CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL

ISSN 0719-4110

CUADERNO DE TRABAJO N°14-2019

ATRIBUCIÓN EN EL CIBERESPACIO: PIEDRA TOPE EN EL DERECHO INTERNACIONAL

CUADERNOS DE TRABAJO es una publicación orientada a abordar temas vinculados a la Seguridad y Defensa a fin de contribuir a la formación de opinión en estas materias.

Los cuadernos están principalmente dirigidos a tomadores de decisiones y asesores del ámbito de la Defensa, altos oficiales de las Fuerzas Armadas, académicos y personas relacionadas con la comunidad de defensa en general.

Estos cuadernos son elaborados por investigadores del CIEE de la ANEPE, pero sus páginas se encuentran abiertas a todos quienes quieran contribuir al pensamiento y debate de estos temas.

CUADERNO DE TRABAJO DEL CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS es una publicación electrónica del Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos y está registrada bajo el **ISSN 0719-4110 Cuad. Trab., - Cent. Estud. Estratég.**
Dirección postal: Avda. Eliodoro Yáñez 2760, Providencia, Santiago, Chile.
Sitio Web www.anepe.cl. Teléfonos (+56 2) 2598 1000, correo electrónico ciee@anepe.cl

ATRIBUCIÓN EN EL CIBERESPACIO: PIEDRA TOPE EN EL DERECHO INTERNACIONAL

2019

Pía Martabit Tellechea*

Resumen

El anonimato en el ciberespacio es el problema fundamental que tienen hoy los diversos actores que buscan hacer de este un lugar seguro. La atribución de las acciones delictuales o ataques en Internet es la piedra angular faltante y necesaria en todos los marcos jurídicos que se pretendan formar institucionalidad normativa que busquen impedir o retribuir los daños efectuados por estas acciones. Es, por otro lado, una ventaja para aquellos actores internacionales que muestren interés en realizar ataques de carácter oculto para evitar las consecuencias de dicha acción. Por otro lado, el anonimato resulta una ventaja vital para diferentes actores, sobre todo organismos civiles, que requieren de comunicaciones fuera de la supervisión del Estado, y a su vez es un carácter fundamental si se aborda desde la privacidad como un bien. La incapacidad de atribuir una acción hostil no es, como se ha generalizado, necesariamente un problema, sino más bien un fenómeno que se debe analizar de acuerdo a la naturaleza de los participantes de la sociedad global y sus respectivos y diversos intereses.

Palabras clave: Seguridad internacional, ciberseguridad, anonimato, Derecho internacional

Introducción

El coronel Eric F. Mejia escribió para la revista Strategic Studies Quarterly de la Fuerza Aérea de los Estados Unidos sobre la importancia de la atribución a la hora de un ciberataque. En dicho artículo compara experiencias que sufrieron dos individuos en la isla de Hawaii. El primer suceso fue el ataque a la base naval Pearl Harbor el año 1941, en donde el sargento técnico Joe Pesek fue víctima del bombardeo sorpresivo por parte de los japoneses en la isla[1]. El segundo caso fue el comandante Shelly Johnson que, 70 años después, fue víctima de un masivo ciberataque que le impidió acceder a su cuenta bancaria[2]. Esta agresión se lo atribuyó el grupo islamista Cyber Fighters de Izz Ad-Din Al Qassam.

* Docente del Instituto de Humanidades, Universidad del Desarrollo. Cientista político de la Universidad del Desarrollo y magíster en Periodismo Mención Prensa Escrita de la Pontificia Universidad Católica de Chile, con estudios de diplomado en Seguridad Internacional y Ciberseguridad de la Universidad de Chile. piajomte@gmail.com

[1] MEJIA, E. Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework. Strategic Studies Quarterly, 8(1), pp.114-132, Primavera 2014. [En línea] Disponible en:<http://www.jstor.org/stable/26270607>

[2] Ibíd.

Sin embargo, investigadores cuestionaron la real responsabilidad de dicho "*hackeo*" masivo a bancos norteamericanos[3]. Mejía señala que, ante estos casos de ciberataques, surgen más preguntas que respuestas: "¿Podría incluso considerarse un ataque y, de ser así, qué fue vulnerado: los clientes, los bancos, la economía de los Estados Unidos? ¿Quién respondería y cómo?"[4]. Ante estas interrogantes y en base a estos dos casos puestos en la isla de Hawaii, Mejía busca establecer la problemática de atribución.

> "En el caso de Pearl Harbor, hubo un ataque armado hostil directamente atribuible a un actor estatal conocido. Estos hechos establecieron la respuesta adecuada —la guerra— y el respondedor adecuado: los militares. En el segundo escenario, el acto y el actor eran inciertos; en consecuencia, la respuesta y el respondedor adecuados fueron igualmente inciertos"[5].

Es esta cuestión de atribución, que se enmarca en el derecho internacional, que resulta problemático a la hora de establecer estrategias y toma de decisiones en materia de seguridad fundamentales para responder efectivamente ante este tipo de ataques. El objetivo general y principal de este artículo es analizar el problema de atribución como el desafío más importante en la institucionalidad internacional, y también nacional, para ser un mecanismo efectivo de "segurización" del ciberespacio. Para eso, se analizará la naturaleza de dicho espacio informático y la variable del anonimato de esta dimensión. Luego se revisarán aquellos actores y casos donde la incapacidad de atribución se transforma en un beneficio o perjuicio. Finalmente, se establecerá un análisis crítico que permita aseverar que la reducción del anonimato sería la política más eficiente y eficaz para aumentar la ciberseguridad.

"Los esfuerzos de los organismos y entes para generar marcos jurídicos y de regulación efectivos en el ciberespacio resultarán insuficientes, si en la eventualidad de un conflicto no se generan los estímulos para resolver el problema de atribución."

Los esfuerzos de los organismos y entes para generar marcos jurídicos y de regulación efectivos en el ciberespacio resultarán insuficientes, si en la eventualidad de un conflicto no se generan los estímulos para resolver el problema de atribución. Esto es al menos que se desarrollen mecanismos y estrategias alternativas para minimizar los efectos y costos negativos del anonimato. El objetivo de este análisis es esquematizar el fenómeno en relación a sus alcances positivos y negativos en diversos actores junto a sus roles en el escenario de las relaciones internacionales, profundizando en el fenómeno más allá de su percepción negativa actual que se debería erradicar.

Atribución al actor, atribución al acto

Volviendo al artículo de Mejía, es interesante la distinción que hace con respecto a tipos de atribuciones, determinando que existen dos categorías diferentes. La primera es un tipo asociado al actor, es decir, quién comete el acto, y la segunda es del acto mismo que pretende determinar la severidad de este[6]. Mejía destaca que el objetivo principal de dichos esfuerzos, tanto desde el análisis académico como la puesta en práctica de la atribución, recae en que al no

[3] Ibíd.
[4] Ibíd. p.115.
[5] Ibíd.
[6] Ibíd.

poder determinar culpables y severidad de una agresión, no podrá determinarse una respuesta apropiada, así como quién debe asumir una respuesta[7].

Por ejemplo, en casos donde un ataque alcanza una condición severa tipo "crimen, sin alcanzar una categoría "bélico", es el escenario propicio para el actuar de aquellas instituciones que deben enfrentar este tipo de actos y determinar la respuesta acorde al acto criminal y establecer el castigo dentro de un marco jurídico.

