta establecida por el artículo 51 de la Carta de las Naciones Unidas.

La intervención cibernética, que representa una violación al derecho internacional y que puede afectar la estabilidad de un gobierno en sus esferas políticas, económicas, psicológicas, sociales y estructurales, puede dar lugar a la legítima defensa armada por parte del Estado atacado, siempre y cuando la acción defensiva cumpla con los requisitos de atribución, proporcionalidad y necesidad establecidos por la legislación, jurisprudencia y doctrina internacional, lo cual puede representar también dificultades a la hora

de determinar si un ataque cibernético resulta proporcional con una defensa armada a perpetrar a través de otros dominios de combate, así como si esta defensa resulta necesaria para repeler dicho ataque.

Como no toda violación al derecho internacional significa que la defensa armada sea la vía proporcional y necesaria para el reestablecimiento del orden internacional, cada caso particular deberá analizarse de acuerdo a la escala de severidad y efectos del hecho ilícito.

Para concluir con el presente trabajo de investigación, el autor del presente trabajo se propone seguir investigando sobre el impacto de los ciberataques en el marco de las relaciones diplomáticas internacionales, continuando con el estudio de cuáles son los hechos ilícitos internacionales que pueden dar lugar a la legítima defensa armada, contemplando especialmente el cumplimiento de los requisitos de proporcionalidad y necesidad, en conjunto con el avance progresivo de las tecnologías que a su vez crean nuevas formas alternativas de respuesta que no exceden del quinto dominio, lo cual podría permitir a los Estados atacados la posibilidad de defenderse sin dañar a la población civil, y centraándose únicamente en el detenimiento del ataque original.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo 8: Bibliografía

Afërdita Berisha-Shaqiri y Mihane Berisha-Naman (2015). Information Technology and the Digital Economy. Mediterranean Journal of Social Sciences. MCSER Publishing. Rome-Italy. Vol 6, No 6.

Aida Karazhanova and Elena Dyakonova (2021). Assessing E-Resilience in Kazakhstan, Kyrgyzstan, and Mongolia. Asia-Pacific Information Superhighway Working Paper Series, No. 03/2021. United Nations ESCAP, ICT and Disaster Risk Reduction Division, Bangkok, p.19-25.

Alberto Heimler (11 y 12 de julio de 2006). Competition Policy, Antitrust Enforcement And Banking: Some Recent Developments. Fourth Meeting Of The Latin American Competition Forum. San Salvador, Session II, p.1.

Alexander Pierre Faure (2013). Financial System: An introduction. 1st Edition. Quoin Institute, p.8.

Alison Pert (2017). Proportionality in Self-Defence – Proportionate to What? Pandoras Box, Vol. 24, p. 65-78.

Andreea Bendovschi (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures, 7th International Conference On Financial Criminology, Wadham College, Oxford, United Kingdom, Procedia Economics and Finance 28, p.25.

Andrzej Kozlowski (2014). Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan, European Scientific Journal. Special Edition vol.3. p.237-245.

Annie Himes y Brian J. Kim (2021), Self-Defense on Behalf of Non-State Actors. Penn Law: Legal Scholarship Repository, Vol. 43:1, 2021, p.245.

Ariel Vercelli (2018). La (des)protección de los datos personales: análisis del caso Facebook Inc. - Cambridge Analytica. XVIII Simposio Argentino de Informática y Derecho, p.2.

Armada de los Estados Unidos de América (abril de 2020). Naval Warfare, Naval Doctrine Publication 1, NDP, p.1.

Campos Salazar, J.N. (2019). Análisis de la Carta de la ONU a la luz de los postulados del texto “Zum ewigen Frieden” de Immanuel Kant. El objetivo de la paz y el mecanismo de la guerra. ANIDIP (7), 116-140, p.119.

Can Kasapoğlu (2015). Turkey's Future Cyber Defense Landscape, en Sinan Ülgen, A Primer on Cyber Security in Turkey and the Case of Nuclear Power, The Centre for Economics and Foreign Policy Studies. EDAM. Hare Sokak No: 16, p.4.