En el caso del ciberespacio, como escenario de estas amenazas, es más difícil de definir. Además, la forma de establecer un ataque como materia de seguridad estatal responderá a posibilidades de acción diferente. En el caso de Pearl Harbor, fue innegable que un ataque de ese tipo correspondía replicar con una declaración de guerra, el último recurso de la política (Clausewitz).

Considerando que se busca definir el tipo de respuestas frente a daños ocasionados en la dimensión del ciberespacio, nuestro punto de comparación inicial serán los conflictos armados, junto con las regulaciones que prescriben el Derecho internacional.

Para eso la institucionalidad jurídica referente a los conflictos armados es el que naturalmente debe ser planteado en el contexto del ciberespacio. Es decir, buscar aquellas normas del referente al uso de las armas, su aplicabilidad en esta nueva forma de llevar a cabo conflictos. Dicho esto, necesario será iniciar el estudio manifestando que un escenario bélico presenta como dificultad que los beligerantes tratan con violencia física, es decir que el miedo a la muerte es el principal motor, mientras que la destrucción de recursos pasa a ser secundaria, pero no menos relevante.

El ataque cibernético es en primera instancia un acto que provoca una destrucción de infraestructura y recursos, y no necesariamente una amenaza a la vida e integridad de la población. Esta distinción resulta evidente entre los dos ejemplos que menciona Mejía. Obviamente se pueden presentar otras posibilidades, sobre todo en el futuro con el desarrollo de mayor digitalización y dependencia de las redes por parte de la sociedad, dimensión en que un ciberataque podría causar la muerte de personas, tal como una plataforma aérea lanzara bombas.

"El ataque cibernético es en primera instancia un acto que provoca una destrucción de infraestructura y recursos, y no necesariamente una amenaza a la vida e integridad de la población."

Sin embargo, aún subsiste un margen entre ambos para poder crear una comparación analítica y certera. Esta es una limitante importante a la hora de hacer el ejercicio de trasladar la aplicación del Derecho internacional de regulación de conflictos desde el mundo predominantemente tangible de los espacios no virtuales al orbe predominantemente intangible del ciberespacio.

A pesar de esta aclaración, ya se han desarrollado mecanismos de adaptabilidad de dichos marcos legales; por ejemplo, el Manual de Tallin desarrollado por la OTAN. Mejía en su estudio parte con la aplicación de la Carta de las Naciones Unidas donde se establece la prohibición de los Estados a usar la fuerza contra otros Estados, con las excepciones autorizadas por el Consejo de Seguridad y en que sea por defensa propia[8].

[7] Ibíd.
[8] Ibíd.

La segunda regulación internacional corresponde a las Leyes de la Guerra, (*Law of Armed Conflict* o LOAC en inglés), condición que establece conceptos de distinción, necesidad y proporcionalidad en cuanto a lo que se considera justo o aceptable en los casos de conflicto armado. Mejía considera una problemática en su aplicación al ciberespacio[9]. Su conclusión se basa en que, al igual que las infraestructuras de movilidad de bienes, servicios y personas (rutas de viaje), el ciberespacio es un objeto de uso doble, es decir, tiene una función militar y una civil[10].

Así como las rutas, carreteras, y vías de movilidad de personas y bienes son usadas para transportar tanto fuerzas armadas (poder militar), como bienes (poder económico) y personas (poder social), las infraestructuras de telecomunicaciones son las autopistas donde fluye la información, tanto militar como civil. Además, considera que debe evaluarse el daño colateral ante miembros y actores no militares al realizar ataques y/o represalias en este ámbito de objetos duales[11]. En síntesis, Mejía establece que el marco legal básico es el siguiente:

• Los Estados generalmente no pueden usar la fuerza contra otros Estados.

• Los Estados pueden usar la fuerza contra otros Estados si:
a. La fuerza está autorizada por el Consejo de Seguridad de la ONU, o si,
b. La fuerza se usa en defensa propia contra un ataque armado por (1) otro Estado o (2) un actor no estatal, si el acto puede ser imputado a un Estado.

• La fuerza se puede usar en defensa propia directamente contra actores no estatales, si el Estado anfitrión no puede evitar los ataques armados de actores no estatales.

• El uso de la fuerza está limitado por los principios de Law of Armed Conflict (LOAC)[12].

Entendiendo este escenario, y las limitaciones de la LOAC, concluye Mejía que es determinante para responder apropiadamente a un ataque en el ciberespacio, requiriendo de un adecuado análisis para identificar quién es el actor (Estado, no Estado, desconocido) y cuál es el acto (*armed attack or not an armed attack*), es decir, atribución del actor y atribución del acto[13].

"...al igual que las infraestructuras de movilidad de bienes, servicios y personas (rutas de viaje), el ciberespacio es un objeto de uso doble, es decir, tiene una función militar y una civil."

De manera general, la atribución del actor es una dificultad mayor. En primer lugar, porque dicho espacio corresponde a una red descentralizada de carácter global que cruza fronteras, siendo de soberanía de muchos Estados. En segundo término, porque a su vez la información circulante es propiedad de infinitos actores, públicos y privados, y la estructura que permite el flujo (infraestructura del ciberespacio) pertenece a múltiples empresas privadas (en inglés *Internet Service Providers*, o por sus siglas ISP). Se observa una complicación ontológica inicial cuando hablamos de las acciones (hostiles o no) en el ciberespacio. Entonces la pregunta es ¿cómo damos atribución a un actor en esta red global?

Mejía cita al académico Nicholas Tsagourias, que a su vez cita al exPresidente de los Estados Unidos, Barack Obama, para concluir:

[9] Ibíd.
[10] Ibíd.
[11] Ibíd.
[12] Ibíd. p. 117.
[13] Ibíd.

"es la naturaleza del acto hostil que detona el derecho a la defensa propia, no la naturaleza del actor"[14]. Ambos autores plantean que existe una distinción inicial en que el acto hostil fuera del ciberespacio tiene mayor capacidad de daño que dentro de esta, por su naturaleza informática y no material de los objetivos de valor[15], pero la solución a esta problemática recayó, en la práctica, en considerar que existen infraestructuras críticas fundamentales para el funcionamiento integral de la sociedad que, de ser atacadas, constituirían un daño sustancial de hostilidad contra la seguridad nacional[16].

" Resulta necesario entonces delimitar, en la institucionalidad jurídica internacional, lo que se considera un ataque cibernético en la misma categoría que un ataque armado a un Estado para la aplicabilidad de las normas existentes."

La discusión transita sobre la aplicación del estándar de ataque hostil armado con daño en el mundo no virtual al virtual, incluso en casos de daño a las infraestructuras críticas (que paraliza servicios básicos y fundamentales de una sociedad), afecta en cierta medida a la determinación de la correcta respuesta a dichos ataques y el marco jurídico internacional que lo rige. En los casos de Estonia el año 2007 y en Georgia del 2008, ninguno de los casos se aplicaron reglamentos de ataque armado[17]. Resulta necesario entonces delimitar, en la institucionalidad jurídica internacional, lo que se considera un ataque cibernético en la misma categoría que un ataque armado a un Estado para la aplicabilidad de las normas existentes.

Esta severidad del ataque es lo que Mejía considera el segundo tipo de atribución, es decir, el tipo referido al acto mismo y su impacto. La atribución del acto, aún no central en la discusión de este artículo, es tan necesaria para poder realizar la toma de decisiones con acciones legítimas a la hora de responder a un ciberataque. El rango de las posibilidades de consecuencias negativas y de destrucción que puede tener un ataque informático es bastante amplia, y esta va a definir entonces una amplia gama de contra respuestas dependiendo del caso a caso.

Por el momento, la Estrategia Internacional para el Ciberespacio de la ONU sí reconoce que un ciberataque puede ser considerado como un acto de guerra, o iniciación de esta, pudiendo aplicarse la normativa internacional ya definida, obviamente con un mayor número de consideraciones a evaluar[18]. Estas se pueden agrupar en: (1) severidad o gravedad, (2) inmediatez, (3) relación directa, (4) invasividad, (5) medibilidad, y (6) legitimidad presunta[19].

En estas seis áreas de evaluación los ataques armados tradicionales presentan bastante claridad respecto de los ciberataques, pero dentro de la evaluación de este último tipo de hostilidad subsiste un rango amplio para definir cuándo un ataque informático es considerado una agresión militar o un intento criminal. Es por esto que el fortalecimiento de sistemas de seguridad defensiva, en las infraestructuras definidas como críticas, es fundamental en el presente, ya que es la primera acción de defensa que los Estados pueden realizar con mayor legitimidad[20].

[14] TSAGOURIAS, N. Cyber Attacks, Self-Defence and the Problem of Attribution. Journal of Conflict and Security Law 17, Nº 2 (Summer 2012) pp. 229-244. [En línea] Disponible en:<http://jcsl.oxfordjournals.org/content/17/2/229.full.pdf+html>

[15] MEJÍA, Loc. Cit; TSAGOURIAS. Loc. Cit.

[16] TSAGOURIAS, Loc. Cit.

[17] Ibid.

[18] MEJÍA. Loc. Cit.

[19] Ibíd.

[20] Ibíd.

Retomando los casos comparativos de la isla de Hawai que Mejía plantea en su análisis, podemos ver pasmado las consideraciones anteriormente señaladas. En el caso de 1941, el ataque es evaluado en torno a las víctimas fatales y, en segundo lugar, el costo de los daños a las infraestructuras materiales de la isla, como la misma base naval Pearl Harbor y los buques que fueron hundidos.

Es decir, hay un costo humano y uno monetario (reconstrucción y reemplazo de los recursos militares perdidos). El daño es material e inmaterial. En el segundo caso, el daño es intangible si consideramos que fue una pérdida de dinero para la institución bancaria, así como lo son los asaltos a bancos y cajeros (pero de mayor envergadura). El primero es claramente materia de guerra, y el segundo es materia de crimen. En estos dos casos distintos responden a mecanismos y organismos de ejecución diferentes ligados a la seguridad y defensa.

Un ciberataque puede ser militar o puede ser criminal, dependiendo nuevamente de la similitud del acto hostil con lo ya definido en los marcos jurídicos nacionales e internacionales, es decir, con el rango de severidad y daño de dicho acto hostil. Sin embargo, obviamente existe la posibilidad de casos híbridos, donde el continuo y constante ataque de carácter criminal reiterado podría llegar a constituirse como militar, si a la larga el daño a las infraestructuras críticas termina siendo destructivo[21].

Cuando hablamos, entonces, del tipo de atribución asociado a la severidad del acto y cómo esta define el tipo de respuesta, esta última debe estar concebida de manera proporcional al ataque inicial, que sin duda no es un cálculo de fácil realización y dependerá de la particularidad de cada caso. La definición de mecanismos internacionales de cálculos para esta tarea de los aparatos de inteligencia y defensa nacional es una óptima forma para simplificar, estandarizar y regular la legitimidad de las respuestas en el ciberespacio.

“Un ciberataque puede ser militar o puede ser criminal, dependiendo nuevamente de la similitud del acto hostil con lo ya definido en los marcos jurídicos nacionales e internacionales,...”

Anonimato y atribución al actor

El problema del anonimato surge principalmente porque el ciberespacio, en su esquema original, no fue concebido con el propósito de identificar cada una de las partes de la comunicación de manera exhaustiva. “Las redes de computadoras no están diseñadas para facilitar la atribución, y los actores hostiles explotan esta debilidad para ocultar su verdadera identidad”, señala Mejía, donde en Internet no se usa o se prioriza típicamente la identificación del emisor en el proceso comunicacional[22].

La discusión se constituye en torno a la manera como se responde, pero fundamentalmente la cuestión radica, en última instancia, sobre la dirección de la respuesta. En palabras de Tsagourias, “la atribución es, por lo tanto, crítica, pero es un ejercicio muy exigente y complicado en el contexto de los ataques convencionales, como lo demuestra el caso del terrorismo, y más aún en el caso de los ciberataques, debido a la naturaleza del dominio cibernético”[23].

Lo que quiere decir con dimensión del ciberespacio, es que el Internet no se formuló bajo una lógica de futuro basado en la necesidad de determinar quién es el emisor de la información. El objetivo central fue hacer las

[21] Ibíd.
[22] Ibíd. p. 121.
[23] TSAGOURIAS. Op. Cit. p. 233.

comunicaciones de la época más resilientes, en el contexto de la Guerra Fría y en respuesta al miedo de la Destrucción Mutua Asegurada (MAD por sus siglas en inglés)[24]. De esta manera poder afrontar y sobrevivir un ataque nuclear u otro tipo de destrucción, manteniendo intacta la capacidad del sistema de comando y control[25].

Por otro lado, el proyecto antecesor a Internet, ARPANET, fue desarrollado por académicos e investigadores que pretendían crear una red de comunicaciones resistente a los avances e innovaciones tecnológicas del futuro, por ende concentrándose únicamente en que dicha red enviara el mensaje de la manera más eficiente posible, independiente del contenido[26].

De esta forma se implementó el protocolo de conmutación de paquetes (o *packet-switch* en inglés), utilizado hasta hoy, para que la totalidad del mensaje se dividiera en partes para viajar por diferentes rutas pero al mismo destino[27]. Este y otros protocolos, como la versión original del SMTP (*Simple Mail Transfer Protocol*) no fueron diseñados para verificar autenticidad del emisor del correo, principalmente porque los ingenieros poseían vínculos de confianza[28]. Lo que en otras palabras quiere decir que los protocolos que conforman el "ADN del internet" permiten y favorecen la anonimidad en las comunicaciones[29].

Tsagourias menciona tres características particulares del ciberespacio que hacen que la atribución sea extremadamente difícil:

> "El primero es el "anonimato" en que los atacantes pueden ocultar su identidad; la segunda es la posibilidad de lanzar ciberataques de múltiples etapas, ya que una cantidad de computadoras operadas por diferentes personas y ubicadas en diferentes jurisdicciones se infiltran antes de que se lance un ataque; y el tercero es la velocidad con la que se puede materializar un ciberataque" [30].