Carlos Alfredo Pérez Aquino (2017). Teorías en Pugna para Explicar las Guerras Actuales. Visión Conjunta. Año 9. Núm. 16, p. 47.

Carta de las Naciones Unidas (26 de junio de 1945).

Casson Moreno, V., Reniers, G., Salzano, E. y Cozzani, V. (26 de marzo de 2018). Analysis of Physical and Cyber Security Related Events in the Chemical and Process Industry. Process Safety and Environmental Protection, 116, 621-631.

Centro de las Naciones Unidas de Lucha Contra el Terrorismo y Oficina de Naciones Unidas contra el Terrorismo (2018). The protection of critical infrastructures against terrorist attacks: Compendium of good practices, p.48.

Cevat Özarpa et al. (Octubre de 2021). Cyber Attacks on Scada Based Traffic Light Control Systems in the Smart Cities. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLVI-4/W5-2021 The 6th International Conference on Smart City Applications. Karabuk University, Turkey, p.412.

Chris Dougherty (Mayo de 2021), More than Half the Battle: Information and Command in a New American Way of War, Center for a New American Security, p.37.

Comisión de Derecho Internacional de Naciones Unidas (2001). Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.° período de sesiones, Volumen II, Segunda Parte, p.32.

Convención de Viena sobre el Derecho de los Tratados (23 de mayo de 1949). Documento de Naciones Unidas A/CONF.39/27. Artículo 32.

Convenio de Ginebra para Aliviar la Suerte que Corren los Heridos y los Enfermos de las Fuerzas Armadas en Campaña (12 agosto de 1949) del Comité Internacional de la Cruz Roja, Suiza, artículo 2.

Cristian Altavilla (2009). El Sistema Tributario Argentino. Breve Consideración Sobre Su Evolución Y Situación Actual. Revista de la Facultad. Vol. X, Nº 2, Nueva Serie II, p.171-200.

Cristiano Castelfranchi (diciembre de 2007). Six critical remarks on science and the construction of the knowledge society. Journal of Science Communication. SISSA – International School for Advanced Studies Journal of Science Communication, p.1.

Cybersecurity and Infrastructure Security Agency of the United States Government (2019). A Guide to Critical Infrastructure Security and Resilience, p.4 y 22.

Daniel Bethlehem (2012). Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors, The American Journal Of International Law, Vol. 106:000, 2012, p.1.

David A. Deptula (2015). Una nueva era para el comando y control de operaciones aeroespaciales, Air & Space Power Journal en Español, Air University, Maxwell AFB, AL, Volumen 27, Nº 4 - 4to Trimestre, p.55.

David E. Johnson (2018). An Overview of Land Warfare, en Dakota L. Wood (2018). Index of U.S. Military Strength. Davis Institute For National Security And Foreign Policy. The Heritage Foundation, p.32.

Decisión del 11 de diciembre de 2000 de la Organización Mundial de Comercio, relativo al caso "Korea-Measures Affecting Imports of Fresh, Chilled and Frozen Beef", WT/DS161/AB/R, párrafo. 164.

Declaración Universal de los Derechos Humanos (1948) de la Asamblea General de Naciones Unidas. Paris, artículo 11, párrafo 1.

Duić, I., Cvrtila, V. y Ivanjko, T. (Mayo de 2017) International Cyber Security Challenges. 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, p.1525.

Economic Commission for Latin America and the Caribbean (2021). Digital technologies for a new future. Ref. LC/TS.2021/43, Santiago, p.7 y 79.

Efrén Gustavo Marqués Rueda (2009). El acto y crimen de agresión en el derecho internacional público y su repercusión en las relaciones políticas internacionales, Anuario Mexicano de Derecho Internacional, vol. IX, Ciudad de México, p.343.

Enmiendas al Estatuto de Roma de la Corte Penal Internacional relativas al Crimen de Agresión (11 de junio de 2010). Conferencia de Revisión de la Corte Penal Internacional. Resolución N°6. Anexo 1. Artículo 8 bis.

Eric Talbot Jensen (2002). Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 Stan. J. Int'l L. 207, p.218.

Eric Talbot Jensen (2017). The Tallinn Manual 2.0: Highlights and Insights. 48 Georgetown Journal of International Law, p.735-738.

Eugene Eg Tan (2 de abril de 2018). Cyber Deterrence in Singapore. Framework & Recommendations, S. Rajaratnam School of International Studies, Singapore, vol. 309, p.28-29.

Fabián Novak Talavera (2002). La intervención de los Estados Unidos de América en Afganistán: ¿hecho ilícito internacional? Agenda Internacional, Año VIl, N°16, p. 24.

Farwell, James P. y Rohozinski, Rafal (2011). Stuxnet and the Future of Cyber War, Survival, 53:1, p.24-25.

Fernando Thauby García (1996). Escenarios Bélicos Futuros. Clausewitz. Revista de Marina, Núm 4/96, p.374.

Frank D. Fincham y Joseph M. Haspars (1980). Attribution of Responsibility: From Man the Scientist to Man As Lawyer, en Leonard Berkowitz. Advances in Experimental Social Psychology, 1st Ed., Volume 13, p.82.

Fu-Shun Lin (1963). Self-Defence - A Permissible Use of Force under the U.N. Charter, Volume 13 Issue 1, DePaul Law Review 43.

Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan y Jared Stancombe (2021). Opportunities for Public and Private Attribution of Cyber Operations, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Papers Young Scholar Edition No. 12, 2021, p.6.

Germán Ramírez Bulla (diciembre de 2008). El ejercicio de la soberanía territorial de acuerdo con los tratados y principios del derecho internacional. El caso colombiano. Revista Derecho del Estado n.º 21, p.124.

Gonzalo de Salazar Serantes (2004). El nuevo desafío: la proliferación nuclear en el umbral del siglo XXI, Documentos CIDOB, Seguridad y Defensa, Número 4, p.7.

Gracienne Lauwers (2019). Reshaping Teacher Training to Get the Right Education System for a Knowledge Society. En Marta Kowalczuk-Walêdziak, Alicja Korzeniecka-Bondar, Wioleta Danilewicz y Gracienne Lauwers (2019). Rethinking Teacher Education for the 21st Century. Trends, Challenges and New Directions, Verlag Barbara Budrich, p.43.

Grzegorz Strupczewski (2021). Defining cyber risk, Safety Science 135, p.1-2.

Guan, T.; Han, Y., Kang, N., Tang, N., Chen, X. y Wang, S. (2022). An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles. Sustainability, 14, 5211, p. 1-17.

Guy-Philippe Goldstein (septiembre de 2013). Cyber Weapons and International Stability: New Destabilization Threats Require New Security Doctrines. Military and Strategic Affairs, Volume 5, No. 2, p.9.

Hernán Santa Cruz (1995). La creación de las Naciones Unidas y de la CEPAL. En Aníbal Pinto (1995). Revista de la CEPAL 57, Santiago de Chile, p.18.

Informe de la Asamblea General de las Naciones Unidas A/70/174 (22 de julio de 2015), Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Párrafo 13, punto b.

Interpol (abril de 2021). Guía sobre la Estrategia Nacional contra la Ciberdelincuencia, p.2

Ioannis Agrafiotis et al. (2018). A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate, Journal of Cyber-security. Vol. 0, Num. 0, p. 7.

Irwansuah Maskun, Yunus Ahsan , Safira Armelia y Lubis Nurhalima Siti (2021). Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with It. Jambe Law Journal, Vol. 4 No. 2, p.135.

James J. Wirtz (2015). Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy, capítulo 3. En Kenneth Geers (2015), Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications, Tallinn, p.30.

James Jay Carafano (2018). America's Joint Force and the Domains of Warfare. En Dakota L. Wood (2018). Index of U.S. Military Strength, Davis Institute For National Security And Foreign Policy. The Heritage Foundation, p.23.

James K. Wither (2020). Defining Hybrid Warfare, Per Concordiam, Journal of European Security and Defense Issues, Perspectives on Hybrid Warfare. Volume 10, Issue 1, p.7.