"El resultado fue el desarrollo del Manual de Tallin en manos de la OTAN que buscaba dar lineamientos sobre cómo aplicar la normativa internacional de conflictos armados al ciberespacio;..."

El estudiado incidente de Estonia del año 2007 materializa estas tres dificultades: 85 mil computadoras en 178 países fueron secuestradas para efectuar un ataque de tipo *DDoS*[31]. El resultado fue el desarrollo del Manual de Tallin en manos de la OTAN que buscaba dar lineamientos sobre cómo aplicar la normativa internacional de conflictos armados al ciberespacio; sin embargo, esto no ha resultado una tarea sencilla en la práctica para generar habilidades de Defensa y Seguridad legítimas alrededor del globo, y aún resulta necesario seguir trabajando en esta materia. Y principalmente porque el anonimato confiere un desafío en el ámbito de lo técnico, político y legal[32]. La problemática tecnológica ya fue desplegada en torno a la naturaleza anónima de los protocolos básicos de las vías de flujo de la información en la red.

[24] NAUGHTON, J. The evolution of the Internet: from military experiment to General Purpose Technology, Journal of Cyber Policy, 1:1, 5-28, 2016. [En línea] Disponible en:<https://www.tandfonline.com/doi/pdf/10.1080/23738871.2016.1157619?needAccess=true>

[25] Ibíd.

[26] Ibíd.

[27] Ibid.

[28] Ibíd.

[29] ISAACSON, W. How to Fix the Internet: Anonymity has poisoned online life. The Atlantic, Technology. 15 diciembre 2016. [En línea] Disponible en:<https://www.theatlantic.com/technology/archive/2016/12/how-to-fix-the-internet/510797/>

[30] TSAGOURIAS, Op. Cit. p. 233.

[31] Ibíd.

[32] Ibíd.

En cuanto al entorno político, la evaluación de relaciones de poder entre diversos actores es fundamental para, al menos, identificar una lista de posibles sospechosos. En el caso de Estonia se pudo establecer con un grado de certeza técnica mínima y con mayor grado de certeza política, que los ataques habrían sido perpetrados desde Rusia. Sin embargo, de acuerdo a la falta de institucionalidad en el Derecho internacional, poco pudo hacerse excepto focalizar los esfuerzos para la protección pasiva y no en defensa activa.

Esta distinción recae en que la defensa pasiva implica "medidas adoptadas para reducir la probabilidad de minimizar efectos en cuanto al daño causado por una acción hostil, sin la intención de tomar la iniciativa"[33]. Tampoco es necesario tener claridad de la identidad de un enemigo para efectuarla, si no que al menos la idea de que existe un enemigo potencial. Este tipo de defensa apunta entonces a fortalecer las barreras de protección e integridad de las comunicaciones del ciberespacio.

Por otra parte, la defensa activa hace referencia a "la implementación de acciones ofensivas limitadas y contraataques para denegar un área contestada o posición del enemigo"[34]. Se requiere reconocer, al menos, la identidad del perpetuador para contratacar de manera legítima al actor que corresponda. En este escenario existen dos formas de contrataque, uno de carácter mitigante y otro de tipo retributivo: el primero, hace alusión a usar solo la fuerza necesaria para proteger un sistema, mientras que el segundo alude a castigar al atacante[35]. Según señala Mejía, en Derecho internacional solo el primer tipo de defensa activa es realmente defensivo[36], mientras que el segundo pasa a ser ofensivo.

Las dificultades que presenta la determinación de atribución que genera el anonimato en el dominio cibernético, incentiva la supervigilancia de manera preventiva frente a potenciales fuentes de agresiones en el espacio virtual. Y la cuestión de vigilancia, indudablemente, supera las limitantes técnicas al problema de atribución, pero incrementa el enfoque estatal. Aquí la discusión en torno a la relación "seguridad versus privacidad" se torna en una discusión de índole político, en donde los diversos tipos de actores tendrán diferentes intereses para sacrificar una variable (seguridad o libertad) en pro de fortalecer la otra (libertad o seguridad).

"Las dificultades que presenta la determinación de atribución que genera el anonimato en el dominio cibernético, incentiva la supervigilancia de manera preventiva frente a potenciales fuentes de agresiones en el espacio virtual."

En materia de buscar y asignar atribuciones, la recopilación de evidencia resulta esencial; sin embargo, en el ciberespacio resulta engorroso obviamente dada la naturaleza. En cuanto siga siendo la red troncal del Internet propiedad de múltiples empresas privadas, que cruzan distintas jurisdicciones (de distintos Estados), y que los titulares de la información sean múltiples y diferentes actores, adicionalmente a su carácter anónimo de la transmisión, la recopilación de evidencia es suficientemente compleja[37].

[33] MEJÍA. Op. Clt. p. 120.
[34] Ibíd. p. 120.
[35] Ibíd.
[36] Ibid.
[37] TSAGOURIAS. Loc. Cit.

No existe en el Derecho internacional estándares específicos de pruebas en asuntos que involucran la defensa y la autodefensa, generando un problema de probidad de la evidencia[38]. Sin embargo, sí se podrían aplicar los criterios utilizados en las cortes criminales y civiles para determinar distintos grados de subjetividad de testimonios desplegados para acusar a un actor, se puede establecer relativa certeza para imputar acciones a observados actores, de acuerdo a lo que plantea Mejía[39]. Tsagourias argumenta que en la práctica es más subjetivo, ya que al ser la evidencia casi puramente producto de los esfuerzos de inteligencia, que suelen ser confidenciales, difícilmente son solicitados por tribunales como lo ocurrido con el genocidio Bosnio en la Corte Internacional de Justicia[40].

Es evidente que el problema de atribución resulta una dificultad para la aplicabilidad del Derecho internacional en casos de ciberataques. En palabras de Tsagourias:

> "De lo anterior se desprende que las normas relativas a la disponibilidad y la probidad de la evidencia en casos de ataques armados, usos de la fuerza o intervenciones son bastante laxas y lo son aún más en el caso de los ataques cibernéticos debido a sus características particulares como se mencionó anteriormente. Dicho esto, incluso si el estándar de prueba no es el mismo que el requerido para el enjuiciamiento penal de individuos e incluso si "un enfoque más político de la atribución... podría aceptar estándares menos exigentes", cabe destacar que un Estado no debe recurrir a la legítima defensa sobre la base de pruebas casuales o inferencias políticas descabelladas"[41].

En otras palabras, la dificultad de determinar la atribución a actos hostiles en el ciberespacio es alta, y la tentación política a justificar actos de defensa, sin legitimidad jurídica, es también alta. La incertidumbre que provocan los ciberataques es tal que resulta necesario principalmente reducir la posibilidad y viabilidad de contrataques como formas defensivas; en consecuencia, sería prudente concentrar los esfuerzos en aumentar los niveles de seguridad y defensa de infraestructuras críticas esenciales. Este mecanismo resulta el más legítimo de la defensa pasiva, y evita entrar en la discusión política sobre "seguridad" y "privacidad" que sostiene la vigilancia.

"En otras palabras, la dificultad de determinar la atribución a actos hostiles en el ciberespacio es alta, y la tentación política a justificar actos de defensa, sin legitimidad jurídica, es también alta."

Resulta necesario recordar que el ciberespacio, como las ya señaladas palabras de Mejía, es de uso doble u objetivo doble, condición que no solo abarca lo militar, si no que civil también, por ende, el mecanismo de vigilancia en pro de la seguridad tiene como efecto colateral la privacidad de los ciudadanos. India es un ejemplo en tanto ya ha desarrollado e implementado varias tecnologías (cámaras de seguridad y reconocimiento facial) que en su conjunto constituyen, de acuerdo a sus críticos, en un sistema de seguridad digital estatal que ha permitido identificar niños perdidos pero, a su vez, constituir un sistema de supervigilancia masiva con más de 90% de su población registrada en un único sistema de reconocimiento facial[42].

[38] Ibíd.

[39] MEJÍA. Loc. Cit.

[40] TSAGOURIAS. Loc. Cit.

[41] Ibíd. p. 235.

[42] DATTA, S. & SINGH, K. A creeping surveillance net over India: Government surveillance measures and laws lack protection for citizen's rights. Asia Times, 27 julio 2019. [En línea] Disponible en:<https://www.asiatimes.com/2019/07/article/a-creeping-surveillance-net-over-india/>; DEVLIN, H. 'We are hurtling towards a surveillance state': the rise of facial recognition technology. The Guardian, Technology, Facial Recognition, 5 octubre 2019. [En línea] Disponible en:<https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state>

En conclusión, Mejía determina que es fundamental determinar la atribución del actor en casos de ciberataques y que la evidencia técnica es necesaria para fortalecer las conclusiones subjetivas[43]. Obviamente esa evidencia técnica debe estar enfocada en fortalecer y mejorar los protocolos de identificación de mensajes (esfera técnica), pero el excesivo esfuerzo en esta materia podría llevar a una supervigilancia que se debe delimitar para mantenerse en la órbita de una legitimidad mínima (esfera política) y dentro de las posibilidades jurídicas (esfera jurídica).

Es necesario determinar, recalcar y no olvidar que la ventaja comparativa que tienen las agresiones informáticas por sobre un ataque tradicional (como el realizado a la base Pearl Harbor) es el anonimato: "ningún actor hostil, ya sea un Estado-nación o un individuo deshonesto, será disuadido de la actividad cibernética hostil si puede negar efectivamente la responsabilidad"[44]. Por otro lado, como los ciberataques hasta ahora no suponen un impacto de daño de la misma envergadura que un ataque tradicional, la legitimidad de una respuesta siempre será considerablemente menor; por ende, un contrataque ofensivo supone una respuesta ínfimamente válida tanto para la sociedad global (esfera política) como para la institucionalidad del Derecho internacional (esfera jurídica).

Resulta necesario acotar que la conclusión final de Mejía es el llamado a desarrollar una convergencia entre los expertos jurídicos, que manejan el arte de la atribución de crímenes y hostilidades, inherente a cualquier práctica del Derecho, y los expertos técnicos que manejan de mejor manera los protocolos y los metadatos (datos sobre la información)[45].

Sin embargo, hasta el momento hemos analizado la atribución asumiendo que los Estados solo pueden cometer actos hostiles de manera directa, es decir, dentro de una toma de decisiones de miembros que lo representan y su estructura, y que son efectuados con recursos estatales. En palabras de Tsagourias:

> "A partir del derecho y la práctica internacionales, se pueden identificar tres estándares principales de atribución: según el primero, los ataques de los órganos estatales se atribuyen a ese Estado; de acuerdo con los segundos ataques de agentes estatales, es decir, las entidades instruidas, dirigidas o controladas por un Estado se atribuyen a ese Estado; y según el tercero, los ataques de entidades toleradas por un Estado se atribuyen a ese Estado. En todos los casos anteriores, se pueden tomar medidas de autodefensa contra el Estado implicado. Si nada de lo anterior se aplica pero un actor no estatal ataca a otro Estado, ese actor no estatal se convierte en el objetivo directo de la acción de defensa propia"[46].

Esta definición de limitaciones, a la hora de efectuar un contrataque, es aquella misma que se aplica para casos de terrorismo, donde difícilmente se puede vincular con un alto grado de certeza una acción hostil a un Estado en particular, e incluso a un grupo terrorista que se ha adjudicado dicho acto.

En el derecho internacional actual, para el caso de actos hostiles atribuibles al Estado y sus órganos pueden estar bajo una atribución de "*jure o de facto*". El primero, se refiere a cuando el actor hostil es un grupo u órgano que por ley es parte del aparato estatal, mientras que el segundo es cuando existe (y se puede demostrar) un alto nivel de control del Estado por sobre dicho grupo, a pesar de que no se constituye por derecho dicha relación[47]. El grado

[43] MEJÍA. Loc. Cit.
[44] Ibíd. p.129.
[45] Ibíd.
[46] TSAUGOURIAS. Op. Cit. p. 236.
[47] Ibíd.

de dependencia debe ser alto, de lo contrario no podría constituirse una atribución de *facto*[48]. Existen casos de relativa dependencia de una agencia o un grupo hostil con el aparato estatal, pero prevalece la evidencia que la orden provino de un Estado en particular o agencia con dependencia de este. En esta condición se habla de una relación "*ad hoc*" y debe ser probada la reciprocidad entre un grupo y el Estado[49].

En el derecho internacional se observa un precedente y fue establecido en el antiguo Tribunal Penal Internacional para la ex Yugoslavia, Corte que indicó una distinción en caso de individuos y grupos no organizados de los organizados. Para el primer caso, el estándar de evaluación del control del Estado debe ser mayor que en el caso del segundo. En otras palabras, para el asunto de individuos o grupos no organizados debe haber una orden explícita de ataque (control efectivo), mientras que para el segundo se estimaría solo algún grado de financiamiento, equipamiento o asesoramiento de la planificación de su actividad militar (control general)[50]. Este tipo de materia difiere de la relación de *facto* principalmente porque no se evidencia un grado de dependencia con el Estado[51].

Un ataque en la dimensión del ciberespacio correspondería hacer responsable a un Estado cuando este ejerce control general sobre un grupo organizado de *hackers* o *hacktivistas*, o cuando exista una intervención efectiva del aparato estatal sobre ellos. Sin embargo, los precedentes revisados en la Corte Internacional de Justicia, hoy en operación, señalan que solo actos realizados por "entidades bajo el control efectivo" del Estado pueden ser atribuidos a este[52].

"Un ataque en la dimensión del ciberespacio correspondería hacer responsable a un Estado cuando este ejerce control general sobre un grupo organizado de *hackers* o *hacktivistas*, o cuando exista una intervención efectiva del aparato estatal sobre ellos."

Es necesario aclarar que los criterios establecidos en ambas Cortes se refieren a casos de violación a la ley internacional humanitaria[53], y de acuerdo a las categorizaciones de Mejía, la atribución del daño (envergadura del daño efectuado por el ciberataque) no resulta suficiente para ser comparables ni aplicable de igual manera. Hasta el momento no existe suficiente desarrollo e innovación tecnológica, dependencia a la digitalización, ni completa fusión de la vida humana con el ciberespacio para poder generar un genocidio a través de un ataque informático. Incluso en los casos de genocidio, los tribunales han determinado que el control general resulta demasiado amplio como criterio para atribuir responsabilidad al aparato estatal[54].