Javier López de Turiso y Sanchez (2012). La Evaluación del Conflicto Hacia un Nuevo Escenario Bélico, en Ministerio de Defensa de España. Centro Superior de Estudios de la Defensa Nacional. El Ciberespacio. Nuevo Escenario de Confrontación, p.143.

Jawwad A. Shamsi, Sherali Zeadally y Zafar Nasir (2016). Interventions in Cyberspace: Status and Trends, IT Pro, 2016, The IEEE Computer Society, p.18.

Jeffrey Thomas Biller (2013). Cyber-Terrorism: Finding a Common Starting Point, Journal Of Law, Technology & The Internet, Vol. 4, No. 2, p.292.

John Keegan (1993). A History Of Warfare, London, Hutchinson, cap. I.

John L. Douglas (2008). The Role Of A Banking System In Nationbuilding, Maine Law Review, Vol. 60:2, p.512.

Jorge José Torres (noviembre de 2002). Estados Unidos, el Terrorismo Internacional y el Sistema de Seguridad Colectiva, la legítima defensa preventiva y la nueva doctrina de la seguridad del Presidente Bush, Primer Congreso en Relaciones Internacionales del Instituto de Relaciones Internacionales de la Universidad Nacional de La Plata.

Jorge Rodríguez Rodríguez (2019). El uso de la fuerza contra actores no estatales. Una crítica a la teoría "unwilling or unable" desde el Derecho Internacional vigente. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales, p.1-31.

Jose Diaz de Leon (2021). Understanding Multi-Domain Operations in NATO. The Three Swords Magazine No. 37, p.92.

José Javier Muñoz Castresana (1996). El Control del Espacio Aéreo en Situaciones de Paz, Crisis y Guerra. En Ministerio de Defensa de España (1996). Secretaría General Técnica, Boletín de Información Núm. 247.

José Luis Vallarta Marrón (2009). El derecho inmanente a la legítima defensa individual o colectiva en caso de ataque armado. ¿Se justifica una interpretación extensiva para incluir medidas preventivas y punitivas? Una visión israelí. Anuario Mexicano de Derecho Internacional, Vol. 9, Ciudad de México.

José Luis Vallarta Marrón (2011). La Incorporación del Crimen de Agresión en el Estatuto de la Corte Penal Internacional, Anuario Mexicano de Derecho Internacional, vol. XI, p.443.

Juan Jose Terrados (2019). Hybrid Warfare, The Three Swords Magazine No. 35, p.45.

Judith Gail Gardam (julio de 1993). Proportionality and Force in International Law, The American Journal of International Law Vol. 87, No. 3, p.391-413.

K. Patel y S. Patel (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing, Vol 6, Issue No. 5, p.1.

Kosmas Pipyros, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis y Theodoros Apostolopoulos (mayo de 2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual, Computers and Security, Volume 74, p.375.

Kretzmer (2013). The Inherent Right to Self Defence and Proportionality in Jus Ad Bellum. The European Journal of International Law Vol. 24, No. 1.

Kristin Ven Bruusgaard (2021). Russian nuclear strategy and conventional inferiority. Journal of Strategic Studies, 44:1, p.8.

Lima Quintanilha, T., Torres da Silva, M. y Lapa, T. (2019). Fake news and its impact on trust in the news. Using the Portuguese case to establish lines of differentiation. Communication & Society, 32(3), p.18.

Luis Feliu Ortega (2012). La Ciberseguridad y la Ciberdefensa. En Centro Superior de Estudios de la Defensa Nacional (2012), El Ciberespacio. Nuevo Escenario de Confrontación. Monografías de CESEDEN 126. Ministerio de Defensa de España, p.44.

Maggie Gray y Amy Ertan (2021). Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, p.8.

Manual de Tallin 2.0 sobre Derecho Internacional Aplicable a las Ciber Operaciones, del 2017, preparado por el Grupo Internacional de Expertos invitado por la NATO Cooperative Cyber Defence Centre of Excellence (CCDCE). Michael N. Schmitt, Cambridge University Press.