Sin embargo, se evalúa también que está en el "*ethos*" del Estado su monopolio exclusivo de la fuerza, y que al no poder ejercer plenamente su autoridad sobre el territorio y control de amenazas por grupos no estatales internos, el Estado víctima puede atacar directamente al actor no estatal hostil[55]. Aquí se aplica principalmente la tradición e institucionalidad

[48] Ibíd.
[49] Ibíd.
[50] Ibíd.
[51] Ibíd.
[52] Ibíd.
[53] Ibíd.
[54] Ibíd.
[55] Ibíd.

del derecho internacional referida a los grupos terroristas, como el argumento de defensa propia que efectuó Israel en 2006 al atacar al grupo Hezbolá en el Líbano, porque este último no pudo prevenir dichos ataques[56].

Tsagourias plantea que, según el propósito que persigue la fuente de las normativas internacionales, que es mantener la paz, resulta contraproducente que se determine un marco y tradición jurídica que proteja a los actores no estatales y sus agresiones atribuidas a la condición de no Estado[57].

Bajando el análisis entonces a los grupos no estatales hostiles que poseen poca relación con una institución estatal que los aloja, ya sea voluntariamente o involuntariamente, la tradición y marcos aplicados para los casos de terrorismo a partir de la destrucción de las Torres Gemelas en 2001, muestran lineamientos en esta materia, respaldados por las sentencias del Consejo de Seguridad[58]. En estos casos existen suficientes precedentes para poder efectuar un acto de defensa propia.

A partir del reconocimiento establecido por el derecho internacional, al menos, se evidencia un lineamiento mínimo para determinar cuándo son legítimos los contrataques defensivos basado en la naturaleza de los actores. Queda esclarecido que, difícilmente, un Estado pueda llevar a cabo un ataque directo utilizando virus cibernéticos, y que principalmente son actores no estatales los que llevan a cabo estas acciones, utilizando la fachada o relación con otro Estado. También se puntualiza que el anonimato es favorable para actores hostiles, y por ende esfuerzos entre lo técnico, lo político y lo judicial deben desplegarse para fortalecer la identificación de las partes de la comunicación, sin violar la privacidad del contenido de la información.

“En el mundo virtual es la integridad y privacidad de la información que se ve amenazada y que dependiendo de la importancia de esta se determinará la legitimidad de una respuesta defensiva del Estado víctima.”

La legislación internacional revisada en este trabajo al referirse a la atribución del acto de agresión, hace referencia a casos de hostilidades y violencia contra la vida de personas y no contra la información que circula en el ciberespacio. En el mundo no virtual la violencia extrema puede provocar la muerte, y es esa condicionante la que se evalúa y sustenta la institucionalidad de seguridad y paz en el escenario internacional. En el mundo virtual es la integridad y privacidad de la información que se ve amenazada y que dependiendo de la importancia de esta se determinará la legitimidad de una respuesta defensiva del Estado víctima.

Por esta razón el principal mecanismo para proteger las infraestructuras básicas y fundamentales para un normal y correcto funcionamiento de la vida en sociedad (y por ende mantener la paz), es la defensa pasiva. De esta forma se busca mejorar y mantener un estándar mínimo de seguridad técnica en los sistemas y estructuras informáticas de dichos servicios básicos.

Analizando el impacto que alcanza un ataque hostil no virtual versus un ciberataque, se produce un abismo considerable para que el derecho internacional humanitario sea cabalmente aplicado. Dicho esto, existen dos

[56] Ibíd.
[57] Ibíd.
[58] Ibíd.

formas por las cuales un Estado se puede ver amenazado en el ciberespacio: el primero, es el espionaje y, el segundo, la destrucción de la infraestructura crítica[59].

El espionaje y el ciberespionaje en la actualidad son prácticamente lo mismo. Sostengamos que la digitalización es un proceso global necesario, y por ende la información de alta sensibilidad de los Estados se encuentra transcrita en *bits* y *bytes*, conectada a algún tipo de red privada, que puede ser interceptada por algún individuo (en nombre del Estado o no) con capacidad y conocimiento informático suficiente para realizar dicha disrupción. Este tipo de ataque, entonces, debe considerarse dentro de los paradigmas del espionaje clásico, y lo podemos constatar en las declaraciones de Edward Snowden, al referirse al espionaje y vigilancia masiva realizado por Estados Unidos[60], ningún Estado lo ha considerado como un ataque hostil para contratacar al gobierno norteamericano. Las infraestructuras críticas, que en caso de mal funcionamiento pueden generar caos, y de ser agredidas, podrían causar daño vital o a la corporalidad de la población de un Estado.

"... un Estado puede y debe fortalecer las defensas de sus infraestructuras críticas para la seguridad nacional, y contar con equipos de respuesta para aminorar los daños y reestablecer los servicios."

Otras consideraciones

Es así como Hare plantea las mismas problemáticas asociadas a la atribución en el ciberespacio en diversa literatura, y que concluye al igual que este trabajo, que resulta clave tener una claridad de quién es el perpetuador de un ataque para poder realizar una defensa legítima de acuerdo a la institucionalidad jurídica internacional[61]. Sin embargo, Hare replantea la problemática más que determinar caminos para la respuesta, focaliza que los esfuerzos deben ir a cómo hacer que los ataques que ya se han hecho no puedan volver a ocurrir[62].

En el caso del espionaje, como requiere que la información que está siendo interceptada llegue a un tercero, aquí se podría desarrollar una capacidad técnica en el Estado para poder perseguir dicho flujo de información a su origen y así recopilar evidencia que sustentaría la atribución del ciberespionaje[63]. En el caso del daño a la infraestructura crítica, el incidente de Estonia del año 2007 sigue siendo fuente de inspiración para obtener lecciones aprendidas. En principio, debe de generarse desarrollo de Seguridad y Defensa pasiva técnica a las infraestructuras críticas[64] de manera proactiva y no reactiva, con sistemas de apoyo eficientes que puedan minimizar el daño ocurrido, y para poder reestablecer el normal funcionamiento de servicios afectados.

En otras palabras, un Estado puede y debe fortalecer las defensas de sus infraestructuras críticas para la seguridad nacional, y contar con

[59] HARE, F. The Significance of Attribution to Cyberspace Coercion: A Political Perspective. NATO CCD COE Publications, 4th International Conference on Cyber Conflict, 2012, Tallin. [En línea] Disponible en:<https://ccdcoe.org/uploads/2012/01/2_5_Hare_TheSignificanceOfAttribution.pdf>

[60] THE ECONOMIST. Big Brothers: Edward Snowden's memoir reveals some (but not all). The Economist, Books and Arts, 13 septiembre 2019. [En línea] Disponible en:<https://www.economist.com/books-and-arts/2019/09/13/edward-snowdens-memoir-reveals-some-but-not-all?cid1=cust/dailypicks1/n/bl/n/20190913n/owned/n/n/dailypicks1/n/n/LA/308551/n>

[61] HARE. Loc. Cit.

[62] Ibíd.

[63] Ibíd.

[64] Ibíd.

equipos de respuesta para aminorar los daños y reestablecer los servicios. Sin embargo, "sin atribución, los atacantes carecen de disuasión"[65], esto ya que:

> "En el mejor de los casos, los sistemas seguros aumentan la cantidad de tiempo que le toma a un atacante encontrar una vulnerabilidad a un punto más allá de lo que el atacante está dispuesto a pasar. Sin los incentivos adecuados para restringir el comportamiento del atacante malicioso, ya sea estatal o no estatal, no es razonable esperar que la situación actual cambie"[66].

Se debe considerar que existen tres niveles de atribución: máquina, operador humano, y partido (actor político directamente beneficiario) responsable[67]. Revisamos que se cuenta con capacidad técnica para identificar, al menos, la máquina de la cual procede el ataque, mientras que para el operador humano y partido responsable la capacidad técnica no alcance y requiere de asistencia del análisis político y lineamientos del recurso jurídico para determinar algún grado de atribución.

La evidencia que detona el vínculo entre el computador y el perpetuador se sintetiza en "lenguaje común, actividad durante horas específicas, objetivos de blanco elegidos, y el nivel de la complejidad del ataque"[68].

Por otro lado, de acuerdo a un estudio realizado entre 2016 y 2018, entre 70% y 85% de incidentes de ciberataques que vieron la luz pública, fueron públicamente adjudicados a algún actor, y en ningún caso existe una forma sistémica y establecida de establecer atribución, muchos de los que tampoco existe una estandarización de evaluación de pruebas y evidencia[69]. En similitud con la proliferación de armamento nuclear, Mueller et al proponen la creación de una especie de Organismo Internacional de Energía Atómica, que sirva específicamente para determinar parámetros y, por ende, resultados a la hora de establecer atribución de ataques informáticos, y que esta sea de manera independiente a los intereses políticos de los Estados, sea víctima o victimario[70].

> "La Organización Internacional de Atribución propuesta en el Convenio Digital de Ginebra de Microsoft, y su posterior articulación, es una de esas propuestas. Esta propuesta incluía un lenguaje que sugería que una organización de atribución independiente debería 1) abarcar el sector público y privado al tiempo que incluye a la sociedad civil y la academia 2) investigar y cumplir un rol de intercambio de información y 3) parecerse a la Agencia Internacional de Energía Atómica (OIEA). La propuesta inicial contenía una ambigüedad significativa en cuanto a si esto describe un modelo multilateral o de múltiples partes interesadas"[71].

Este modelo, aun cuando habría detalles que determinar, resulta más atingente para resolver el problema de atribución considerando que son acciones que usan espacios de doble uso, militar y civil, donde la vigilancia extrema genera daño colateral civil a la hora de utilizarse para consolidar la certeza de una atribución, además de poder tener una imparcialidad necesaria en la instancia de evaluar políticamente las responsabilidades de dichos actos y los actores sospechosos.

[65] MUELLER, M., GRINDAL, K., KUERBIS, B. & BADIEI, F. (2019). Cyber Attribution: Can a New Institution Achieve Transnational Credibility? The Cyber Defense Review, 4(1), 107-122. [En línea] Disponible en:<https://www.jstor.org/stable/26623070>

[66] Ibíd. p. 108.

[67] LIN, H. Attribution of Malicious Cyber Incidents: From Soup to Nuts. SSRN Scholarly Paper, Rochester, NY: Social Science Research Network, 2 septiembre 2016. En: MUELLER et al. op. cit. p.108

[68] MUELLER "et. al." Op. Cit. p. 109

[69] Ibíd.

[70] Ibíd.

[71] Ibíd. p. 111.

Finalmente, es necesario profundizar el debate entre vigilancia y privacidad en relación a la protección de los civiles y sus vínculos con las comunicaciones, sobre todo cuando consideramos que existe una mayor penetración de Internet que libertad democrática a nivel global[72]. Las preocupaciones sobre el abuso de la tecnología para controlar a la población, ya sea en nombre de la seguridad o algún bien público (legítimo o no), está en la agenda de la opinión pública y es necesario considerar este aspecto a la hora de poder estimar correctamente la legitimidad de acciones hostiles o contrataques en el ciberespacio.

"Resulta necesario combinar las perspectivas de la seguridad nacional, así como la seguridad del régimen democrático a la hora de determinar parámetros internacionales para la seguridad del ciberespacio y minimizar posibles ciberataques."

Para muchos, el ciberespacio ha permitido el empoderamiento de la sociedad en su aspecto general para poder constituir fuera de la persecución del Estado una disidencia contra regímenes autoritarios[73]. Se entendía que la globalización de las comunicaciones y su misma capacidad, anónimamente, iba a permitir que se esparciera el "virus" democratizador a regímenes autoritarios o totalitarios que permitieran, por diversas razones, la penetración del Internet. Sin embargo, actualmente, dichos regímenes han sabido sostener el poder y extender formas de control al ciberespacio.

El presidente de Freedom House, Michael J. Abramowitz, señala en el último informe sobre libertad en la red que "China está exportando su modelo de censura y vigilancia para controlar la información dentro y fuera de sus fronteras"[74]. En otras palabras, el acceso a la red les entrega a los ciudadanos la capacidad de potenciar las libertades así como a los regímenes autoritarios expandir su poder, es decir, puede "alimentar democracias como desestabilizar dictaduras"[75].

Resulta necesario combinar las perspectivas de la seguridad nacional, así como la seguridad del régimen democrático a la hora de determinar parámetros internacionales para la seguridad del ciberespacio y minimizar posibles ciberataques.

Un régimen internacional de derecho que establezca criterios de atribución bajo por un lado permitiría el abuso de las declaraciones y retóricas políticas y un estado de violencia mayor al validar mayormente acciones de defensa activa y contrataque, incrementando la inseguridad en el ciberespacio. Un régimen internacional de derecho que establezca criterios de atribución alta, por otro lado, permitiría el abuso del anonimato por grupos que podrían ser legítimos o ilegítimos, si se observan desde la valoración de la democracia y los derechos humanos. Esto último lo determinaría la naturaleza del régimen del Estado víctima, y los principios morales de los grupos disidentes que perpetúan el atraco, tensando entonces la esfera política de la discusión sobre el anonimato en el ciberespacio.

[72] FREEDOM HOUSE (a). Freedom in the World 2018: Democracy in Crisis. 2019. [En línea] Disponible en:<https://freedomhouse.org/report/freedom-world/freedom-world-2018>; INTERNET WORLD STATS. Usage and Population Statistics. [En línea] Disponible en:<https://internetworldstats.com/stats.htm>

[73] BREMMER, I. Democracy in Cyberspace: What Information Technology Can and Cannot Do. Foreign Affairs, Noviembre/Diciembre 2010. [En línea] Disponible en:<https://www.foreignaffairs.com/articles/2010-10-21/democracy-cyberspace>

[74] FREEDOM HOUSE (b) Freedom on the Net: The Rise Of Digital Authoritarianism. 2019. [En línea] Disponible en:<https://freedomhouse.org/report/freedom-net/freedom-net-2018>

[75] bíd.

Finalmente, una evaluación del orden global actual es necesario. Observamos potencias mundiales reconocidas por su violación a los derechos humanos mínimos, ya sea dentro o fuera del ciberespacio, e instituciones como Freedom House que fundamentan que la democracia y las libertades en el mundo virtual y no virtual han ido disminuyendo en los últimos años[76].