Manual de Tallin sobre Derecho Internacional Aplicable a la Ciberguerra, del 2013, preparado por el Grupo Internacional de Expertos invitado por la NATO Cooperative Cyber Defence Centre of Excellence (CCDCE). Michael N. Schmitt, Cambridge University Press.

Marcus A. Jones y Jose Diaz de Leon (2020). Multi-Domain Operations, Awareness continues to spread about the importance of operating in multiple domains, The Three Swords Magazine 36/2020, p.41.

Mario Bergara, et al. (2003). Economía para no economistas, Departamento de Sociología, Facultad de Ciencias Sociales, Universidad de la República, p.13.

Marjan Laal (2012). 2nd World Conference on Innovation and Computer Sciences, AWER Procedia Information Technology & Computer Science 2, p.1-2.

Marko Milanovic (2020). Special Rules of Attribution of Conduct in International Law, International Law Studies, Stockton Center for International Law, Vol. 96, p.315.

Massimo Cavino (junio de 2009). Intención del legislador y significado de la Ley Ordinaria en la Jurisprudencia de la Corte Constitucional Italiana. Derechos y Libertades Número 21, Época II, pp. 17-55.

Merriam, Sharan B. (2002). Qualitative research in practice: Examples for discussion and analysis. The Jossey-Bass Higher and Adult education Series, John Wiley & Sons; Ed. No. 1.

Merrick E. Krause (2015). El poderío aéreo en la guerra moderna. Air & Space Power Journal en Español. Air University, Volumen 27, Nº 4 - 4to Trimestre 2015, p.34.

Metodi Hadji-Janev y Stevan Aleksoski (2013). Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace. Mediterranean Journal of Social Sciences, Rome-Italy, Vol 4 No 14, p.117.

Michael N. Schmitt (diciembre de 2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harvard International Law Journal Online, Vol. 54, p.14-15.

Michael Schmitt y Liis Vihul (2017). Tallin Manual 2.0. Cambrigde: Cambridge University Press.

Michael W. Benítez (2016). La guerra aérea del siglo XXI y la Guerra Invisible, Agilidad Estratégica. Air & Space Power Journal En Español, Air University, Maxwell AFB, AL, Volumen 28, Nº 3, p.90.

Michał Choraś, Rafał Kozik, Adam Flizikowski, Witold Hołubowiczand y Rafał Renk (2016). Cyber Threats Impacting Critical Infrastructures, Cap.7. En R. Setola et al. (2016). Managing the Complexity of Critical Infrastructures, Studies in Systems, Decision and Control, 1st Ed., p.139.

Michel Schmitt (1999). Computer Network Attack and the Use of force in International law. The Columbia Journal of Transnational Law, Volume 37, p.885-937.

Mihane Berisha-Namani y Myrvete Badivuku-Pantina (2009), Information Society and Knowledge Economy, Lex ET Scientia. IT Series, LESIJ No. XVI, Vol. 2, p.556.

Mohammad Furqan Ali, et al. (junio de 2019). The Internet of Things and Benefits at a Glance. International Journal of Science and Engineering Investigations, vol. 8, issue 89, p.98.

Mohammad Sameen (2019). Psychological Warfare: A Critical Study of Tactics and conceptualization in Indian perspective. National Seminar on emerging contours of Defence laws and National Security.

Mónica Pinto (2003). La Noción de Conflicto Armado en la Jurisprudencia del Tribunal Penal Para la Ex Yugoslavia, en Mary Beloff (2003), Lecciones y Ensayos 78, Facultad de Derecho, Universidad de Buenos Aires, 1° ed., p.310.

Naciones Unidas (1947). Yearbook of the United Nations 1946-47, Department of Public Information, United Nations, Lake Success, New York, p.1.

Naciones Unidas (2018). Technology and Innovation Report 2018, Harnessing Frontier Technologies for Sustainable Development. Docuemento UNCTAD/TIR/2018, p.7-20.

Najman Alexander Aizenstatd Leistenschneider (2012). La Responsabilidad Internacional de los Estados por Actos Ilícitos, Crímenes Internacionales y Daños Transfronterizos. Anuario Mexicano de Derecho Internacional, Vol XII, p.10.

Nico K. Schrijver (2006). The Future of the Charter of the United Nations, Max Planck Yearbook of United Nations Law, Volume 10, p.7.

OECD (2013). Supporting Investment in Knowledge Capital. Growth and Innovation, OECD Publishing, p.24.

OECD (2018). Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation. 4th Edition. The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing, p.33.

Oona A. Hathaway, et al. (agosto de 2012). The Law of Cyber-Attack. California Law Review, Inc., Vol. 100, No. 4, p. 817-885.

Opinión Consultiva del 8 de julio de 1996 de la Corte Internacional de Justicia, sobre la legalidad de la amenaza o el empleo de armas nucleares, párrafos 38 y 39.

Patrik Aspers y Ugo Corte (2019). What is Qualitative in Qualitative Research. Qualitative Sociology 42:139–160.

Pilar Pozo Serrano (2018). La legitima defensa frente a actores no estatales a la luz de la práctica del Consejo de Seguridad de las Naciones Unidas, Anuario Español De Derecho Internacional, Vol. 34.

Plunkett, Leah y Urs Gasser (2016). Student Privacy and Ed Tech (K-12) Research Briefing. Berkman Klein Center for Internet and Society Publication Series, p.3.

Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (8 de junio de 1977), Comité Internacional de la Cruz Roja, artículo 1, párrafo 4.

Rabea Alqamoudi (abril de 2021). The Concept of Internacional Law. International Journal of Scientific and Research Publications, Volume 11, Issue 4, p.520.

Raúl Moralez Reséndiz (2019). Cooperación Internacional y su Papel en la Gestión del Riesgo Cibernético. En Organización de los Estados Americanos (octubre de 2019). Desafíos Del Riesgo Cibernético en el Sector Financiero Para Colombia Y América Latina, Primera Ed., p.45.

Reglamento (UE) 2019/881 del Parlamento Europeo y Consejo de Europa, del 17 de abril de 2019, considerando 3.

Renato Nuño Luco (2003). La guerra aérea y el derecho internacional humanitario. En Gabriel Pablo Valladares (2003). Derecho internacional humanitario y temas de áreas vinculadas, Lecciones y Ensayos nro. 78, Lexis Nexis Abeledo Perrot, p.201-237.

Resolución 1523/2019 (12 de septiembre de 2019) de la Jefatura de Gabinete de Ministros, Secretaria de Gobierno de Modernización de la República Argentina. Anexo I, punto I, primer y segundo párrafo.

Resolución 2131 de la Asamblea General de Naciones Unidas, del 21 de diciembre de 1965, relativa a la Declaración sobre la inadmisibilidad de la intervención en loa asuntos internos de los Estados y protección de su independencia y soberanía.

Resolución 2625 de la Asamblea General de las Naciones Unidas (24 de octubre de 1970). Declaración sobre 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 (A/802). Punto 1, párrafo 24-25.

Resolución 3314 de la Asamblea General de las Naciones Unidas (14 de diciembre de 1974). Definición de Agresión. Artículo 3.

Resolución 55/25 de la Asamblea General de las Naciones Unidas (8 de enero de 2001). Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Artículo 6

Resolución 808 del Consejo de Seguridad de las Naciones Unidas, del 22 de febrero de 1993, párrafo 5.

Resolución de la Asamblea General de las Naciones Unidas AG/56/83 (12 de diciembre de 2001). Responsabilidad del Estado por hechos internacionalmente ilícitos. Artículo 4.

Roberto Uzal (8 de agosto de 2013). Conferencia sobre “Cyber Money Laundering” variante “Cyber Gambling”. Consejo Argentino de Relaciones Internacionales, Universidad Nacional de San Luis, p.4.

Roberto Uzal, Daniel Riesco, German Montejano, Walter Agüero y Claudio Baieli (2015). Lavado Transnacional de Activos en el Ciberespacio. Presentación del contexto, planteo del problema y formulación de propuestas, SIE 2015, 9º Simposio de Informática en el Estado, p.178.

Ronald L. Jackson II, Darlene K. Drummond y Sakile Camara (2007). What Is Qualitative Research?, Qualitative Research Reports in Communication, 8:1, p.21-28.

Russell Buchan (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? Journal of Conflict & Security Law, Vol. 17, No. 2, p. 211-227.

Ryan Hayward (marzo de 2017). Evaluating 'Imminence' of a Cyber Attack for Purposes of Anticipatory Defense, Columbia Law Review, Vol. 117, No. 2, p.399-434.

Samson Olasunkanmi Oluga et al. (marzo de 2014). An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats. International Journal of Computer Science and Information Security, Vol. 12, No. 3.

Sentencia del 2 de octubre de 1995 del Tribunal Penal Internacional para la ex-Yugoslavia, relativo al caso "Prosecutor v. Dusko Tadic", párrafo 70.

Sentencia del 26 de febrero de 2007 de la Corte Internacional de Justicia, relativa a la aplicación del Convención sobre Prevención y Represión del Delito de Genocidio (Bosnia y Herzegovina c/ Serbia y Montenegro), Considerando 401.

Sentencia del 27 de junio de 1986 de la Corte Internacional de Justicia, en el caso Relativo a las Actividades Militares y Paramilitares en Nicaragua y Contra Nicaragua (Nicaragua c/ Estados Unidos de América), considerando 165.

Sentencia del 6 de noviembre de 2003 de la Corte Internacional de Justicia, en el caso relativo a las Plataformas Petrolíferas (República Islámica de Irán c/ Estados Unidos de América), considerando 73.

Sergio G. Eissa, Sol Gastaldi, Iván Poczynok y María Elina Zacarías Di Tullio (noviembre de 2012). El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino. VI Congreso de Relaciones Internacionales, Instituto de Relaciones Internacionales, Universidad Nacional de La Plata, p.1.

Stephen Blank (2017). Cyber War and Information War à la Russe. En Georg Perkovic y Ariel E. Levite (2017). Understanding Cyber Conflict: Fourteen Analogies, Georgetown University Press, p.88-90.

Steven J. Anderson (2016). Artifacts for Cyber Power Targeting, Airpower Lessons for an Air Force Cyber-Power Targeting Theory. Air Force Research Institute, Air University Press, Drew Paper No. 23, School of Advanced Air and Space Studies, p.62-72.

Thomas Callender (2018). The Naval Warfare Domain. En Dakota L. Wood (2018). Index of U.S. Military Strength, Davis Institute For National Security And Foreign Policy, The Heritage Foundation, p.32.

Thomas Cottier et al. (diciembre de 2012). The Principle of Proportionality in International Law, Working Paper No 2012/38. NCCR Trade Regulation, Swiss National Centre of Competence in Research.

Ukwandu, E. et al. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. Information, MDPI, 13:146.

Vyacheslav A. Perepelkina, Elena V. Perepelkinaa y Elena S. Morozova (2016). Evolution of the Concept of “Human Capital” in Economic Science. International Journal of Environmental & Science Education, Vol. 11, No. 15, p.7650.

Walter G. Sharp (1999). Cyberspace and the use of force. Aegis Research Corporation, p.15.

William C. Ashmore (2009). Impact of Alleged Russian Cyber Attacks, School of Advanced Military Studies. United States Army Command and General Staff, AY No. 08, p.13.

Wojciech Filipkowski (junio de 2008). Cyber Laundering: An Analysis of Typology and Techniques, International Journal of Criminal Justice Sciences, Vol 3 Issue 1, p.17.

Xingan Li (19 de febrero de 2017). A Review of Motivations of Illegal Cyber Activities. Criminology & Social Integration Journal Vol. 25 No. 1. School of Governance, Law and Society, Tallinn University, Estonia.

Zang, Jinyan (2021). Case Studies in Public Interest Technology. Doctoral Dissertation, Harvard University Graduate School of Arts and Sciences, p.3.

Zs. Haig (2021). Advances in Military Technology Relationships between Cyberspace Operations and Information Operations, Vol. 16, No. 1, p.93-100.