Como ya se ha señalado, países como China e India han optado por la vigilancia como mecanismo de defensa pasiva ante inseguridades y amenazas dentro y fuera de la red. En muchos casos con considerable cuestionamiento a la protección de los derechos humanos. Otros Estados, como Rusia, han sabido integrar el ciberespacio y sus ventajas con un realismo considerable en sus estrategias globales de seguridad[77], como por ejemplo, hacer vista gorda a su gran cultura hacker[78]. Por otro lado, Estados Unidos frente al caso de Google Analytica y el de Edward Snowden no tiene mucho que envidiar a los mencionados, a pesar de su aparente salud democrática.

Conclusiones

Ya expuestas diversas consideraciones que se enmarcan en lo jurídico, lo político y lo técnico sobre el problema de atribución en el ciberespacio, es necesario determinar en primeria instancia que cualquier régimen jurídico que se establezca debe de tener el foco del objeto a asegurar es el individuo civil y sus derechos y libertades humanas establecidas por la Carta de Derechos Humanos de la Organización de las Naciones Unidas, respetando los principios liberales.

Resulta necesario fortalecer, desde lo técnico, las capacidades preventivas de las infraestructuras críticas para evitar abusar de mecanismos de supervigilancia masiva con el pretexto de la seguridad nacional. Ante esto, el derecho internacional humanitario en relación a la atribución de un acto hostil no virtual aplicado al ciberespacio es el primer paso hacia un espacio virtual seguro; sin embargo, el establecimiento y apoyo de una agencia independiente internacional que establezca mecanismos imparciales de asignación de atribución a casos de ciberataques sería plausible.

Bajo estos parámetros nos encontramos con una principal dificultad, y es que no habría, en una evaluación preliminar, voluntad política de los “Estados Potencia” para generar mecanismos y estrategias de seguridad del ciberespacio y sus infraestructuras críticas que protejan la privacidad de su población.

Finalmente, se postula por apoyar a las fuerzas políticas, jurídicas y técnicas para que tengan en consideración que el hacer del ciberespacio constituya un lugar seguro, así como un espacio de libertades, para poder discernir entre los actores y la magnitud e intencionalidad de sus actos: autonomía para separar aquellos casos de ciberataques que buscan, por ejemplo, apoyar un grupo disidente en un régimen totalitario o bien de un grupo terrorista que busca incitar violencias en regímenes democráticos. Esta última distinción, aunque suene contraproducente desde un punto de vista jurídico, violando la igualdad ante la ley, en la práctica resulta absolutamente necesario sobre todo si la democracia, la seguridad internacional y la protección de las libertades humanas y civiles se quiere proteger en el ciberespacio.

[76] FREEDOM HOUSE. Op. Cit. (a) y (b).

[77] WIRTZ, J.J. Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. Capítulo 3 en GEER, K. (ed.) Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications, Tallin, 2015. [En línea] Disponible en:<https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf>

[78] MCDOUGAL, T. Establishing Russia’s Responsibility for Cyber-Crime Based on Its Hacker Culture, 11 BYU Int’l L. & Mgmt. R. 55, 2015. [En línea] Disponible en:<https://digitalcommons.law.byu.edu/ilmr/vol11/iss2/4>

Bibliografía

BREMMER, I. Democracy in Cyberspace: What Information Technology Can and Cannot Do. Foreign Affairs, Noviembre/Diciembre 2010. [En línea] Disponible en:<https://www.foreignaffairs.com/articles/2010-10-21/democracy-cyberspace>

DATTA, S. & SINGH, K. A creeping surveillance net over India: Government surveillance measures and laws lack protection for citizen's rights. Asia Times, 27 julio 2019. [En línea] Disponible en:<https://www.asiatimes.com/2019/07/article/a-creeping-surveillance-net-over-india/>

DEVLIN, H. 'We are hurtling towards a surveillance state': the rise of facial recognition technology. The Guardian, Technology, Facial Recognition, 5 octubre 2019. [En línea] Disponible en:<https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state>

FREEDOM HOUSE (a). Freedom in the World 2018: Democracy in Crisis. 2019. [En línea] Disponible en:<https://freedomhouse.org/report/freedom-world/freedom-world-2018>

FREEDOM HOUSE (b) Freedom on the Net: The Rise Of Digital Authoritarianism. 2019. [En línea] Disponible en:<https://freedomhouse.org/report/freedom-net/freedom-net-2018>

HARE, F. The Significance of Attribution to Cyberspace Coercion: A Political Perspective. NATO CCD COE Publications, 4th International Conference on Cyber Conflict, 2012, Tallin. [En línea] Disponible en:<https://ccdcoe.org/uploads/2012/01/2_5_Hare_TheSignificanceOfAttribution.pdf>

INTERNET WORLD STATS. Usage and Population Statistics. [En línea] Disponible en:<https://internetworldstats.com/stats.htm>

ISAACSON, W. How to Fix the Internet: Anonymity has poisoned online life. The Atlantic, Technology. 15 diciembre 2016. [En línea] Disponible en:<https://www.theatlantic.com/technology/archive/2016/12/how-to-fix-the-internet/510797/>

MCDOUGAL, T. Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker Culture, 11 BYU Int'l L. & Mgmt. R. 55, 2015. [En línea] Disponible en:<https://digitalcommons.law.byu.edu/ilmr/vol11/iss2/4>

MEJIA, E. Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework. Strategic Studies Quarterly, 8(1), pp.114-132, Primavera 2014. [En línea] Disponible en:<http://www.jstor.org/stable/26270607>

MUELLER, M., GRINDAL, K., KUERBIS, B., & BADIEI, F. (2019). Cyber Attribution: Can a New Institution Achieve Transnational Credibility? The Cyber Defense Review, 4(1), 107-122. [En línea] Disponible en:<https://www.jstor.org/stable/26623070>

NAUGHTON, J. The evolution of the Internet: from military experiment to General Purpose Technology, Journal of Cyber Policy, 1:1, 5-28, 2016. [En línea] Disponible en:<https://www.tandfonline.com/doi/pdf/10.1080/23738871.2016.1157619?needAccess=true>

THE ECONOMIST. Big Brothers: Edward Snowden's memoir reveals some (but not all). The Economist, Books and Arts, 13 septiembre 2019. [En línea] Disponible en:<https://www.economist.com/books-and-arts/2019/09/13/edward-snowdens-memoir-reveals-some-but-not-all?cid1=cust/dailypicks1/n/bl/n/20190913n/owned/n/n/dailypicks1/n/n/LA/308551/n>

TSAGOURIAS, N. Cyber Attacks, Self-Defence and the Problem of Attribution. Journal of Conflict and Security Law 17, no. 2, Verano 2012. [En línea] Disponible en:<http://jcsl.oxfordjournals.org/content/17/2/229.full.pdf+html>

WIRTZ, J.J. Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. Capítulo 3 en GEER, K. (ed.) Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications, Tallin, 2015. [En línea] Disponible en:<https://ccdcoe.org/uploads/2018/10/Ch03_Cyber

DIRECCIÓN DEL CUADERNO

DIRECTOR

CONSEJO EDITORIAL


CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL