Doble Grado en Derecho y Administración y Dirección de Empresas

TRABAJO DE FIN DE GRADO DE DERECHO (21067)

Curso académico 2019-2020

LA ATRIBUCIÓN DE RESPONSABILIDAD A UN ESTADO POR OPERACIONES LLEVADAS A CABO POR ACTORES NO ESTATALES EN EL CIBERESPACIO.

HACIA UNA INTERPRETACIÓN EXTENSIVA DEL UMBRAL DE «CONTROL EFECTIVO».

RICARDO LÓPEZ HERNÁNDEZ

(ricardo.lopez1997@gmail.com)

Tutor del trabajo:

Dr. Ángel J. Rodrigo Hernández

Profesor Titular de Derecho Internacional Público
y Relaciones Internacionales

RESUMEN

La atribución de responsabilidad a un Estado ha sido regulada tradicionalmente por normas de Derecho Internacional. Los artículos de *Responsibility of States for Internationally Wrongful Acts* (2001) se aplican a las operaciones llevadas a cabo en o a través del ciberespacio. Así se establece en el Capítulo 4 del *Manual de Tallinn 2.0* (2017), texto de *soft-law*, no vinculante. La regla de "control efectivo", propuesta por la CIJ en el Caso *Nicaragua*, se emplea en el proceso de atribución de la responsabilidad a un Estado por ciberoperaciones llevadas a cabo de manera encubierta a través de Actores No Estatales. El objeto de esta investigación es analizar la atribución de aquellas que no pueden ser consideradas ataques armados. Pero esta regla de "control efectivo" no fue concebida para la atribución en el ciberespacio, y esto genera una serie de problemas, tales como la difícil determinación del vínculo debido al anonimato que opera en el ciberespacio, y el acceso limitado a contramedidas de que dispone el Estado damnificado al no poder atribuir la responsabilidad. A estos efectos, se propone como principal solución la extensión del umbral de "control efectivo".

Palabras clave: ciberseguridad, ciberespacio, ciberoperaciones, responsabilidad, atribución, manual de Tallinn 2.0, estados, actores no estatales, control efectivo, interpretación extensiva.

ABSTRACT

The attribution of responsibility to a State has traditionally been regulated by International Law rules. The articles contained in the Responsibility of States for Internationally Wrongful Acts *(2001) apply to operations carried out in or through cyberspace. This is stated in Chapter 4 of the* Tallinn Manual 2.0 *(2017), a non-binding, soft-law text. The "effective control" rule, proposed by the ICJ in the* Nicaragua *Case, is employed in the process of attributing responsibility to a State for cyber operations carried out covertly through Non-State Actors. The object of this research is to analyze the attribution of those that cannot be considered armed attacks. But this rule of "effective control" was not conceived for attribution in cyberspace, and this generates several problems, such as the difficult determination of the link due to the anonymity that operates in cyberspace, and the limited access to countermeasures that the injured State has since responsibility cannot be attributed. To this end, the extension of the "effective control" threshold is proposed as the main solution.*

Keywords: *cybersecurity, cyberspace, cyber operations, responsibility, attribution, Tallinn Manual 2.0, states, non-state actors, effective control, extensive interpretation.*

ÍNDICE

INTRODUCCIÓN.

La regulación y gestión de la seguridad nacional ha correspondido tradicionalmente a los Estados. Estos han sido quienes, a través de sus instituciones y por medio de su legislación interna, han velado por la protección de sus estructuras, por el buen funcionamiento de sus órganos, por la defensa de su integridad territorial y por su población ante potenciales ataques, tanto internos como externos, que pudieran causarles daño.

Sin embargo, en un mundo globalizado carece de sentido estudiar el ámbito de la seguridad desde un punto de vista estrictamente interno. Los Estados interactúan de manera habitual tanto con Actores No Estatales, en el desarrollo de sus funciones, como con otros Estados, ya sea multilateralmente en el marco de las organizaciones internacionales en las que se hayan implicado o en el marco de las relaciones bilaterales que tengan establecidas. Y lo que es cierto es que existen una serie de objetivos comúnmente compartidos por todos ─o la mayoría─ de Estados en el campo de la seguridad que pueden tratarse de manera más eficaz si se afrontan de manera conjunta. Por eso, se ha ido avanzando cada vez más hacia la globalización del concepto de "seguridad". Y, en este proceso, la proliferación de normativa internacional, así como la consolidación de distintas instituciones internacionales como competentes para tratar e intervenir en esta cuestión han resultado inevitables. Es por ello por lo que se puede afirmar sin reservas que el Derecho Internacional Público ha devenido una de las piezas clave en la configuración normativa de la seguridad internacional.

Este estudio trata sobre la atribución de responsabilidad a un Estado por operaciones llevadas a cabo por Actores No Estatales en el ciberespacio. La tecnología no es el futuro; es el presente. Y las amenazas que producen una multiplicidad de sujetos tanto a Estados en particular como al conjunto de la Comunidad Internacional a través de una infraestructura digital de la información y de las comunicaciones globalmente conectada no son solamente una realidad, sino que, además, resultan cada vez más frecuentes. Por ello, en este momento, más que nunca, conviene precisar en qué medida las clásicas normas internacionales pueden ser aplicables a la ciberseguridad, así como qué nueva normativa específica existe en el ámbito de las ciberoperaciones y qué enfoque es necesario que esta siga para que resulte exitosa.

Finalmente, quisiera agradecer sinceramente al Prof. Dr. Ángel José Rodrigo Hernández la valiosa ayuda prestada para la realización de este trabajo.

Espero que resulte interesante.

CAPÍTULO I

MARCO CONCEPTUAL.

«El mundo era tan reciente que muchas cosas carecían de nombre, y para nombrarlas había que señalarlas con el dedo.»

GABRIEL GARCÍA MÁRQUEZ, *Cien años de soledad*.

1. SOBRE LAS CIBEROPERACIONES.

1.1. El ciberespacio como quinto dominio estratégico.

El ciberespacio es un concepto que designa aquel ámbito virtual, de contornos imprecisos, creado por medios informáticos.[1] Al tratarse de un concepto que hace referencia a un espacio caracterizado por su dinamismo, la definición de ciberespacio es, en consecuencia, también dinámica, pues ha variado en función del momento en que se ha tratado de delimitar aquello que el ciberespacio es, así como de la situación que ha propiciado la necesidad de definirlo.

En un primer momento, el Gobierno de los Estados Unidos de América, en su National Security Presidential Directive 54/Homeland Security Presidential Directive 23, definió el ciberespacio, como "la red interdependiente de infraestructuras de tecnología de la información; e incluye Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores incorporados en industrias críticas."[2] Posteriormente, se matizó el concepto de interdependencia al definirlo como "la infraestructura digital de la información y de las comunicaciones conectada globalmente".[3]

[1] REAL ACADEMIA ESPAÑOLA: Diccionario de la lengua española, 23.ª ed., [versión 23.3 en línea]. <https://dle.rae.es/ciberespacio> [29/01/2020].

[2] The White House. (2008). *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* (NSPD-54/HSPD23). Encyclopedia of Security and Emergency Management, 1, 1-9. https://doi.org/10.1007/978-3-319-69891-5_20-1, p.3.

[3] The White House. (2009). Cyberspace Policy Review. *Assuring a Trusted and Resilient Information and Communications Infrastructure*. Security, 3, 1-37. https://fas.org/irp/eprint/cyber-review.pdf, p.1.

Siguiendo esta línea, el grupo internacional de expertos que elaboró el Manual de Tallinn 2.0 sobre el Derecho Internacional aplicable a las ciberoperaciones lo definió como "el entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos utilizando redes informáticas".[4]

La creciente presencia de las TIC en el ámbito público y privado de la sociedad actual y su enorme incidencia en el desarrollo de nuestra vida cotidiana ha creado enormes oportunidades. No obstante, ha generado, a su vez, riesgos antes inimaginables que, por su carácter sistémico, afectan a todos los ámbitos materiales y al sistema internacional en su conjunto.[5] Y parte de este peligro está vinculado al hecho de que actualmente el ciberespacio es el quinto dominio operativo y estratégico y, sin embargo, es aún hoy un espacio poco regulado. Y esto genera ciberinseguridad.

La ciberinseguridad es una situación de predominancia de incertidumbre y desprotección que los actores que poseen una infraestructura digital de comunicaciones pueden sufrir, derivada del posible impacto que puede tener en el buen funcionamiento de su actividad cualquier potencial intervención llevada a cabo por cualquier actor que opere en el ciberespacio con este propósito. En este sentido, la preocupación por la seguridad en el ciberespacio ha aumentado considerablemente a medida que ha aumentado el número de ciberataques y que los actores han tomado conciencia de su vulnerabilidad.[6] Y es precisamente esta proliferación de ataques en el ciberespacio lo que le convierte en un nuevo ámbito de actuación, en el que operan distintos actores para aumentar su cuota de poder, del mismo modo en el que sucede en tierra, mar, aire y espacio y, por tanto, como si del quinto campo de batalla se tratase.[7]

Por el contrario, la ciberseguridad se presenta como la situación de protección de los medios digitales y de las tecnologías de la información frente a accesos ─o intentos de acceso─ no autorizados.[8] Esta protección también está encaminada a evitar la explotación o el daño a

[4] Schmitt, M. N. (ed.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. https://doi.org/10.1017/9781316822524, p.564.

[5] García Segura, C. (2020). *La construcción de normas globales, entre el avance del cosmopolitismo blando y el retorno de la geopolítica. La regulación global de la ciberseguridad*, p.29.

[6] García Segura, 2020, *op. cit.*, nota 5, p.33.

[7] Moussu, N., Llouquet, A.-L., & Chaumei, G. (2011). *Cyberespace, 5ème champ de bataille*. Armées d'aujourd'hui, 365/201. https://www.irsem.fr/data/files/irsem/documents/document/file/790/ADA365.pdf, p.32.

[8] Finnemore, M., & Hollis, D. B. (2016). *Constructing Norms for Global Cybersecurity*. American Journal of International Law, 110(3), 425-479. https://doi.org/10.1017/s0002930000016894, p.431.

los ordenadores, sistemas de comunicación electrónica, y otras tecnologías de la información, incluida la tecnología de la plataforma de información, así como la información que contiene, para asegurar su disponibilidad, integridad, autentificación y confidencialidad.[9]

No obstante, sigue existiendo un cierto debate doctrinal en cuanto a la naturaleza jurídica del ciberespacio. Algunos académicos lo consideran un ámbito sobre el cual los Estados pueden ejercer su soberanía valiéndose de la *doctrina de los efectos*, pues esta permite la regulación de las actividades que tienen impacto en el territorio de un Estado al margen de dónde hayan tenido lugar. Otros, sin embargo, lo consideran parte de los *global commons* y, por lo tanto, un recurso común sobre el que ningún Estado puede reclamar jurisdicción alguna.[10] Pero esta última visión presenta una serie de imprecisiones derivadas de la dificultad de encaje en esta definición: en primer lugar, porque las redes digitales de comunicación de la información son tanto públicas como privadas; en segundo lugar, porque a ellas se le aplican tanto normas nacionales como normas internacionales; y, en tercer lugar, porque a diferencia de los demás *global commons*, no son un recurso físico. De este modo, algunos autores han optado por el concepto de *commons* imperfecto o *pseudo-commons*.[11]

Pero aun así, este punto de vista implicaría la imposibilidad de regular el ciberespacio a no ser que se lograse una posición de consenso internacional, compromiso y aceptación global que permitiese considerarlo Patrimonio Común de la Humanidad. Y, con independencia de que este sea el posible régimen jurídico que pueda llegar a alcanzarse para los recursos básicos del ciberespacio, lo cierto es que la posición de Naciones Unidas desde 2013, manifestada a través del "Tercer Grupo de Expertos Gubernamentales (GEG) sobre los Desarrollos en el Ámbito de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional", es que efectivamente se aplica el principio de soberanía estatal. Y esta consideración implica aceptar que el ciberespacio tiene fronteras, puesto que depende de una infraestructura física que está sujeta a un control soberano.[12]

---

[9] Office of the Chairman of the Joint Chiefs of Staff. (2019). *DOD Dictionary of Military and Associated Terms*. Joint Education and Doctrine Division, J-7, April, 382. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf, p.56.

[10] García Segura, 2020, *op. cit.*, nota 5, p.32.

[11] Segura Serrano, A. (2017). *Ciberseguridad y Derecho internacional*. Revista Española de Derecho Internacional, 69(2), 291-299. https://doi.org/10.17103/redi.69.2.2017.2.02, p.292.

[12] Lewis, J., con el soporte de K. V. (2016). *Report of the International Security Cyber Issues Workshop Series*. UN Institute for Disarmament Research (UNIDIR); CSIS (Center for Strategic and International Studies) -

1.2. Ciberamenazas, ciberoperaciones y ciberataques.

1.2.1. Aclaratio Terminis.

La operatividad en el ciberespacio es una realidad pero, sin embargo, las dificultades para conocer la identidad de quien está operando o la intención con la que lo está haciendo puede complicar enormemente la correcta conceptualización del acto que se está llevando a cabo o que ya se ha llevado a cabo. Por ello resulta imprescindible nombrar con precisión cada hecho que tiene lugar en el ciberespacio en función, en primer lugar, de aquella acción, en sí misma, que ha tenido o está teniendo lugar; en segundo lugar, del método de ejecución que se ha seguido; y, en tercer lugar, de las consecuencias que ha ocasionado. Y esto es evidentemente significativo puesto que, además, en función de la calificación nominal que se haga de aquello que ha ocurrido, el régimen jurídico aplicable variará.

Generalmente, para fijar la definición de aquello que un ciberacto representa conceptualmente se parte de una analogía entre el acto acaecido en el ciberespacio y un acto convencional equivalente o semejante. Esto, por un lado, se debe a la escasa regulación específica del ciberespacio; pero, de hecho, precisamente la escasa regulación existente, paradójicamente, cuando define conceptualmente aquellos actos llevados a cabo en el ciberespacio, se vale de estas analogías mencionadas.

Siguiendo esta línea, a efectos de este trabajo, conviene precisar los siguientes términos: *ciberamenaza*, *ciberoperación* y *ciberataque.*

Una *ciberamenaza* puede ser entendida como una intimidación o provocación que se lleva a cabo en el ciberespacio, o a través del ciberespacio. Si bien esta definición es ampliamente aceptada en el ámbito doctrinal, la concepción real que los Estados pueden llegar a emplear del concepto de "ciberamenaza" puede ser entendida también en sentido amplio. En este caso, consistiría en cualquier operación que sea susceptible de ser considerada como potencialmente perjudicial para los intereses de un Estado llevada a cabo en el ciberespacio, de la que no se tiene control, y que implica generalmente tanto el reconocimiento de la cibercapacidad del actor que la está llevando a cabo ─o que la ha llevado a cabo─ como el

Workshop Series. https://www.unidir.org/publication/report-international-security-cyber-issues-workshop-series, p.6.

reconocimiento de una cibervulnerabilidad concreta por parte del Estado afectado. Se trata, por supuesto, de una interpretación mucho más subjetiva del concepto de ciberamenaza.[13]

Las *ciberoperaciones* son actuaciones en las que se emplean las capacidades del ciberespacio con el propósito principal de alcanzar unos objetivos concretos tanto el ciberespacio como a través de él.[14]

Los *ciberataques* son aquellas acciones realizadas por Estados ─o por Actores No Estatales cuyas actuaciones pueden ser atribuidas a los Estados─, que crean efectos hostiles tales como la degradación, la perturbación, la manipulación o la destrucción, y que se llevan a cabo en el ciberespacio o a través de él.[15] Cuando este tipo de ataques se llevan a cabo por individuos o por entidades privadas, sin que pueda derivarse de ellos un vínculo concreto de conexión con un Estado, se habla de *ciberdelitos* y *cibercrímenes*, siendo la diferencia entre ambos la gravedad de la acción perpetrada.[16]

Desde el punto de vista teórico pueden surgir confusiones conceptuales debido a la cierta similitud entre estos dos últimos términos. Pero, además, los problemas de interpretación se agravan al introducir el concepto de *ciberguerra*. Por *ciberguerra* se entienden aquellas acciones que lleva a cabo un Estado para penetrar en los ordenadores, redes informáticas o medios digitales de información de otro Estado con el propósito de causar daño o interrupción.[17]

Tomando esto en consideración, han de tenerse en cuenta las dos principales diferencias que existen entre una *ciberoperación* y un *ciberataque*. La primera es de carácter subjetivo: mientras que una *ciberoperación* puede ser llevada a cabo por cualquier actor en el ciberespacio cuya actuación se ajuste a la definición proporcionada, un *ciberataque* debe ser efectuado por un Estado, ya sea directamente ─por él mismo─ o indirectamente ─actuando por medio de Actores No Estatales─, además de materializarse, por supuesto, en una acción constitutiva de ser denominada como tal. La segunda diferencia es de carácter objetivo: una *ciberoperación* que causa destrucción física, heridos o víctimas debe ser considerada un *ciberataque* y, si tiene

[13] Finnemore & Hollis, 2016, *op. cit.*, nota 8, p.432.

[14] Office of the Chairman of the Joint Chiefs of Staff, 2019, *op. cit.*, nota 9, p.56.

[15] Office of the Chairman of the Joint Chiefs of Staff, 2019, *op. cit.*, nota 9, p.55.

[16] García Segura, 2020, *op. cit.*, nota 5, p.36.

[17] Clarke, R. A., & Knake, R. K. (2010). Cy*ber War: the Next Threat To National Security and What To Do About It.* 2(6), 1-140. https://doi.org/10.22456/2178-8839.20585, p.11.

estas consecuencias indicadas, entonces es constitutivo del uso de la fuerza ─véase apartado 1.2.2─.

Así pues, se puede afirmar que los *ciberataques* son aquellas *ciberoperaciones* perpetradas por Estados de manera directa o indirecta; y que equivalen al uso de la fuerza si los efectos o resultados que comportan son similares al uso de la fuerza armada. Y, si esto ocurre, se dice que el ciberataque se produce en un contexto de *ciberguerra* ─siendo el rasgo distintivo principal de la misma el uso de la tecnología de la información y de los medios digitales de comunicación como medio, y no necesariamente como objetivo─.

1.2.2. El «uso de la fuerza» en el ciberespacio.

El artículo 2.4 de la Carta de Naciones Unidas (1945) establece lo siguiente:

> *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*.

Tomado en consideración lo dispuesto en este artículo, es inevitable plantear el modo en que las ciberoperaciones pueden calificarse de "fuerza". En este sentido, cabe destacar que existe consenso en la literatura académica a la hora de considerar que el término "fuerza" es sinónimo de "fuerza armada" o de "fuerza militar" aunque, en cualquier caso, la Corte Internacional de Justicia ─en adelante, CIJ─ afirmó en *Legality of the Threat or Use of Nuclear Weapons, advisory opinión,* §*39* (1996) que la prohibición del artículo 2.4 de la Carta se aplica "a todo uso de la fuerza, independientemente de las armas empleadas". Y, en esta línea, existen razones de peso para considerar que, si las ciberoperaciones tienen efectos análogos a los que se derivarían del empleo de armas convencionales ─tales como daños físicos o funcionales─, estas quedarían comprendidas en la prohibición expresada en este artículo.[18]

Sin embargo, la mayor dificultad para encajar el concepto clásico de "fuerza" en las ciberoperaciones reside en aquellas que no causan directamente la muerte, ni producen lesiones, ni ocasionan destrucción. Además, esta dificultad se intensifica si se tiene en cuenta que, mientras que en numerosas ocasiones las ciberoperaciones tienen por objeto último causar coacción política ─en cualquiera de sus vertientes─ por medio del caos provocado por ataques

[18] Melzer, N. (2011). *Cyberwarfare and International Law*. Cyberwarfare and International Law - UNIDIR Resources, 38, p.7.

a servicios digitales de información, el artículo 41 de la Carta propone "la interrupción de las comunicaciones" como una medida que no implica el uso de la fuerza armada.

Ante esto, Melzer sostiene que debe primar una perspectiva teleológica de la carta, basada en el hecho de que ésta "tan solo puede lograr sus propósitos generales de mantener la paz y la seguridad internacionales" ─promulgada en el artículo 1 de la Carta─, así como de "preservar a las generaciones venideras del flagelo de la guerra" ─expresada en el preámbulo de la Carta─, "si prohíbe el recurso a toda medida de fuerza que pueda provocar una reacción militar y, en última instancia, el estallido de un conflicto armado internacional; puesto que, por lógica, la Carta no puede permitir que la prohibición de la fuerza interestatal se eluda mediante la aplicación de medios y métodos no violentos que, a todos los efectos, equivalen a una ruptura de la paz entre los Estados implicados".[19]

Y, en este sentido, la situación de desorden y confusión provocada por una interrupción deliberada de las comunicaciones llevada a cabo por medios cibernéticos, aunque pudiera no calificarse como ciberataque por no causar o desencadenar consecuencias equivalentes a los de los ataques armados convencionales, sí podría ser susceptible de ser considerado como un acto en el que se ha hecho uso de la fuerza y, en consecuencia, una acción contraria al artículo 2.4 de la Carta. De ser así, la principal diferencia operativa, pues, entre hacer uso de la fuerza y constituir un ataque armado estaría en la legitimación del damnificado para hacer uso de contramedidas, entendidas estas como un ejercicio constitutivo de legítima defensa.

Pero aunque esta interpretación goce de sentido a la luz de la visión teleológica expuesta, la realidad es que hoy en día sigue sin haber consenso en la comunidad internacional acerca de cuándo, cómo y por qué las ciberoperaciones que no causan muertes, lesiones ni destrucción deben equivaler a un "uso de la fuerza".

1.2.3. La actualización del concepto de «ataque armado».

Por el contrario, más consenso hay a nivel doctrinal en considerar que un ciberataque que tenga una "escala y efectos" cualitativamente análogos a los de un ataque armado deba ser considerado como tal conforme al artículo 51 de la Carta y que, en consecuencia, justifique el recurso a la legítima defensa.[20]

[19] Melzer, 2011, *op. cit.*, nota 18, p.8.

[20] Segura Serrano, 2017, *op. cit.*, nota 11, p.294.

El artículo 51 de la Carta de Naciones Unidas (1945) establece lo siguiente:

> *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* […].

Por un lado, se debe tener en cuenta que el concepto de "ataque armado" implica necesariamente el uso de un arma. En este sentido, algunos autores ya han planteado la calificación como "arma" que "puede llegar a tener" el ciberespacio. Lo hacen basándose en dos parámetros: por un lado, la intención con la que se usa; y, por otro lado, el efecto que puede provocar su empleo.[21] Y, de este modo, superando las complejidades asociadas a la identificación del arma empleada en un ciberataque en concreto ─que sería el propio ciberespacio *per se*─, resulta relativamente intuitivo recurrir al criterio inicialmente expuesto de equivalencia de "escala y efectos" para extender la aplicabilidad del concepto de ataque armado al ciberataque en cuestión.[22]

Y, puesto que la CIJ confirmó que el concepto de "ataque armado" al que hace referencia el artículo 51 de la Carta es requisito para que opere el derecho de legítima defensa, los Estados que hubieren sufrido ciberataques de "escala y efectos" análogos a los de un ataque armado, en términos de destrucción, podrían efectivamente tener acceso a desarrollar contramedidas ─incluido el recurso a la fuerza militar tanto dentro como fuera del ciberespacio─ valiéndose del levantamiento de la prohibición del uso de la fuerza.[23] Y, siguiendo este planteamiento, a nivel cibernético operaría, del mismo modo que a nivel convencional, la *legítima defensa anticipada* ─posibilidad de un Estado de actuar adelantándose a un ataque cuando hay indicios fehacientes de que va a ser atacado y en caso de que, además, el no actuar le provoque la pérdida de la capacidad de defensión─, y se descartaría la *legítima defensa preventiva* ─consistente en efectuar acciones similares a las que se podrían

[21] Melzer, 2011, *op. cit.*, nota 18, p.13.

[22] International Court of Justice. (1986). *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America), merits. The International Court of Justice, The American Journal of International Law, 81(1). https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

[23] International Court of Justice, Nicaragua v. United States of America, 1986, *op. cit.*, nota 22.

llevar a cabo en caso de legítima defensa anticipada, pero sin disponer de evidencias de que el potencial atacante realmente vaya a atacar─.[24]

Sin embargo, este planteamiento basado en la equiparación de los efectos destructivos causados por un ataque convencional con los efectos destructivos causados por un ciberataque implica perpetuar la dificultad de extensión del concepto de "ataque armado" al ámbito cibernético, habida cuenta de que las consecuencias de los ciberataques se caracterizan más por su condición perturbadora que por su condición destructiva.[25]

Así pues, si bien existe cierto consenso en la literatura académica a la hora de considerar que la analogía cualitativa de "escala y efectos" es adecuada para identificar qué ciberoperaciones deben ser susceptibles de ser consideradas como ciberataques, no existe una posición comúnmente extendida acerca de la interpretación de la idea de "equivalencia" asociada a esta analogía mencionada; esto es, cuándo la escala y los efectos son análogos y cuándo no ─especialmente, cuando no hay destrucción─. En esta línea, quizá se podría plantear que la analogía se llevase a cabo sobre la perturbación causada, y no sobre la destrucción ocasionada, pero esto igualmente traería consigo dificultades interpretativas y operativas tanto o más arduas que las ya existentes.

El modo de dar respuesta a estas cuestiones a través de los planteamientos expuestos indujo a uno de los puntos de mayor discordia entre los expertos que participaron en las conferencias que dieron lugar al Manual de Tallinn.

Respecto a esto, cabe mencionar que el Manual de Tallinn, en su Regla 14, sección 1, Cap. 4, establece qué ciberactos son internacionalmente ilícitos. Y, por otro lado, también considera que resulta de aplicación a las ciberoperaciones la cláusula Martens, mediante la cual debe entenderse que no porque un acto no esté expresamente prohibido en el Manual debe ser considerado legal. Así, "cuando no haya Derecho Internacional aplicable, los civiles y combatientes quedarán bajo la protección y la autoridad de los principios de Derecho Internacional consuetudinario, de los principios de humanidad y de los dictados de la conciencia política".[26]

[24] García Segura, 2020, *op. cit.*, nota 5, p.51.

[25] Melzer, 2011, *op. cit.*, nota 18, p.14.

[26] García Segura, 2020, *op. cit.*, nota 5, p.51.

2. LOS ACTORES EN EL CIBERESPACIO.

Todo aquél que actúe en o a través del ciberespacio, en los términos indicados en el apartado 1.1, es susceptible de ser considerado como "actor en el ciberespacio". Si bien hay un vasto número de agentes que operan en él, para tratarlos debidamente, en este trabajo se les agrupa por su naturaleza. De este modo, puede afirmarse que son actores en el ciberespacio tanto los Estados como los Actores No Estatales.

Debe considerarse "Estado" todo aquel país soberano, reconocido como tal en el orden internacional, cuya población se halla asentada en un territorio determinado, y que está dotado de órganos de gobierno propios.[27] Por el contrario, en este trabajo se entiende que a todo actor diferente al Estado que intervenga en el ciberespacio se le debe considerar Actor No Estatal. En este sentido, se incluyen como Actores No Estatales a todas aquellas personas, corporaciones, organizaciones no gubernamentales, instituciones, asociaciones, agencias, grupos terroristas, grupos paramilitares y grupos de resistencia armada, entre otros, que de modo particular interactúan en el ciberespacio.

Existen cuatro principales amenazas identificadas para la seguridad internacional que provienen del ámbito cibernético: la ciberguerra, el ciberterrorismo, el ciberespionaje y el cibercrimen.[28] Y en cada una de ellas intervienen predominantemente unos determinados actores en concreto. Así, en la ciberguerra intervienen principalmente los Estados; en el ciberterrorismo, principalmente grupos terroristas y grupos paramilitares o de resistencia armada; en el ciberespionaje, además de los Estados, la participación de las corporaciones es cada vez más copiosa; y, en el cibercrimen, aunque destacan los llamados "hacktivistas", en realidad intervienen de manera agregada una pluralidad de actores.

Los próximos capítulos se van a centrar en el ámbito de la ciberguerra y, en concreto, en el papel que desarrollan los Actores No Estatales en este entorno predominantemente integrado por Estados. El punto de partida es que, si bien los Estados operan en el ciberespacio, no siempre lo hacen de manera directa. El motivo es evidente: la fácil revelación del vínculo entre una ciberoperación llevada a cabo y un Estado como ejecutante de la misma implica, por un lado, para el Estado damnificado, la prácticamente incuestionable y manifiesta detección del

[27] REAL ACADEMIA ESPAÑOLA: Diccionario de la lengua española, *op. cit.*, nota 1, <https://dle.rae.es/estado> [07/02/2020].

[28] Boletín Oficial del Estado (2010). *Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001*. 78847-78896.

Estado causante a la hora de emprender contramedidas; y, por otro lado, supone un relativamente sencillo reconocimiento como culpable ante la Comunidad Internacional por la acción ilícita que ha llevado a cabo, y esto facilita enormemente el desarrollo e imposición de sanciones previstas.

Así pues, los Estados pueden optar por actuar de manera indirecta; esto es, actuando de manera encubierta a través de Actores No Estatales. Los mecanismos de análisis del vínculo entre los Actores No Estatales que ejecutan y el Estado que hay detrás que financia, idea, instruye, planifica, ordena, dirige, controla u opera de manera encubierta a través de los primeros, así como el régimen de atribución de la responsabilidad a un Estado por ciberoperaciones que aparentemente no han sido llevadas a cabo por este, y que no pueden ser consideradas como ataques armados, es el principal objeto de estudio del Capítulo II.

CAPÍTULO II

LA ATRIBUCIÓN DE RESPONSABILIDAD A UN ESTADO ANTE CIBEROPERACIONES DE ACTORES NO ESTATALES.

«Sé extremadamente sutil, discreto, hasta el punto de no tener forma.
Sé completamente misterioso y confidencial, hasta el punto de ser silencioso.
De esta manera podrás dirigir el destino de tus adversarios.»

SUN TZU, *El arte de la guerra*.

3. NORMATIVA APLICABLE EN MATERIA DE ATRIBUCIÓN.

3.1. La reinterpretación de los artículos de *Responsibility of States for Internationally Wrongful Acts* (2001).[29]

En el momento en que los expertos que participaron en la elaboración del Manual de Tallinn deliberaron acerca de la responsabilidad internacional de los Estados por operaciones llevadas a cabo en el ciberespacio hubo consenso en que el derecho consuetudinario en esta materia debía aplicarse también a las actividades cibernéticas; y que, en consecuencia, la doctrina de la responsabilidad del Estado, contenida principalmente en *The International Law Commission's Articles on State Responsibility*, debía extenderse a las ciberoperaciones.[30] Así pues, en este sentido, conviene precisar el alcance reintepretativo en materia de ciberseguridad de los artículos contenidos en el Capítulo I ─*General principles*─ y en el Capítulo II ─*Attribution of conduct of a State*─ de dicho texto de Naciones Unidas.

El artículo 1 establece que todo acto internacionalmente ilícito llevado a cabo por un Estado le genera responsabilidad internacional por este. Al extenderse la interpretación de estos artículos al campo de las ciberoperaciones resulta indiscutible considerar que cualquier acto llevado a cabo por un Estado en el ciberespacio que, por un lado, sea atribuible a este Estado

[29] International Law Commission. (2001). *Responsibility of States for Internationally Wrongful Acts*. General Assembly, vol. II (Part Two). Annex to General Assembly resolution 56/83 of 12 December 2001.

[30] Jensen, E. T. (2017). *The Tallinn Manual 2.0: Highlights and Inisghts*. Georgetown Journal of International Law, 43(3), 735-778. https://www.law.georgetown.edu/international-law-journal/in-print/volume-48-number-3-spring-2017/the-tallinn-manual-2-0-highlights-and-insights/, p.750.

mediante el Derecho Internacional, y que, por otro lado, constituya una vulneración de una obligación internacional, tanto por acción como por omisión, acarrea al Estado actuante u omisivo responsabilidad internacional ante este. En este sentido, el artículo 2 es incuestionable. Además, el artículo 3 especifica diáfanamente que en la determinación de la ilicitud internacional de un acto deben tenerse en cuenta únicamente las normas internacionales ─esto es, con independencia de lo que establezca al respecto la legislación interna del Estado─.

La conexión entre la "ilicitud internacional de un acto" y "la responsabilidad internacional por dicho acto" se lleva a cabo mediante un vínculo en el que el Estado, como sujeto de Derecho Internacional, resulta ser el nexo. Y el proceso de determinación de la conexión entre el acto acaecido u omitido que ha sido constitutivo de ilicitud internacional y el Estado que lo ha llevado a cabo o lo ha omitido se denomina "proceso de atribución de responsabilidad". La atribución es una operación normativa; esto es, un mecanismo a través del cual se determina, en virtud de unas normas establecidas, cuándo existe un vínculo lo suficientemente estrecho entre un determinado comportamiento y un Estado como para poder considerar que éste ha sido causado por él. Y estas normas atributivas responden a criterios normativos, como se verá a continuación, "y no al mero reconocimiento de un vínculo de causalidad fáctico".[31] Siguiendo esta línea, se debe tener especialmente en cuenta que la atribución de responsabilidad involucra al Estado como persona jurídica que, aunque actúa con capacidad legal propia, fácticamente lo hace a través de personas que ocupan distintos cargos con deberes y obligaciones diversas, y cuyas funciones conforman el conjunto de actuaciones del Estado. Es por ello por lo que también corresponde al Derecho Internacional, por tanto, determinar cuándo y por qué un acto puede ─o no─ atribuirse a un Estado.

En este sentido, el Capítulo II ─artículos 4 a 11─ contiene estas disposiciones normativas mencionadas en forma de reglas y a través de las cuales, debido a su carácter *numerus clausus*, a excepción de los casos en los que sea aplicable una *lex specialis* en virtud del artículo 55, únicamente se puede atribuir la responsabilidad de un acto internacionalmente ilícito ─como una ciberoperación revestida de ilicitud─ a un Estado en función de los siguientes criterios y parámetros.

[31] Crawford, J. (2002). *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries.* Cambridge University Press. https://doi.org/10.2307/3100134, p.91.

El artículo 4.1 establece que todo acto internacionalmente ilícito llevado a cabo por órganos estatales con funciones legislativas, ejecutivas o judiciales será considerado un acto cuya responsabilidad asumirá el Estado del que estos órganos formen parte, con independencia de la posición que ocupe el órgano en cuestión en la organización formal o territorial del Estado. Así pues, si se exporta esta regla al campo de las ciberoperaciones, el primer criterio atributivo que se observa es que, desde el punto de vista de la responsabilidad, el Estado responde a nivel internacional por cualquier ciberoperación ilícita llevada a cabo por cualquiera de sus órganos. Esta afirmación, sin embargo, debe matizarse: las actividades llevadas a cabo por órganos de un Estado generan responsabilidad a dicho Estado cuando estos órganos mencionados actúan de manera oficial, y no como meras personas privadas. Esta distinción conlleva a menudo problemas atributivos basados en la dificultad de distinguir en la práctica un acto con carácter *ultra vires* de un acto privado. En este sentido, Crawford afirma que "para que la atribución sea posible, sólo hace falta que el órgano actúe en calidad aparentemente oficial o con aspecto de autoridad".[32]

Y el artículo 4.2 delimita el concepto de "órgano" al indicar que se debe "incluir" como órgano a toda persona o entidad a la que el derecho interno le brinde esta condición. Es ciertamente importante el matiz de "inclusión" que añade este segundo párrafo, puesto que implica que la calificación como "órgano" no puede limitarse únicamente al hecho de ser considerado como tal por el derecho interno. O, dicho de otro modo, si bien todos los órganos así clasificados por el derecho interno del Estado deben ser considerados como "órganos" a los efectos atributivos de este texto de Naciones Unidas, este criterio no es exhaustivo: el Derecho Internacional puede determinar que una entidad o grupo organizado de personas resulta ser fácticamente un órgano de un Estado en base a criterios normativos basados en distintos tipos de vínculos, tal y como distintos tribunales internacionales ya han dictaminado.[33] La razón no es otra que "evitar la elusión de la responsabilidad de un Estado por el comportamiento de un ente que en realidad actúa como uno de sus órganos simplemente negándole esa condición en el derecho interno".[34]

El artículo 5 hace referencia al comportamiento de las personas o entidades que ejercen elementos de autoridad gubernamental. Sobre estos, se establece que, si actúan con un poder

[32] Crawford, 2002, *op. cit.*, nota 31, p.99.

[33] Dixon, M. (2007). *Textbook on International Law*. Oxford University Press, p.248.

[34] Crawford, 2002, *op. cit.*, nota 31, p.98.

público proveniente de la legislación interna, sus actos le generan responsabilidad a Este estado. Por tanto, toda ciberoperación ilícita llevada a cabo por personas o entidades no susceptibles de ser consideradas como "órganos" por el artículo 4.2 pero que actúan revestidas de poder público ─y que desarrollan valiéndose de sus capacidades oficiales─ generan responsabilidad al Estado que le ha dotado de este poder. Se podría decir que el vínculo que existe con el Estado y que permite justificar la atribución es la propia habilitación como autoridad gubernamental que le dota a la entidad en cuestión el derecho interno. La razón de ser de este precepto es evitar que los Estados eludan su responsabilidad internacional mediante la delegación de funciones a organismos recientemente privatizados y con carácter aparente y presuntamente autónomo.

El artículo 6 resuelve la problemática atributiva derivada de la puesta a disposición de un Estado un órgano de otro Estado, indicando que la responsabilidad internacional por el acto internacionalmente ilícito ─en este caso, la ciberoperación controvertida llevada a cabo─ la ostentará aquel Estado a disposición del cuál el órgano en cuestión se encuentre. Resulta de aplicación este precepto, por tanto, a cualquier puesta a disposición de un Estado de infraestructura cibernética o de medios tecnológicos por parte de otro Estado. En caso de que el Estado que tenga a su disposición esta infraestructura mencionada se valga de esta para desempeñar ciberactividades ilícitas, tal y como se indica en este artículo, este Estado mencionado será internacionalmente responsable de ellas.

El artículo 7 establece que, aunque haya habido un exceso de atribuciones por parte de un órgano, grupo de personas o entidades, o aunque haya habido una contravención de instrucciones, el Estado del que estas dependan será responsable a nivel internacional por el comportamiento observado si actúan ejerciendo elementos de poder público en el desempeño de sus funciones públicas. El exceso de atribuciones en materia cibernética se podría situar, sobre todo, en aquellos órganos asociados a los Cuerpos y Fuerzas de Seguridad del Estado especializados en el campo de la ciberseguridad, así como a aquellas entidades dependientes del Ministerio de Defensa con tareas y funciones de operatividad en el ciberespacio.

El artículo 8 contiene el precepto más relevante en la cuestión de la atribución de responsabilidad a un Estado que compete en esta investigación. Este hace referencia a la atribución de responsabilidad al Estado ante comportamientos de personas o grupos de personas sin un aparente nexo formal con el Estado. El artículo 8 establece que un acto será considerado como propio de un Estado si es llevado a cabo por terceros "bajo la dirección o el control de este Estado". Así pues, el vínculo entre la actividad internacionalmente ilícita que ha tenido

lugar y un Estado en concreto se halla en el control que este Estado ejerce sobre los terceros que han desempeñado dicha actividad internacionalmente ilícita. En estos casos, como se puede apreciar, la operación atributiva se fundamenta en la relación fáctica entre Estado y terceros, y no en una relación jurídica concreta, pues esta es aparentemente inexistente. La razón de ser de este artículo es impedir que un Estado que ha instruido, ordenado o controlado un comportamiento internacionalmente ilícito ─en el caso aquí tratado, una ciberoperación revestida de ilicitud─ que ha sido llevado a cabo por particulares pueda eludir la responsabilidad que entraña por este; y, en consecuencia, supone una excepción al principio general de que los actos de particulares no deben atribuirse al Estado.[35]

Pero, llevando este análisis al campo de la ciberseguridad, resulta imprescindible tomar en consideración una cuestión esencial ─quizá la más significativa en este ámbito─, que es: ¿cómo se demuestra que una ciberoperación realizada por Actores No Estatales ─esto es, actores que operan en el ciberespacio distintos al Estado─ ha sido instruida, dirigida o controlada por un Estado? Y, siguiendo este planteamiento, inevitablemente surgen cuestiones tales como: ¿qué nivel de dirección y control es necesario que se demuestre que ha existido entre el Estado y el Actor No Estatal en cuestión para atribuir la responsabilidad al Estado? O, ¿cómo opera esta disposición en el contexto de anonimato fáctico que caracteriza al ciberespacio? Distintos tribunales internacionales se han pronunciado al largo de los años sobre estas cuestiones y han llevado a cabo interpretaciones de este precepto aplicadas al caso concreto sobre el que debían pronunciarse, respectivamente. En el apartado 4 se proporciona una exposición detallada acerca de esta cuestión.

El artículo 9 trata acerca de las conductas llevadas a cabo por personas o grupos de personas en ausencia de autoridades oficiales. En este sentido, se indica que sus actuaciones serán atribuibles en materia de responsabilidad internacional al Estado si estas ejercen de hecho elementos de autoridad gubernamental en ausencia o en defecto de autoridades oficiales, y en circunstancias tales que exijan el ejercicio de esos elementos de autoridad. Los potenciales supuestos de hecho enmarcables en del campo de las ciberoperaciones ciertamente se limitan a casos específicos que nunca han sucedido y que resulta difícil que se den en la práctica.

[35] International Law Commission (2001). *Draft articles on Responsibility of States for Internationally Wrongful Acts*, with commentaries, Fifty-third A/56/10 (2001).
https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, p.47.

El artículo 10.1 establece que una conducta llevada a cabo por un movimiento insurreccional cuyos impulsores acaban convirtiéndose en el nuevo gobierno del Estado en cuestión debe ser considerada como un acto de este Estado. Paralelamente, y siguiendo esta línea, las conductas realizadas por movimientos que establezcan un nuevo Estado en parte del territorio de un Estado se deberán entender como actos de cuya responsabilidad internacional debe responder el nuevo Estado ─artículo 10.2─. Por el contrario, de lo dispuesto en este artículo se deduce el hecho de que si el movimiento insurreccional en cuestión ni logra situarse al frente del gobierno de un Estado ni logra crear un Estado nuevo, la conducta se deberá atribuir a las personas que constituyen el movimiento, y no al Estado en el que éste ha tenido lugar. La extensión de lo dispuesto al ámbito cibernético resulta mismamente inusual y excepcional.

Subsidiariamente a todo lo expuesto, el artículo 11 introduce un precepto mediante el cual la responsabilidad de cualquier acto internacionalmente ilícito que sea reconocido y asumido como propio por un Estado le será atribuible a dicho Estado.

Estos artículos presentados, cuyas reglas han sido expuestas, constituyen los ocho supuestos previstos normativamente en el texto de Naciones Unidas *Responsibility of States for Internationally Wrongful Acts* (2001) que dan lugar a la atribución de responsabilidad internacional a un Estado. Pero, si bien estos artículos indudablemente resultan de aplicación en caso de producirse situaciones análogas a las establecidas en ellos a través del ciberespacio, la realidad es que no fueron concebidos para este fin, y esto genera una serie de imprecisiones que obstaculizan que la aplicación que se pueda hacer de ellos en este ámbito sea realmente eficaz desde un punto de vista teleológico.

Sin duda, la naturaleza compleja del ciberespacio exige una regulación propia que tome en consideración las particularidades de este entorno y que pueda tratar exitosamente desde el punto de vista del Derecho las problemáticas que en él se generan ─o que pueden potencialmente generarse─ en materia de atribución.

3.2. La regulación específica de la ciberseguridad: el *Manual de Tallinn 2.0* (2017).[36]

El *Manual de Tallinn 2.0 sobre Derecho Internacional aplicable a las ciberperaciones* es un documento académico ─y, en consecuencia, no vinculante─ que recoge en forma de preceptos con apariencia normativa el resultado consensuado de las deliberaciones adoptadas por el Grupo Internacional de Expertos que, a propuesta del Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN, se conformó en 2017 para tratar distintas cuestiones acerca de la aplicabilidad del Derecho Internacional en el ciberespacio. A pesar de no ser vinculante, pretende ser un documento al que los Estados ─especialmente, aquellos miembros de la OTAN─ puedan recurrir como guía tanto a la hora de legislar como a la hora de hacer frente a las distintas situaciones que se pueden derivar de un empleo cada vez más frecuente de las ciberoperaciones por parte de cada vez más actores con todo tipo de intenciones. El resultado de este proyecto lleva el nombre de la capital de Estonia, por ser este el Estado donde se perpetró el primer ataque cibernético de un país a otro.[37]

Se trata de una actualización y revisión de un primer Manual, llamado *Manual de Tallinn sobre Derecho Internacional aplicable a la ciberguerra*, elaborado entre 2009 y 2012, y publicado en 2013. Las principales diferencias del segundo Manual respecto del primero son, en primer lugar, que en su elaboración se amplió el origen geográfico de los expertos, como modo de aceptar y solventar constructivamente parte de las críticas que recibió el primer Manual debido a la procedencia eminentemente occidental de los miembros del primer grupo de expertos. En segundo lugar, que en esta segunda versión se analizan aquellas ciberoperaciones más comunes en la práctica, que son aquellas que acaban sin poder considerarse constitutivas del uso de la fuerza y que no se dan en contextos de conflictos armados. Y, en tercer lugar, que se añadió un examen en detalle de la aplicabilidad de distintos aspectos del Derecho Internacional que inciden directamente en el campo de las ciberoperaciones, tales como los Derechos Humanos, el Derecho del Mar y del Espacio, o el Derecho diplomático y consular.[38] En él, no obstante, se reafirma una de las principales

[36] Schmitt, M. N. (ed.), 2017, *op. cit.*, nota 4.

[37] Fonseca, C. E. (2014). *El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra*. Revista de la ESG, 11.
http://www.cefadigital.edu.ar/bitstream/123456789/993/1/Revista ESG no.588-2014_Fonseca_172.pdf, p.136.

[38] García Segura, 2020, *op. cit.*, nota 5, p.53

conclusiones que quedó plasmada en el primer Manual: la incuestionable aplicabilidad del Derecho Internacional existente en el ámbito de la ciberseguridad.

La cuestión es que el Manual de Tallinn 2.0 trata una multiplicidad de aspectos acerca de las ciberoperaciones. Y, en este sentido, contiene una Regla que hace referencia expresa a la atribución de responsabilidad al Estado por operaciones llevadas a cabo por Actores No Estatales en el ciberespacio, materia que es propia de este estudio. De este modo, a continuación se procederá a analizar en detalle esta regla mencionada ─la Regla 17, sobre "Atribución de ciberoperaciones de Actores No Estatales"─ como *Lex Specialis*.

La Regla 17 del Manual de Tallinn 2.0 establece lo siguiente:

> *Las ciberoperaciones realizadas por Actores No Estatales son atribuibles a un Estado cuando:*
> *(a) Se efectúen en conformidad con sus instrucciones o bajo su dirección o control; o*
> *(b) El Estado reconozca y adopte las operaciones como propias.*

Se debe tener en cuenta que el Grupo Internacional de Expertos entendió que, al ser aplicable el Derecho Internacional convencional al ámbito de la ciberseguridad, en las reglas del Manual de Tallinn 2.0 sobre "Derecho de la Responsabilidad Internacional" ─Reglas 14 a 31; Capítulo 4, Secciones 1 a 4; Parte 1: *Derecho Internacional General y Ciberespacio*─ se debían tomar como referencia los artículos plasmados por la Comisión de Derecho Internacional en el texto de Naciones Unidas *Responsibility of States for Internationally Wrongful Acts* (2001) ─véase apartado 3.1─. Es por esto por lo que no es de extrañar que los comentarios adjuntos que constituyen los 19 puntos aclarativos que contiene la Regla 17 hagan mención constante a artículos como el 8 de este texto de Naciones Unidas mencionado, sobre el que se basa para desarrollar la teoría sobre responsabilidad internacional aplicable a este tipo de ciberoperaciones, tal y como se va a ver a continuación.

Como regla general, las ciberoperaciones llevadas a cabo por personas o grupos de personas no son atribuibles a Estados[39]. Pero, como se ha indicado anteriormente, el artículo 8 de *Responsibility of States for Internationally Wrongful Acts* (2001) ─y, en consecuencia, la Regla 17 del Manual de Tallinn 2.0─ constituyen una excepción a este principio general mencionado, mediante la cual una ciberoperación realizada por un Actor No Estatal "que actúe de hecho bajo las instrucciones de un Estado, o bajo la dirección o control de un Estado,

[39] International Law Commission, 2001, *op. cit.*, nota 35; Article 8, para. 7 of commentary.

comportará la atribución de responsabilidad internacional" a este Estado mencionado por la ciberoperación que haya perpetrado este Actor No Estatal, por entenderse que el Estado ha actuado a través de éste, o valiéndose de éste.[40]

Además, la Regla 17, como *Lex Specialis*, aporta al ya mencionado artículo 8 de la Comisión de Derecho Internacional un matiz acerca de qué debe entenderse como Actor No Estatal. A estos efectos, y tal y como se ha indicado en el apartado 2, deben considerarse como tales tanto a "personas" como a "grupos de personas", con independencia de que constituyan una corporación o no, de que sean jerárquicos o no, de que estén organizados o no, y de que posean personalidad jurídica nacional o no. Además, se ofrece una lista no exhaustiva de potenciales sujetos susceptibles de ser considerados como Actores No Estatales. A estos efectos, se mencionan: hackers; grupos informales como Anonymous; organizaciones delictivas dedicadas a la ciberdelincuencia; personas jurídicas tales como empresas comerciales de servicios de TIC, software y hardware; así como ciberterroristas o insurgentes cibernéticos.[41]

Pero, ¿qué situaciones exactamente pueden implicar, conllevar o suponer que la responsabilidad por una ciberoperación llevada a cabo por un Actor No Estatal sea atribuida a un Estado? En los comentarios a la Regla 17 se establece que tanto "las directrices específicas" dadas por un Estado a un Actor no Estatal en relación con una ciberactividad concreta a desarrollar, como "el ejercicio del control sobre un grupo" constituyen certezas que comportan la asunción de responsabilidad internacional al Estado. Pero, si bien cada caso es distinto, estos dos parámetros tomados en consideración se deberán aplicar ajustándose a los propios hechos de cada caso concreto para valorar la cuestión de la atribución cuando corresponda.[42]

Para ello, la Regla 17, en tanto que *Lex Specialis*, también aporta indirectamente al artículo 8 de *Responsibility of States for Internationally Wrongful Acts* (2001) una enumeración con carácter *numerus clausus* de circunstancias que pueden tener lugar en el ámbito de las ciberoperaciones que, de producirse, conllevarían la atribución de responsabilidad al Estado, a pesar de haber sido llevadas a cabo, de manera directa o indirecta, efectiva o aparente, por Actores No Estatales, precisamente por ser una manifestación inequívoca de alguno de los dos parámetros descritos en el párrafo anterior. Estas son las siguientes:

[40] Schmitt, M. N. (ed.), Tallinn Manual 2.0, 2017, *op. cit.*, nota 4; Rule 17, cmt. 1.

[41] *Ibíd*; cmt. 2.

[42] *Ibíd*; cmt. 3.

1. Las ciberoperaciones realizadas por Actores No Estatales siguiendo instrucciones emitidas por un Estado.[43] Esto generalmente se produce en contextos en los que el Actor No Estatal se entiende que desempeña una función de entidad auxiliar *de facto* del Estado en cuestión, por necesidad o por conveniencia. Con lo cual, se desprende que, si la ciberoperación llevada a cabo ha seguido instrucciones dadas por un Estado, por extensión dicha conducta ha sido autorizada por éste.

2. Las ciberoperaciones realizadas por Actores No Estatales por requerimiento de un Estado.[44] Tal y como sucede en la circunstancia 1, esta situación también se caracteriza por la naturaleza eventualmente fáctica de entidad auxiliar que reviste al Actor No Estatal en cuestión respecto del Estado que, por necesidad o conveniencia, le ha requerido el desarrollo de la ciberoperación que corresponda. Pueden producirse, o no, bajo un contexto de amenaza del Estado al Actor No Estatal para que las desarrollen.

3. Las ciberoperaciones realizadas por Actores No Estatales en cumplimiento de un contrato celebrado con un Estado para llevarlas a cabo.[45] Se entiende que la petición formal de un Estado a un Actor No Estatal para llevar a cabo ciberoperaciones ilícitas manifestada a través de un contrato genera responsabilidad internacional por la ciberoperación desarrollada al Estado contratante. El comentario 7 a la Regla 17 añade, además, que es necesario, para poder atribuir responsabilidad al Estado, "que este dirija el proceso" de desarrollo de las ciberoperaciones. Esto puede tener lugar de dos formas: o bien, posteriormente, guiando y coordinando el proceso en consecución de este objetivo; o bien, anteriormente, estableciendo o imponiendo por medio del contrato mencionado el *modus operandi*, en una praxis susceptible de ser considerada como de "dirección diferida". En cualquier caso, cumpliría este requisito de "dirección" sutilmente incorporado en este comentario indicado.

4. Las consecuencias en forma de daño sobrevenido causadas por Actores No Estatales a terceros Estados en el desarrollo de una ciberoperación ─o contramedida─, legal o ilegal, que se efectuaba bajo dirección o instrucción de un Estado.[46] Puesto que el Estado

[43] *Ibíd*; cmt. 4.

[44] *Ibíd*.

[45] *Ibíd*; cmt. 7.

[46] *Ibíd*; cmt. 12.

estaba al mando de las ciberoperaciones que este Actor No Estatal debía realizar, se le debe atribuir la responsabilidad de cualquier efecto derivado no previsto.

5. Las ciberoperaciones llevadas a cabo por Actores No Estatales consideradas como *ultra vires*, únicamente "si constituyen una parte esencial de la operación" sobre la que el Estado ejerce un "control efectivo".[47] Cuando esto sucede, "la atribución se produce incluso si el Actor No Estatal ignora o desobedece las instrucciones que el Estado ha dado para la realización de la operación concreta". Esto es, cuando un Actor No Estatal se excede mediante su actuación de las funciones o actividades indicadas por un Estado en un contexto de "control efectivo" por parte de éste, si la ciberoperación *ultra vires* es considerada "esencial" para llevar a cabo la instrucción ─o el objetivo de la instrucción─ que el Estado ha dado al Actor No Estatal, entonces procede la atribución de responsabilidad al Estado. Como "esencial" debe entenderse aquella actuación que supone una condición *sine qua non* para el desarrollo de la medida ordenada; esto es, aquella ciberoperación sin la cuál no sería posible ─o no hubiera sido posible─ lograr el objetivo previsto.

6. Las ciberoperaciones que, aun no habiendo podido ser atribuidas a un Estado por inexistencia de vínculo de imputación ─esto es, entre su origen y su efectuación─ entre un Estado y un Actor No Estatal, hayan sido reconocidas y adoptadas como propias por un Estado.[48] Se prevé, incluso, que un Estado pueda reconocer y adoptar tan sólo parcialmente la actuación efectuada por Actores No Estatales. Ambas situaciones están inspiradas en el artículo 11 de *Responsibility of States for Internationally Wrongful Acts* (2001), que se articula en los términos indicados en el apartado 3.1. No obstante, para que tenga lugar la atribución se requiere "algo más que el mero respaldo o aprobación ─tácita o expresa─" a las ciberoperaciones que han tenido lugar. Debe haber una involucración manifiesta del Estado en ─o ante─ la ciberoperación ocurrida, que puede materializarse a través de hechos constitutivos de defensa y soporte de la misma. Un ejemplo que se menciona en los comentarios a la Regla 17 es la puesta a disposición de capacidades cibernéticas, por parte de un Estado a un Actor No Estatal, de manera intencionada, para protegerlo de las posibles contramedidas que pueda sufrir como consecuencia de la ciberoperación controvertida realizada, o por tal de facilitar el

[47] *Ibíd*; cmt. 13.

[48] *Ibíd*; cmt. 15.

desarrollo futuro de más ciberoperaciones similares ─esto es, de la perpetuación en el tiempo de la ciberoperación ilícita o de los efectos de la misma─. En este caso, la atribución se aplicará de manera estricta. Sin embargo, este planteamiento entraña un asunto ciertamente controvertido, arriesgado y comprometido por lo que a la materia atributiva respecta, y es que podría darse el caso de Estados que pretendiesen "utilizar" o "valerse" de Actores No Estatales para emprender ciberoperaciones internacionalmente ilícitas y luego sencillamente rechazasen dotarles de cualquier tipo de protección. De este modo viciado podría conseguirse el objetivo deseado de perpetrar un ciberacto ilícito y, a su vez, evitar una situación en la que la atribución resultase imperativa por ausencia de materialización fáctica de la asunción como propios de los hechos ocurridos por parte del Estado, en los términos descritos anteriormente. Otras cuestiones derivadas, tales como qué sucedería, en materia atributiva, si la capacidad para la defensa posterior del Actor No Estatal se proporcionase antes incluso de que se llevase a cabo el ciberacto internacionalmente ilícito, siguen aún sin tener respuesta.

7. Las ciberoperaciones realizadas por Actores No Estatales sobre las que un Estado ejerce un "control efectivo". Esto incluye aquellas ciberoperaciones que son "dirigidas o controladas" por un Estado.[49] En relación con su carácter, se puede entender tanto que funciona como cláusula de cierre en esta enumeración de circunstancias en las que la existencia de las cuales se entiende genera atribución, como que resulta el único parámetro a partir del cual, dada su naturaleza holgada, se articulan todas las circunstancias atributivas anteriores ─a excepción de la situación atributiva Nº6─. El hecho de se especifique que es el "control efectivo" el grado de incidencia de un Estado sobre un Actor No Estatal que se requiere para atribuirle la responsabilidad es otra de las precisiones que aporta la Regla 17, como *Lex Specialis*, al artículo 8 de la Comisión de Derecho Internacional. El concepto de "control efectivo", que proviene de la resolución de la CIJ en el caso *Nicaragua*, se analizará detenidamente en el apartado 4.1.

Paralelamente, los comentarios a la Regla 17 del Manual de Tallinn 2.0 también incorporan una relación de circunstancias que pueden producirse en el ciberespacio entre Estados y Actores No Estatales y que se caracterizan por no ser susceptibles de generar, por sí solas, responsabilidad a un Estado. Estas son las siguientes:

[49] *Ibíd*; cmt. 5-6.

a) El apoyo general de un Estado a un Actor No Estatal.[50]

b) El apoyo general de un Estado a la ciberoperación realizada por un Actor No Estatal.[51]

c) El mero fomento, incitación, ánimo, exhortación, motivación, estimulación o aliento de un Estado a un Actor No Estatal para realizar una ciberoperación específica.[52]

d) Los actos de un Estado que complementen a las ciberoperaciones llevadas a cabo por un Actor No Estatal.[53]

e) El mero suministro por parte de un Estado de herramientas susceptibles de ser potencialmente empleables por un Actor No Estatal en el desarrollo de una ciberoperación.[54]

f) El desarrollo por parte de un Estado de una función particular en el proceso de efectuación de la ciberoperación por parte de un Actor No Estatal.[55]

g) La participación preponderante o decisiva de un Estado en la financiación, organización, capacitación, suministro y equipamiento, selección de sus objetivos ─ya sean militares o paramilitares─ o en la planificación de la operación ─aun siendo esta total─ de los Actores No Estatales en cuestión.[56]

h) La mera propiedad estatal de una empresa, sobre la que no se ha podido reunir las condiciones para ser considerada como un órgano de este Estado en cuestión ─de lo contrario, resultaría de aplicación la Regla 15─, que efectúa ciberoperaciones internacionalmente ilícitas.[57]

i) Las ciberoperaciones que constituyen actos *ultra vires*; esto es, aquellas que son desarrolladas por Actores No Estatales excediéndose en el ejercicio de su actividad o

[50] *Ibíd*; cmt. 8.

[51] *Ibíd*.

[52] *Ibíd*.

[53] *Ibíd*.

[54] *Ibíd*.

[55] *Ibíd*.

[56] *Ibíd*; cmt. 9.

[57] *Ibíd*; cmt. 10.

sus funciones, o excediéndose de los límites que le marca la Ley.[58] Aun así, el Grupo Internacional de Expertos advirtió que la aplicación de este principio general puede llegar a ser tan compleja en la práctica "que conviene que cada caso se evalúe separadamente, en base a sus propios hechos".

j) Las ciberoperaciones que desarrollan Actores No Estatales al margen de las instrucciones que un Estado les ha indicado.[59] Constituiría una variación de la situación descrita en "i)" debido al carácter *ultra vires* de la ciberoperación realizada, en la que se constataría que no se puede atribuir responsabilidad a un Estado por una ciberoperación llevada a cabo bajo la única voluntad, criterio y decisión del Actor No Estatal en cuestión, por inexistencia de vínculo de imputación ─esto es, entre instrucción y desarrollo─ entre ambos, por lo que a la ciberoperación controvertida respecta.

Todas estas situaciones anteriores han sido indicadas expresamente por el Grupo Internacional de Expertos en el Manual de Tallinn 2.0 como circunstancias que resultan *per se* insuficientes para establecer atribución. En cualquier caso, como esta enumeración claramente no es exhaustiva, se puede entender que cualquier ciberoperación que no cumpla por completo la cláusula de cierre descrita para las operaciones que sí generan atribución ─esto es, aquellas ciberoperaciones sobre las que el Estado ejerza un "control efectivo"; situación atributiva Nº7─ no le genera responsabilidad internacional a éste.

No obstante, es ciertamente importante tomar en consideración el hecho de que, a pesar de que estas últimas situaciones descritas no generen *per se* atribución de responsabilidad, esto no significa que el Estado no pueda ser responsable de su apoyo al Actor No Estatal en cuestión si efectivamente este presunto apoyo es constitutivo en sí mismo de una vulneración de una regla o principio previsto en el Derecho Internacional ─por ejemplo, una violación del principio de no intervención del Estado, en los términos establecidos en la Regla 66 del Manual de Tallinn 2.0─.[60] [61]

[58] *Ibíd*; cmt. 11.

[59] *Ibíd*; cmt. 12.

[60] *Ibíd*; cmt. 9.

[61] *Ibíd*; cmt. 19.

3.3. La proliferación de declaraciones nacionales: un enfoque actual a través del estado de la cuestión.

La utilización cada vez más frecuente del ciberespacio para desarrollar todo tipo de pretensiones en relación con terceros Estados ha comportado que la ciberseguridad devenga una cuestión de la máxima importancia para la seguridad nacional. Y, ante esto, dada la rapidez de los avances tecnológicos en relación con una evolución del Derecho ─especialmente el Internacional─ mucho más lenta en comparación, ha resultado inevitable que proliferen declaraciones estatales sobre la aplicabilidad del Derecho Internacional a las ciberoperaciones, así como de planes de estrategia nacional sobre ciberseguridad.[62]

En este apartado se presenta un enfoque actual a través del estado de la cuestión por medio de las recientes declaraciones que han llevado a cabo dos países europeos por lo que al asunto de la atribución de la responsabilidad respecta: la República Francesa y el Reino de los Países Bajos.

3.3.1. República Francesa.

Francia ha emitido recientemente *Droit international appliqué aux opérations dans le cyberespace* ─en castellano: Derecho internacional aplicado a las operaciones en el ciberespacio─. Se trata de una declaración publicada el 9 de septiembre de 2019 por el Ministerio de las Fuerzas Armadas de la República Francesa que constituye, tal y como se indica en su introducción, una respuesta al creciente número de amenazas que se efectúan por medio del ciberespacio, que supone, a su vez, un aumento de la vulnerabilidad de los Estados en este ámbito. Mediante esta, Francia pretende aclarar su posición sobre la aplicación del Derecho Internacional a las operaciones cibernéticas, dejando claro, en todo momento, que el respeto a las obligaciones internacionales contraídas por Francia son la base de esta declaración.[63]

Sobre la cuestión de la atribución de la responsabilidad, se indica que, siendo conscientes de que las ciberoperaciones "son, por naturaleza, difíciles de caracterizar en el ciberespacio" ─debido al carácter anónimo que caracteriza a su operatividad─; tomando en

[62] García Segura, 2020, *op. cit.*, nota 5, p.38.

[63] Ministère des Armées; RÉPUBLIQUE FRANÇAISE. (2019). *Droit international appliqué aux opérations dans le cyberespace*. https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf, p.4.

consideración "la dificultad de rastrear y controlar las actividades" que en él se llevan a cabo; observando "la participación cada vez mayor de agentes no estatales"; y conociendo "las posibilidades que se ofrecen a los Estados de utilizar a estos agentes privados como intermediarios para desarrollar actividades maliciosas", por tal de evitar "la particularmente difícil tarea de identificación de los autores y promotores" de estas ciberoperaciones, para Francia "la atribución de un ciberataque de origen estatal es una decisión política nacional".[64]

Además, en esta declaración se menciona el modo con el que Francia tiene previsto determinar la identidad del instigador de la ciberoperación internacionalmente ilícita. Lo hace en base a los "elementos técnicos reunidos durante las investigaciones del ataque cibernético, incluida la determinación de la infraestructura de ataque y de tránsito de la operación cibernética y su ubicación", en función de "la identificación de los modos de operación adversos, la cronología general de las actividades del autor, el alcance y la gravedad del incidente y el perímetro comprometido", y, además, toman en consideración para ello "los efectos buscados por el atacante". Estos parámetros también son utilizados para determinar la existencia ─o no─ de un vínculo entre quien ha efectuado la ciberoperación y un Estado en concreto.[65]

En relación con la tarea atributiva propiamente dicha, se establece que una ciberoperación será considerada como realizada por un Estado cuando: (a) haya sido llevada a cabo "por uno de sus órganos" ─tal y como establece el artículo 4 de *Responsibility of States for Internationally Wrongful Acts* (2001)─; (b) haya sido efectuada "por una persona o entidad que ejerza autoridad gubernamental" ─artículo 5 del citado texto de Naciones Unidas─, o (c) haya sido desarrollada "por una persona o grupo de personas que actúan siguiendo instrucciones o directrices, o bajo el control de ese Estado" ─basado en el ya mencionado artículo 8─.[66] Con lo cual, resulta indiscutible que Francia se basa en la redacción y establecimiento de esta declaración nacional en el Derecho Internacional vigente.

Y, además, se indica que "la identificación de un Estado como responsable de un ataque cibernético que constituye un hecho internacionalmente ilícito no obliga al Estado lesionado a hacer una atribución pública".[67] De este modo, Francia "se reserva el derecho de atribuir

[64] Ministère des Armées; RÉPUBLIQUE FRANÇAISE, 2019, *op. cit.*, nota 63, p.10.

[65] *Íbid*; p.11.

[66] *Íbid*.

[67] *Íbid*.

públicamente, o no, un ciberataque del que ha sido víctima, y de poner esta información en conocimiento de su población, de terceros Estados o de la comunidad internacional", sin perjuicio de la cooperación y coordinación que deba ejercer debido a las obligaciones que pueda haber contraído con sus aliados y con Organizaciones Internacionales ─OTAN, por ejemplo─ o Regionales ─la Unión Europea, sin duda─ de las que forme parte.[68]

Finalmente, se establecen dos aspectos realmente atractivos desde el punto de vista atributivo. Por un lado, constata que "el derecho internacional no exige a los Estados que revelen las pruebas en las que se basan para atribuir públicamente un ataque cibernético", con lo cual, se aleja de cualquier polémica o controversia que pueda surgir debido a la falta de argumentación consciente e intencionada en el momento de llevar a cabo una atribución pública sobre una ciberoperación perpetrada.[69] Y, por otro lado, una consideración realmente significativa en la práctica: en la declaración, Francia considera como "ciberataque" a toda "operación cibernética llevada a cabo por un Estado contra los intereses del Estado francés".[70] La relevancia de esta consideración yace en el hecho de que, ante esto, cualquier ciberoperación que sufra Francia, al poder tener, por medio de este precepto, la consideración de "ciberataque", abre la puerta al *Ius ad Bellum*; esto es, a todo el sistema de efectuación de contramedidas ─las cuales, añade, podrán efectuarse incluso "ante la falta de atribución pública"─.[71]

3.3.2. Reino de los Países Bajos.

El 5 de julio de 2019, el Ministro de Asuntos Exteriores de los Países Bajos envió una Carta al Presidente de la Casa de Representantes de este país abordando la cuestión de la aplicabilidad del orden jurídico internacional en el ciberespacio, tal y como se había comprometido previamente, en una sesión plenaria acerca del espionaje de Rusia, celebrada el 20 de diciembre de 2018.[72]

---

[68] *Íbid*.

[69] *Íbid*.

[70] *Íbid*; p.18.

[71] *Íbid*; p.11.

[72] Ministry of Foreign Affairs of the Kingdom of the Netherlands. (2019a). *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace.* https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, p.1.

Esta Carta consta de un Apéndice en el que se exponen las principales normas de Derecho Internacional que se aplican en el ciberespacio, así como la interpretación que hace de ellas el Gobierno neerlandés. Proporciona, además, una síntesis sobre el estado actual de distintas cuestiones normativas del ámbito de las ciberoperaciones que conciernen a los Países Bajos tanto a nivel internacional como a nivel interno.[73]

En cuanto a la atribución de responsabilidad, se establece en este Apéndice que, para que un Estado sea considerado responsable de una operación internacionalmente ilícita, "debe ser posible atribuir la ciberoperación en cuestión a un Estado". Indica, además, que la atribución es una condición necesaria para el emprendimiento de contramedidas. Y la atribución, prosigue, "se basa siempre en una decisión gubernamental".[74]

También se afirma que la decisión política de atribuir la responsabilidad se basa en el grado de información de que dispone el Gobierno acerca de lo ocurrido, pudiendo tomar en consideración tanto información propia como información obtenida por distintos canales externos.[75]

En este Apéndice, el Gobierno neerlandés distingue tres formas distintas de atribución: en primer lugar, una "atribución técnica", que se basaría en el resultado de una "indagación factual y técnica acerca del origen de la ciberoperación perpetrada con un porcentaje elevado de fiabilidad"; en segundo lugar, una "atribución política", que se correspondería con aquella "consideración" que haría el Gobierno neerlandés, sin que de ella se pudiese desprender ningún tipo de consecuencia jurídica, y con independencia de que se haga ─o no─ públicamente; y, en tercer lugar, una "atribución legal", que sería una decisión mediante la cual los Países Bajos reconocerían a un Estado en concreto como "legalmente responsable de una violación de una obligación de Derecho Internacional", a todos los efectos.[76] Y, si bien puede desprenderse de esta distinción entre tipos de atribuciones que no toda atribución requiere estar basada necesariamente en indicios fehacientes provenientes de análisis técnicos e informáticos

[73] Ministry of Foreign Affairs of the Kingdom of the Netherlands, 2019a, *op. cit.*, nota 72, p.3.

[74] Ministry of Foreign Affairs of the Kingdom of the Netherlands. (2019b). *Appendix: International law in cyberspace.* https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, p.6.

[75] Ministry of Foreign Affairs of the Kingdom of the Netherlands., 2019b, *op. cit.*, nota 74, p.6.

[76] *Íbid*.

detallados, sí se establece que deberán aportarse todo tipo de pruebas ante cualquier tribunal internacional que esté conociendo del caso, si esto ocurre, como medio de acreditación de la legitimidad de las contramedidas que puedan haberse llevado a cabo por parte de los Países Bajos amparado en el ejercicio del derecho a la legítima defensa que operaría en tal caso.[77]

En relación con los Actores No Estatales, se establece que, "en principio, un ciberacto de un Actor No Estatal no es atribuible a un Estado", pero que "la situación cambia si hay un Estado que tiene control efectivo sobre este, o bien si lo acepta como propio".[78] Se puede apreciar, pues, como el Gobierno de los Países Bajos incorpora a nivel interno el requisito de la existencia de este grado de control indicado en la Regla 17 del Manual de Tallinn 2.0 para atribuir la responsabilidad por una ciberoperación internacionalmente ilícita a un Actor No Estatal. Además, por otro lado, resulta destacable el hecho de que indique textualmente que un Estado será responsable de una conducta efectuada por un Actor No Estatal en el ciberespacio si "el Actor No Estatal ─o "proxy"─ lleva a cabo la (ciber)operación por instrucción o bajo la dirección o el control de ese Estado", pues es exactamente lo mismo que establece el artículo 8 de *Responsibility of States for Internationally Wrongful Acts* (2001).

También añade que "el umbral para establecer un control efectivo es alto". En este sentido, este Apéndice vuelve a situarse en consonancia con lo dispuesto en la Regla 17 del Manual de Tallinn 2.0, tal y como se verá en el apartado 4. Sin embargo, especifica que en Derecho Internacional no existe ninguna norma de *hard law* mediante la cual se estipule un tipo de control en concreto necesario para atribuir la responsabilidad y que, en este sentido, la CIJ ha aceptado distintos tipos de pruebas ─de control─ según el caso concreto; con lo cual, la posición del Gobierno de los Países Bajos es que "la carga de la prueba efectivamente variará dependiendo de la gravedad del acto que se considere violatorio del Derecho Internacional".[79]

[77] *Íbid*.

[78] *Íbid*.

[79] *Íbid*; p.7.

4. EL GRADO DE CONTROL NECESARIO PARA LA ATRIBUCIÓN DE RESPONSABILIDAD: EL «CONTROL EFECTIVO».

4.1. El concepto de «Control Efectivo»: asunto Nicaragua v. Estados Unidos de América de la Corte Internacional de Justicia.[80]

Si bien en el Grupo Internacional de Expertos que elaboró el Manual de Tallinn 2.0 hubo consenso en que, tal y como se establece en el artículo 8 de *Responsibility of States for Internationally Wrongful Acts* (2001), "el comportamiento de una persona o de un grupo de personas se considerará como un acto de un Estado según el Derecho Internacional si la persona o el grupo de personas actúa de hecho mediante instrucciones o bajo la dirección o el control de ese Estado al llevar a cabo esta conducta en cuestión", y que este precepto era de aplicación en el ámbito de las ciberoperaciones, el Grupo experimentó una patente falta de acuerdo en cuanto al nivel exacto de control que resulta necesario para atribuir a un Estado la responsabilidad por la ciberoperación realizada por un Actor No Estatal.[81]

Finalmente, la posición mayoritaria resultó ser que un Estado debe tener un "control efectivo" sobre los Actores No Estatales en cuestión para poderse proceder a la atribución de responsabilidad. Este concepto que empleó el Grupo Internacional de Expertos ─*effective control threshold*─ proviene de la sentencia de la CIJ en el Caso *Nicaragua*. En él, la Corte trató de determinar la relación entre los Estados Unidos de América y los grupos armados que operaban en el territorio de Nicaragua entre 1981 y 1984, ante la demanda internacional interpuesta por este.

En este caso, la CIJ reconoció que los Estados Unidos, a través de sus funcionarios y oficiales, dieron "soporte logístico, proporcionaron información acerca de la localización y de los movimientos de las tropas *sandinistas*, entregaron métodos sofisticados de comunicación, desplegaron redes de radiodifusión sobre el terreno, entregaron radares…" a los *contras* ─uno de los grupos armados de oposición en contra el Gobierno de Nicaragua─.[82] Además, la CIJ comprobó que, en 1983, el Congreso de los Estados Unidos "previó específicamente fondos para ser utilizados por los servicios de inteligencia de los Estados Unidos para apoyar de manera

[80] International Court of Justice, *Nicaragua v. United States of America*, 1986, *op. cit.*, nota 22.

[81] Schmitt, M. N. (2012). *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*. Harvard International Law Journal, 54 (December 2012), 13-36, p.35.

[82] International Court of Justice, *Nicaragua v. United States of America*, 1986, *op. cit.*, nota 22; para. §106.

directa o indirecta las operaciones militares o paramilitares en Nicaragua"; esto es, a los *contras*.[83] Por todo ello, la CIJ consideró probado que una serie de operaciones militares y paramilitares de los *contras* "fueron decididas y planificadas, si no realmente por los Estados Unidos de América, al menos en estrecha colaboración con ellos".[84]

Sin embargo, aunque se reconoció este soporte que recibieron los *contras* por parte de Estados Unidos, la CIJ consideró que no era convincente que todas las operaciones lanzadas por los *contras* estuvieran basadas en estrategias y tácticas desarrolladas únicamente por los norteamericanos.[85] Por ello, procedió a diseñar un método que permitiera determinar si las fuerzas *contras* actuaron en nombre de los Estados Unidos o, mismamente, si debían ser considerados *de facto* uno de sus órganos. Se presentó del siguiente modo:

> *Procede examinar* […] *si la relación de los contras con el Gobierno de los Estados Unidos era tanto de dependencia por un lado, como de control por otro, que sería correcto equiparar a los contras, a efectos legales, con un órgano del Gobierno de los Estados Unidos, o como si actuaran en nombre de ese Gobierno*.[86]

De este modo, la CIJ estipuló que la determinación del grado de control existente requiere, primero, de un análisis "del control potencial inherente al grado de dependencia de los *contras*" para poder equipararles con un órgano del Gobierno de los Estados Unidos.[87]

Y, sobre esto, la Corte dictaminó que la ayuda que Estados Unidos había prestado a los *contras* no resultaba suficiente para considerar que estos dependieran exclusivamente de ella, sino que, por el contrario, a pesar de la ayuda, "los *contras* seguían constituyendo una fuerza independiente".[88] Y, en consecuencia, se concluyó que, al no poder considerarse que los *contras* eran "completamente dependientes" del soporte prestado bajo estos parámetros, no se podía sostener la tesis de que actuaran en nombre de los Estados Unidos. Este resultado aisladamente insatisfactorio acabaría provocando que la prueba inicialmente observada deviniera bicefálica.

---

[83] *Íbid*; para. §20.

[84] *Íbid*; para. §106.

[85] *Íbid*.

[86] *Íbid*; para. §109.

[87] *Íbid*.

[88] *Íbid*.

Esta primera prueba de control estableció, en palabras de la Corte "un umbral elevado para la atribución de la conducta de los Actores No Estatales a un Estado."[89] Y se debe a que, en ausencia de pruebas fehacientes acerca del vínculo de control entre el Estado y los Actores No Estatales en los términos descritos, resulta imposible atribuir la responsabilidad al Estado. Con lo cual, una de las conclusiones que se puede desprender de la resolución de la Corte fue que el Gobierno de Nicaragua no logró demostrar acertada y adecuadamente ─si es que tenía posibilidades reales de hacerlo─ que los Estados Unidos "realmente ejercieran tal grado de control en todos los ámbitos", requisito imprescindible para haber podido establecer definitivamente que los *contras* actuaban en nombre de los Estados Unidos.[90]

Paralelamente, y en cuanto al *test* aplicado, algunos autores sostienen la tesis de que la CIJ finalmente estableció, en realidad, dos pruebas distintas en el Caso *Nicaragua*: una, ya vista, basada en el concepto de "completa dependencia" y otra, a continuación, basada en el concepto de "control". En este sentido, Abass afirma que el objetivo de la primera es determinar "si los Actores No Estatales que llevaron a cabo el acto ilícito tenían tales vínculos con el Estado en cuestión como para que pueda considerarse que dependían completamente de él", mientras que la segunda pretende esclarecer "si el Actor No Estatal actuó bajo instrucción de un Estado".[91] Y lo justifica precisamente basándose en las palabras de la Corte citadas anteriormente.[92]

Otros autores, como Talmon, también han sostenido esta tesis, razonando que para analizar la atribución de responsabilidad que procedía en el Caso *Nicaragua*, la CIJ se valió de "una interrelación de los conceptos de dependencia y de control".[93] En este sentido, argumenta que "el control es el resultado de la dependencia o, mirándolo desde el otro lado, la dependencia crea el potencial de control". Y que, por ende, debe considerarse que "la dependencia y el control son […] dos caras de la misma moneda".[94]

---

[89] *Íbid*.

[90] *Íbid*; para. §115.

[91] Abass, A. (2008). *Proving State Responsibility for Genocide: The ICJ in Bosnia v . Serbia and the International Commission of Inquiry for Darfur*. Fordham International Law Journal, 31(4), 871-910, p.891.

[92] *Cit.* 86.

[93] International Court of Justice, *Nicaragua v. United States of America*, 1986, op. cit., nota 22; para. §106-115.

[94] Talmon, S. (2009). *The responsibility of outside powers for acts of secessionist entities*. International and Comparative Law Quarterly, 58(3), 493-517. https://doi.org/10.1017/S0020589309001171, p.497.

Siguiendo esta línea, Talmon sostiene que la CIJ encara la cuestión de la atribución de responsabilidad basándose en un enfoque el análisis del cual debe resultar en la medición relativa de la dependencia y del control; y que, por ello, introduce el concepto de "grado": el "grado de dependencia" hace referencia al nivel existente de subordinación necesaria del Actor No Estatal al Estado en cuestión, mientras que el "grado de control" se podría definir como la intensidad con la que el Estado ejerce su poder sobre el Actor No Estatal.[95] Y, partiendo de que ambos conceptos resultan estar interrelacionados, afirma que la Corte distinguió dos grados distintos de control–dependencia: un "control estricto", basado en una "dependencia completa", y un "control efectivo", en casos de "dependencia parcial".[96] De este modo afloran dos pruebas de control que pueden denominarse, en base a su carácter, prueba de "control estricto" y prueba de "control efectivo", y que acabarían materializándose más de una década más tarde en el nivel de control necesario, en primer lugar, para la atribución de actos internacionalmente ilícitos desarrollados por órganos de un Estado o entidades cuya analogía a ellos se haya constatado y, en segundo lugar, para la atribución de actos internacionalmente ilícitos desarrollados por Actores No Estatales; esto es, en el nivel de control que requiere el artículo 4 y el artículo 8 de *Responsibility of States for Internationally Wrongful Acts* (2001), respectivamente.[97]

Prestando atención, en primer lugar, a la prueba de "control estricto", debe entenderse que el primer ejercicio atributivo que hizo la Corte fue tratar de determinar si realmente había habido un vínculo entre Estados Unidos y los *contras* tal que pudiera considerarse que los segundos tenían una relación de "dependencia y control completos" respecto del primero y que, en consecuencia, se pudiera entender que los *contras* actuaron *de facto* como un órgano de los Estados Unidos. Pero, como se ha indicado anteriormente, la CIJ consideró que las pruebas para considerar que los Estados Unidos realmente se habían valido mediante acciones concretas de ese "potencial completo de control" ─que sí quedo acreditado─ fueron insuficientes; esto es, no se pudo probar que los Estados Unidos, aprovechando el "potencial de control" que tenían, lo materializaran y ejercieran realmente sobre los *contras* según sus intereses u objetivos.[98]

[95] Talmon, 2009, *op. cit.*, nota 94; p.498.

[96] *Íbid*.

[97] Crawford, J. (2013). *State Responsibility: The General Part*. Cambridge University Press, Annexed to GA Resolution 56/83 of 2001, the International Law Commission's Articles on the Responsibility for Internationally Wrongful Acts. https://doi.org/https://doi.org/10.1017/CBO9781139033060, p.125.

[98] International Court of Justice, *Nicaragua v. United States of America*, 1986, op. cit., nota 22; para. §110-114.

Así, habiendo descartado que pudiera proseguir con éxito un ejercicio de consideración por analogía de los *contras* como un órgano de los Estados Unidos, y debido al fracaso *per se* del intento de constatación o demostración de la existencia de un vínculo de "dependencia completa" entre ambos sujetos ─que habría implicado, sin duda, un alcance más amplio en el ejercicio de atribución de la responsabilidad internacional─, se procedió a analizar el concepto de "dependencia parcial". Este concepto fue el resultante de la efectuación de la "prueba de control efectivo" por parte de la Corte, al indicar esta que, para que la conducta llevada a cabo por los *contras* diera lugar a la atribución de la responsabilidad jurídica a los Estados Unidos, "en principio habría que demostrar que este Estado tenía el control efectivo de las operaciones militares o paramilitares en el curso de las cuales se cometieron las presuntas transgresiones" y descartar, así, que "estos actos hubieran sido cometidos por los *contras* sin el control de los Estados Unidos". [99]

Se podría decir, por tanto, que la "prueba de control efectivo" se concreta en el hecho de analizar la responsabilidad de un Estado solamente por los actos de los Actores No Estatales sobre los que dicho Estado tiene un control efectivo, y que por ello se basa en la indagación acerca de los vínculos puntuales que materializan la "dependencia parcial" que existe por parte del Actor No Estatal en relación con el Estado, tal y como se ha indicado anteriormente. Y esto se tradujo, en el Caso *Nicaragua*, en que, seguidamente, la CIJ declarase que "los *contras* son responsables de sus actos", y que los Estados Unidos "no son responsables de los actos de los *contras*, sino de su propia conducta con respecto a Nicaragua, incluida la conducta llevada a cabo relacionada con los actos de los *contras*".[100]

Pero una vez aplicada esta "prueba de control efectivo", la Corte volvió a rechazar que se pudiese atribuir la responsabilidad a los Estados Unidos ─tal y como hizo previamente, tras aplicar la "prueba de control estricto"─; de nuevo, por falta de evidencias provenientes de pruebas fehacientes y demostraciones concluyentes en este sentido. Lo expresó de este modo: esta Corte "no encuentra fundamento para concluir que los actos de esa índole que puedan haberse cometido sean imputables a los Estados Unidos de América como actos de los Estados Unidos de América".[101]

---

[99] *Íbid*; para. §115.

[100] *Íbid*; para. §116.

[101] *Íbid*; Fallo, (9).

Cassese sostiene que la "prueba de control efectivo" representa lo que denomina "la prueba de exigencia" ante actos internacionalmente ilícitos realizados por Actores No Estatales cuando un Estado está involucrado en ellos; esto es, el "único criterio aplicable" a actos que tienen lugar en estas circunstancias.[102] Explica, además, que la CIJ entiende que se cumple este criterio de "control efectivo" o bien si el Estado imparte instrucciones para el desarrollo de actos ilícitos específicos al Actor No Estatal en cuestión ─esto es, que el Estado le ordene la efectuación de estas operaciones─; o bien si el Estado involucrado hace cumplir cada instrucción específica al Actor No Estatal ─esto es, que el Estado obligue al Actor No Estatal a llevar a cabo las operaciones indicadas─.[103] Este mismo planteamiento fue hecho por el Grupo Internacional de Expertos que elaboró en 2017 el Manual de Tallinn 2.0, al establecer, basándose en lo expuesto en el Caso *Nicaragua*, que "un Estado está en control efectivo de una operación cibernética determinada por un Actor No Estatal cuando es el Estado el que determina la ejecución y el curso de la operación concreta, y cuando la actividad cibernética realizada por el Actor No Estatal es parte integrante de esa operación".[104]

Así pues, la "prueba de control efectivo", a pesar de que constituye en sí un mecanismo atributivo cuyo alcance es, en comparación con la "prueba de control estricto", más limitado por lo que respecta a la determinación de la responsabilidad internacional mediante una revisión exhaustiva de los hechos; y cuyos requerimientos constatativos a través de pruebas son, del mismo modo, relativamente más limitados y específicos, puesto que se reducen a casos concretos de ejercicio de control real sobre la conducta del Actor No Estatal, sigue siendo una prueba altamente exigente. Esta visión la describió muy acertadamente Talmon al afirmar que "aunque la carga de la prueba en la prueba de control efectivo es menor que en la prueba de control estricto, en la práctica será extremadamente difícil de establecer".[105]

Y esta consideración tiene su fundamento en el hecho de que, a diferencia de lo que sucede en la "prueba de control estricto", donde la supuesta dependencia que se trata de examinar es completa y, en consecuencia, tal es la potencial atribución de responsabilidad en caso de tener lugar, en la "prueba de control efectivo", puesto que el grado de control que se

[102] Cassese, A. (2007). *The Nicaragua and Tadić Tests revisited in light of the ICJ judgment on genocide in Bosnia*. European Journal of International Law, 18(4), 649-668. https://doi.org/10.1093/ejil/chm034, p.653.

[103] Cassese, 2007, *op. cit.*, nota 102; p.657.

[104] Schmitt, M. N. (ed.), Tallinn Manual 2.0, 2017, *op. cit.*, nota 4; Rule 17, cmt. 6.

[105] Talmon, 2009, *op. cit.*, nota 94; p.503.

debe acreditar se basa en una dependencia parcial, el Estado denunciante tiene la carga de la prueba de todos y cada uno de los actos concretos en los que aspire a atribuir la responsabilidad al Estado demandado. Esto es, aplicado al caso en cuestión, Nicaragua debió aportar el máximo número posible de pruebas concluyentes sobre todos y cada uno de los actos en los que, de forma desagregada, reclamó atribuir la responsabilidad a los Estados Unidos, constituyendo, sin duda, un ejercicio de notoria y palpable dificultad fáctica y de compleja consecución.

Los Estados Unidos fueron finalmente considerados responsables de la conducta que ejercieron en relación con los *contras*; esto es, por "entrenar, armar, equipar, financiar y suministrar a las fuerzas *contras*" así como por "alentar, apoyar y ayudar a las actividades militares y paramilitares en y contra Nicaragua". Y, en consecuencia, Estados Unidos fue condenado por "violación de la obligación, con arreglo al Derecho Internacional consuetudinario, de no intervenir en los asuntos de otro Estado". [106] Asimismo, fue condenado por la Corte por "violación de la obligación, con arreglo al Derecho Internacional consuetudinario, de no utilizar la fuerza contra otro Estado".[107] Y, además, fue considerado responsable de elaborar el "manual" *Operaciones psicológicas en Guerra de guerrillas* y difundirlo entre los *contras*, por "alentar la comisión de actos contrarios a los principios generales del Derecho humanitario".[108]

4.2. Análisis de su aplicabilidad en el campo de las ciberoperaciones.

El Grupo Internacional de Expertos consideró que el nivel de control necesario que debe existir ─y acreditarse─ para poder atribuir responsabilidad internacional a un Estado por una ciberoperación internacionalmente ilícita es el "control efectivo" por parte del Estado respecto del Actor No Estatal en cuestión. Pero, como se ha podido constatar en el apartado anterior, demostrar la dependencia y el control real que un Estado puede tener en cada una de las ciberoperaciones que un Actor No Estatal lleva a cabo a través de un umbral tan restrictivo es muy difícil, si no imposible, puesto que resulta extremadamente complejo probar la capacidad real de controlar, dirigir y modificar la conducta que un Estado puede tener sobre el perpetrador de una ciberoperación. Y esto se agrava si se tiene en cuenta que las ciberoperaciones se llevan a cabo en el contexto de secretismo y anonimato que caracteriza al ciberespacio.

[106] International Court of Justice, *Nicaragua v. United States of America*, 1986, op. cit., nota 22; Fallo, (3).

[107] *Íbid*; Fallo, (4).

[108] *Íbid*; Fallo, (9).

Uno de los motivos por los que la CIJ consideró que los *contras* no dependían de los Estados Unidos fue que, tras el cese de envío de soporte en forma de asistencia financiera por parte de los norteamericanos a los *contras*, estos continuaron operando del mismo modo en Nicaragua. Pero resulta elemental tomar en consideración, por un lado, que siguieron actuando del mismo modo porque era el modo con el que se les había instruido por parte de Estados Unidos ─no hay que perder de vista que la elaboración del "manual" *Operaciones psicológicas en Guerra de guerrillas* y su difusión entre los *contras* quedó probado─. Pero además, por otro lado, se plantea la cuestión de si realmente hubieran podido continuar actuando de este modo los *contras* si no hubieran recibido el gran soporte económico que recibieron desde un inicio por parte de los Estados Unidos.

La respuesta, intuitivamente, es que si siguieron actuando de este modo tras el cese de la asistencia económica, fue, sobre todo, porque ya tenían los recursos suficientes como para poder seguir desarrollando de manera autónoma las actuaciones que ya venían llevando a cabo; esto es, un ejercicio de armar, instruir y desarrollar un *modus operandi* susceptible de ser denominado como de trabajar por la creación de un grupo cuyos intereses estuvieran alineados con los de Estados Unidos, que pudieran valerse de medios que fueran incluso ilícitos por tal de conseguir estos objetivos, pero cuya independencia fuera aparente. Y, en consecuencia, se puede plantear la duda de si el cese de ayuda por parte de los Estados Unidos en un momento concreto tiene relación con el hecho de que, a partir de ese momento, los *contras* ya podían actuar con autonomía de recursos. O, dicho de otro modo, se plantea la duda de si los Estados Unidos realmente financiaron, instruyeron y dirigieron a los *contras* hasta el preciso momento en que ellos pudieran actuar con autonomía ─que no quiere decir "con independencia"─.

Y, en este punto, llevando esto al ámbito de las ciberoperaciones, cabe plantearse lo siguiente: si un Estado se vale de un Actor No Estatal para llevar a cabo ciberoperaciones internacionalmente ilícitas, de tal modo que actúa de forma encubierta a través de él, y le dota de la financiación suficiente como para que pueda desarrollar estas ciberoperaciones contra un objetivo en concreto durante un período de tiempo determinado, esta "prueba de control efectivo" resultaría ineficaz e inservible en la práctica, en la gran mayoría de casos, para atribuir la responsabilidad. Sobre todo, porque deviene tremendamente difícil determinar y probar el vínculo que hay entre ambos actores en el ciberespacio. De modo que el establecimiento de una prueba de esta índole, con estas características y exigencias, con el tipo de probatoria que

requiere para atribuir la responsabilidad, supone una perpetuación de la situación de indefensión y vulnerabilidad que agrava aún más la que ya de por sí tenía el Estado damnificado.

Pero, además, esta indefensión persiste si se tiene en cuenta que el éxito atributivo, cuando este se lleva a cabo por medio de la "prueba de control efectivo", en los términos establecidos en el apartado 4.1, depende en excesiva medida de los recursos de los que disponga el Estado damnificado, pues es este quien tiene la carga de la prueba; esto es, quien debe demostrar el vínculo entre el Actor No Estatal y el Estado que hay detrás en todas y cada una de las ciberoperaciones ilícitas que se efectúen. En consecuencia, si el Estado damnificado tiene a su alcance una gran red de servicios tecnológicos de vanguardia con los que indagar acerca del daño sufrido puede resultarle mucho más fácil acceder a determinadas pruebas que usar para atribuir responsabilidad. E, inversamente, si es el Estado que ordena la ciberoperación a través de un Actor No Estatal quien dispone de estos recursos, le será claramente más sencillo perpetrar la ciberoperación con el menor rastro posible y poder destruir todo tipo de indicios, vestigios o pistas que puedan ser utilizados por el damnificado como prueba para conseguir la atribución.

Con lo cual, el éxito en la acreditación de hechos a través de la "prueba de control efectivo" se sustenta enormemente en el nivel de recursos ─tecnológicos, pero también financieros y económicos─ de que dispongan los actores y, por ende, el resultado final de la efectuación de la "prueba de control efectivo" va a ser necesariamente parcial y sesgado, puesto que se habrá valorado, no en base a la verdad y a la realidad ocurrida, sino en base a la capacidad potencial que, como se ha indicado, en función de los recursos de los que dispone ─o puede disponer─, tenga el Estado en materia probatoria.

Y esto genera una vulnerabilidad que se acentúa más aún si se tiene en cuenta que los Estados con mayor potencial informático, técnico y digital ─y defensivo─ a su alcance están emitiendo declaraciones ─como se ha visto en el apartado 3.3─ mediante las que se reservan el derecho a atribuir la responsabilidad a otros Estados según sus propios criterios, lo que implica que aquellos que carezcan de este potencial se verán obligados a buscar el amparo de la Comunidad Internacional, como, por ejemplo, acudiendo ante la CIJ, la cual se vale de esta "prueba de control efectivo" que les es desfavorable por lo que respecta a los medios a emplear en relación con los objetivos esperados ─esto es, realizar una inversión de recursos inmensamente costosa para tratar de demostrar un vínculo sin la certeza de conseguir acreditarlo exitosamente─.

Esto conduce a considerar que quizá la "prueba de control efectivo" es demasiado estricta, demasiado restrictiva, y que habría que tratar de expandir el umbral de lo que se debe entender como "control efectivo". Y esto, en sí, no sería algo descabellado desde el momento en que este ejercicio de ampliar la prueba de control es algo que la misma CIJ llevó a cabo en el Caso *Nicaragua*, después de comprobar que el primero de sus *tests* ─la "prueba de control estricto"─, como su nombre indicaba, era lo suficientemente restrictivo como para impedir la atribución de todo tipo de responsabilidad. De este modo, se puede llegar a considerar que, en el hecho de que el Grupo Internacional de Expertos reconociese consensuadamente que el grado de control necesario que debía haber para atribuir responsabilidad a un Estado fuera el de "control efectivo", hay intrínseca la aceptación y reconocimiento de que el primer *test* no iba a poder aplicarse, y que, en consecuencia, hubiera resultado estéril e inútil, por ser extremadamente restrictivo.

Pero, ¿qué sucede si, en la práctica, la realidad es que la "prueba de control efectivo" sigue resultando tremendamente restrictiva? Para ser justa, puesto que en el Manual de Tallinn 2.0 se indica que el "control efectivo" es el grado de dependencia estipulado para atribuir responsabilidad a un Actor No Estatal, debería tenderse hacia la ampliación del umbral de lo que, por medio de este concepto, se puede entender como "control efectivo".[109]

[109] Schmitt, M. N. (ed.), *Tallinn Manual 2.0*, 2017, *op. cit.*, nota 4; Rule 17, cmt. 6.

CAPÍTULO III

LA NECESIDAD DE REFORMAR LOS CRITERIOS DE ATRIBUCIÓN DE LA RESPONSABILIDAD EN EL CIBERESPACIO.

«Todo aquél que desee el éxito constante debe cambiar su conducta con los tiempos.»

NICOLÁS MAQUIAVELO, *El príncipe*.

5. HACIA UNA INTERPRETACIÓN EXTENSIVA DE LA REGLA DE «CONTROL EFECTIVO».

Como se ha indicado, el Manual de Tallinn 2.0 incorpora, en forma de cláusula de cierre en el conjunto de circunstancias previstas para la atribución de responsabilidad, la regla de "control efectivo"; esto es, será posible la atribución de responsabilidad a un Estado siempre que se demuestre que este ha ejercido tal nivel de control sobre el Actor No Estatal en cuestión por lo que respecta al desarrollo y efectuación de la ciberoperación internacionalmente ilícita que ha tenido lugar. Pero, ¿qué sucede si mediante esta regla no se puede atribuir finalmente la responsabilidad a un Estado en estos términos? Y, ¿qué sucede en estos casos, cuando, además, la ciberoperación en cuestión se efectúa en tiempos de paz; cuando no resulta aplicable, por sus características o efectos, el *ius ad bellum*; y cuando esta ciberoperación no puede ser considerada como "uso de la fuerza"? Para responder a esta cuestión, hay que tomar en consideración lo siguiente.

La realidad es que, en primer lugar, como se ha visto en el apartado 1.1, el ciberespacio se está consolidando como "el quinto campo de batalla", y constituye hoy en día un dominio estratégico en el que los Estados miden sus fuerzas e interactúan con todo tipo de intenciones. Y este tipo de operaciones van a ser cada vez más frecuentes.[110]

En segundo lugar, hay que tomar en consideración que la tecnología avanza a ritmos vertiginosos, y que las formas de realizar una intervención ilícita de un Estado en un tercer Estado a través del ciberespacio ─con objetivos tales como causar desconcierto, confusión o

[110] Moussu, N., Llouquet, A.-L., & Chaumei, G., 2011, *op. cit.*, nota 7; p.32.

incluso destrucción─ van a ser cada vez más sofisticadas: el modo de llevarlas a cabo será cada vez más sutil, su resultado será, como mínimo, igualmente contundente y, sin embargo, cada vez será más difícil acabar pudiendo determinar el vínculo entre el Estado y el Actor No Estatal a través del que actúa de manera encubierta, puesto que el perpetrador pondrá cada vez más énfasis en no dejar rastro de la efectuación de la ciberoperación ─o en dejar el mínimo posible─.

Y, en tercer lugar, se debe tener en cuenta que si un Estado ha sufrido una ciberoperación de estas características, y sucede que, a pesar de que se haya podido esclarecer con cierta seguridad quién ha sido el causante de esta, mediante la actual regla de "control efectivo" resulta imposible la atribución de responsabilidad al Estado detectado como autor último debido a las dificultades que se derivan de su aplicación restrictiva en la práctica, esto creará una sensación de vulnerabilidad que se extenderá por la población. Y, ante esta situación, el Gobierno del Estado damnificado no tendrá más remedio que mostrar que, a pesar de la intervención cibernética que se ha sufrido, el Estado se mantiene fuerte. Así, en este contexto, es muy probable que esta muestra de fuerza se exhiba mediante la efectuación de contramedidas y su posterior revelación y difusión pública. Un ejemplo de esto podrían ser las respuestas militares que la República Francesa emprendió en Siria tras los ataques terroristas que sufrió en 2015.

Con lo cual, a la vista de estos hechos expuestos, y contestando a las preguntas formuladas con anterioridad, resulta inevitable plantearse: ¿qué consecuencias puede tener en el comportamiento de los Estados la aceptación y seguimiento de una interpretación restrictiva de la regla de "control efectivo"? La hipótesis que el autor formula en este estudio es que, a medida que los Estados continúen siendo víctimas de ciberoperaciones que no puedan ser atribuidas a un Estado según patrones restrictivos de atribución, y que las normas de soberanía y diligencia debida no permitan a los Estados-víctima llevar a cabo acciones efectivas contra el Estado implicado, proliferarán las contramedidas unilaterales en un ejercicio constitutivo de autotutela y, paralelamente, se elevará la presión social, jurídica y política sobre la norma restrictiva de atribución para que tienda a consolidarse el umbral de "control efectivo" como un marco más amplio de permisión jurídica al acceso, desarrollo y efectuación de contramedidas.

La cuestión será: ¿a quién ─o a qué─ se contraataca? La respuesta variará en función de dos parámetros: por un lado, de quién haya sido realmente el causante; y, por otro lado, del grado en que se haya podido determinar y acreditar el autor de esta ciberoperación internacionalmente ilícita. En este sentido, existen cuatro escenarios posibles:

I. Que no se pueda constatar el autor ni se haya podido seguir el rastro a través del ciberespacio para identificar potenciales cooperadores. Es el peor de los escenarios, no sólo porque pone de manifiesto la situación de vulnerabilidad que tiene el país, sino porque, además, refleja la incapacidad que este tiene de defenderse. Asimismo, supone la asimilación por parte del Estado damnificado del hecho de que no dispone de los recursos suficientes a nivel tecnológico para identificar el culpable. Quizá podría solucionarse buscando ayuda y cooperación en otros países aliados con mayores recursos en este sentido, o en organizaciones internacionales con capacidades tecnológicas superiores.

II. Que se haya podido constatar que el autor de la ciberoperación internacionalmente ilícita sea un Actor No Estatal, pero sin haberse podido determinar potenciales vínculos con otros agentes más allá de este. Es un escenario complejo, puesto que, tal y como se indica en el Manual de Tallinn 2.0, las contramedidas sólo se podrán efectuar contra los Estados; esto es, no se pueden emprender contramedidas contra Actores No Estatales.[111] Esto situaría a este tipo de ciberoperaciones en el plano del ciberterrorismo, del cibercrimen o del hacktivismo, siempre que estas no puedan ser consideradas como constitutivas del uso de la fuerza. De lo contrario, esta violaría la obligación de prohibición del uso de la fuerza y de respetar la soberanía que todo Actor No Estatal debe a los Estados. Y, en estos casos, el Manual de Tallinn 2.0 prevé que los Estados damnificados tengan derecho a adoptar contramedidas contra los Actores No Estatales.[112]

III. Que se haya podido identificar a un Estado directamente. En este caso, el Estado damnificado efectivamente podría desarrollar contramedidas dirigidas al Estado causante tanto por medios cibernéticos como por medios convencionales.[113] Además, no resultaría necesario que las contramedidas que se llevasen a cabo se dirigiesen al órgano específico del Estado que ha violado previamente el Derecho Internacional, sino que podrían orientarse a cualquier órgano de este Estado, puesto que el propio Estado *per se* es el objetivo[114].

IV. Que se haya podido identificar a un Actor No Estatal como perpetrador y que el seguimiento de rastros cibernéticos haya supuesto el hallazgo de vínculos entre este y un tercer

[111] Schmitt, M. N. (ed.), *Tallinn Manual 2.0*, 2017, *op. cit.*, nota 4; Rule 20, cmt. 7.

[112] *Íbid*.

[113] *Íbid*.

[114] *Íbid*, cmt. 6.

Estado, de manera que podría decirse que el Estado ha actuado valiéndose del Actor No Estatal; o, dicho de otro modo, que el Estado ha actuado de manera encubierta a través de éste. Este escenario permitiría al Estado damnificado el desarrollo de las contramedidas previstas e indicadas en el escenario III para el Estado identificado como autor último. Y, además, si estas fueren constitutivas del uso de la fuerza, se le añadiría la posibilidad de emprender medidas contra el Actor No Estatal en cuestión, en los términos indicados en el escenario II.

Así pues, todo caso en el que un Estado, tras sufrir una ciberoperación internacionalmente ilícita, haya podido identificar únicamente a un Actor No Estatal, sin haber podido demostrar mediante la regla de "control efectivo" que un tercer Estado está detrás, se sitúa en el escenario II. Y esto implica que, salvo ante la excepción vista del uso de la fuerza, no se pueden emprender contramedidas contra este Actor No Estatal. La duda que surge entorno a esta cuestión es: ¿qué hubiera sucedido si la regla de "control efectivo" hubiera sido de carácter más extensivo? Muy probablemente, ante un umbral más amplio de "control efectivo", de existir un tercer Estado que opera de manera encubierta a través del Actor No Estatal identificado, hubiera resultado relativamente más sencillo acreditar la vinculación entre ambos y, en consecuencia, atribuirle la responsabilidad al Estado como autor último.

Pero, ¿quién es actualmente el encargado de atribuir la responsabilidad ante este tipo de ciberoperaciones internacionalmente ilícitas que se llevan a cabo? Una respuesta intuitiva podría ser que los distintos tribunales internacionales, en función de la ciberoperación ocurrida y de los Estados involucrados, pueden tener jurisdicción para resolver este tipo de cuestiones; y que, por ende, el Estado damnificado podría, si lo desease, interponer una demanda por estos hechos ante ellos. Un ejemplo de ello podría ser la competencia que tendría el Tribunal de Justicia de la Unión Europea para resolver sobre un caso en el que un Estado miembro, que haya sufrido una ciberoperación, tenga indicios de que el autor último ─esto es, quien operaba de manera encubierta a través de un Actor No Estatal─ fuese otro Estado miembro. O, por otro lado, si se imagina un hipotético caso en el que lo sucedido en el Caso *Nicaragua* hubiese tenido lugar a través del ciberespacio, al operar los *contras* en esta esfera, al entrar en el ámbito de jurisdicción de la CIJ, este tribunal podría haber sido competente para conocer de esta cuestión.

En cualquier caso, el tribunal internacional que corresponda deberá pronunciarse mediante sentencia acerca de las pretensiones formuladas en la demanda por parte del Estado víctima. Pero suceden dos hechos que deben ser tomados en consideración. Por un lado, que el proceso judicial que se iniciaría sería lo suficientemente lento como para que se prolongase

durante meses, o incluso años. Y, por otro lado, que el Estado damnificado debe suponerse será consciente que, si bien existe una vasta literatura jurídica que muestra que existen distintos criterios clásicos sobre el grado de control necesario para atribuir la responsabilidad a un Actor No Estatal según el tribunal en cuestión, la realidad es que en el campo de las ciberoperaciones resulta cada vez más afianzada la aceptación de que es "control efectivo", y no otro, el grado de dependencia que requiere ser acreditado entre un Estado y un Actor No Estatal para poder atribuir la responsabilidad, tal y como se ha indicado en el apartado 4. Con lo cual, la situación se conformaría del siguiente modo: un Estado que ha sido agredido cibernéticamente mediante una operación que difícilmente pueda considerarse como constitutiva del uso de la fuerza, denuncia ante un tribunal internacional competente ─que, muy probablemente, aplique un criterio de atribución que le es desfavorable─ unos hechos que, con mayor o menor precisión, pretenden constatar o acreditar el supuesto vínculo entre un tercer Estado y un Actor No Estatal a través del cual el primero opera, y cuya decisión final se conocerá, debido a la dilación propia del proceso, cuando haya trascurrido el tiempo suficiente como para que las potenciales contramedidas resulten ineficaces. Esta es la realidad existente hoy.

El problema aparece cuando los Estados que se ven en esta situación desde la posición de la víctima realizan objetiva y estratégicamente una ponderación entre esta manera de proceder y otras formas distintas que, aunque puedan resultar más difíciles de enmarcar en las disposiciones normativas del orden internacional existente, puedan considerarse más eficaces en la práctica atendiendo a unos propósitos de defensa ─o de apariencia de defensa─ en concreto. En primer lugar, por una comparativa de costes asociados a cada estrategia. Es una cuestión de recursos. No todos los Estados van a estar dispuestos o van a poder sufragar los costes que supone realizar una inversión de capital económico y tecnológico tal que permita esclarecer mediante pruebas fehacientes y hechos constatados el vínculo existente entre un Actor No Estatal y un Estado, tanto de manera aislada como en el curso de un litigio en un tribunal internacional.

En segundo lugar, es crucial entender que el tiempo es clave. No solamente para favorecer el esclarecimiento de unos hechos llevados a cabo con discreción y sigilo en el ciberespacio, sino porque los Gobiernos necesitan mostrar a su población, a su electorado, que su país es seguro. Haber sufrido una ciberoperación de este tipo y no emprender contramedidas supone la más evidente constatación de la debilidad y vulnerabilidad del Estado en cuestión.

En tercer lugar, hay que tener en cuenta que el hecho de que el Estado damnificado sea, además, quien deba iniciar las diligencias propias para acreditar el potencial vínculo para posibilitar la atribución de responsabilidad al Estado que ha actuado de manera encubierta a través del Actor No Estatal le deja doblemente en desventaja y, lejos de resolver esta situación, el hecho de que la víctima sea quien adicionalmente tenga la carga de la prueba ahonda su vulnerabilidad, obligándole a llevar a cabo toda demostración necesaria para constatar el hecho que denuncia ─aunque este sea cierto, y aunque resulte excesivamente complicado probarlo─.

Y, en cuarto lugar, si a todas estas circunstancias se le suma la toma de conciencia por parte del Estado-víctima de que a través de la regla de "control efectivo" difícilmente se va a poder atribuir la responsabilidad al Estado detectado como autor último y que ha actuado valiéndose del Actor No Estatal en cuestión, teniendo especialmente en cuenta las dificultades asociadas a la identificación de conductas mediante rastros a través del ciberespacio, la situación deviene insostenible y propicia, por sí misma, la búsqueda de nuevos métodos de autoamparo alternativos.

Un ejemplo de ello sería la actitud que la República Francesa ha materializado en su declaración *Droit international appliqué aux opérations dans le cyberespace* (2019), donde, como se ha indicado en el apartado 3.1.1, expresa que "la atribución de un ciberataque de origen estatal es una decisión política nacional"[115]. Pero esto supone, desde el punto de vista doctrinal, un notorio y evidente fracaso del Derecho Internacional; sobre todo, si esta atribución de carácter político no es una mera calificación, sino la antesala de la efectuación de contramedidas, puesto que si este proporcionara un marco más amplio de acceso a ellas ─que es en sentido último la auténtica necesidad que hay detrás de esta formulación─ a través de una interpretación más extensiva de lo que debe entenderse como "control efectivo", no sería necesario que los Estados recurriesen a tales enunciaciones.

Además, el hecho de que la regla de atribución prevista sea tan restrictiva socava más aún la situación de debilidad y vulnerabilidad que experimentan los países con pocos recursos, puesto que únicamente aquellos Estados con (a) grandes capacidades militares, (b) grandes capacidades económicas y (c) grandes capacidades tecnológicas pueden permitirse incorporar la cuestión atributiva como decisión nacional de una manera efectiva y real, porque verdaderamente tienen a sus espaldas un gran poder en el que fundamentar, defender y con el que hacer cumplir sus decisiones nacionales en la esfera internacional. Por eso se afirma el

[115] Ministère des Armées; RÉPUBLIQUE FRANÇAISE, 2019, *op. cit.*, nota 63, p.10.

fracaso de la tutela por parte del Derecho Internacional a Estados que han sido víctimas de este tipo de ciberoperaciones. E, inversamente, siguiendo el ejemplo expuesto, si Francia, que es un país con una gran fuerza militar, con una economía sólida y con un elevado nivel de desarrollo tecnológico, ha tenido la necesidad de decretar que la atribución de responsabilidad será una decisión política nacional, con más motivo aún debe tomarse en consideración la situación de desventaja y desprotección que brinda la actual regla de "control efectivo" a los Estados con menos capacidades en los ámbitos indicados; porque, si bien es cierto que la imposibilidad de atribuir la responsabilidad no implica que el supuesto Estado autor sea declarado inocente ─porque puede ser declarado, por ejemplo, responsable de una violación del principio de soberanía, del principio de diligencia debida o del deber de no intervención en los asuntos internos de otro Estado, entre otros─, la realidad es que las contramedidas que se puedan efectuar en cada caso serán radicalmente distintas.

Y, finalmente, desde un punto de vista ético resulta insostenible el empleo de una regla que dificulta enormemente ─e incluso en muchos casos hace imposible─ la atribución de responsabilidad al legítimo autor de la ciberoperación internacionalmente ilícita que se ha llevado a cabo. Y cuando una regla como esta llega a obstaculizar desmesuradamente la atribución de responsabilidad ante un vínculo que, a pesar de que sea extremadamente difícil de probar por las característica propias del ciberespacio, existe realmente, debe ponerse especial énfasis en su modificación por tal de asegurar la debida y específica adecuación de una prueba de esta índole al campo de las ciberoperaciones, con el único objetivo de permitir facilitar que se constate lo que realmente existe. Sólo así podrán los Estados seguir observando el Derecho Internacional en la cuestión atributiva para este tipo de ciberoperaciones en concreto, y sin necesidad de que los Estados se autoatribuyan capacidades para actuar ante estas situaciones.

Es esencial e imprescindible que exista una alineación de intereses entre las intenciones de la Comunidad Internacional ─materializadas en la normativa internacional aplicable y en las decisiones de instituciones o tribuales internacionales en este ámbito─ y las necesidades de los Estados para que se cree una sinergia que posibilite el adecuado esclarecimiento de la verdad. Y para ello es necesario que se amplíe el umbral de "control efectivo" actualmente previsto para atribuir la responsabilidad a un Estado ante la ciberoperación que ha efectuado de manera encubierta a otro Estado a través de un Actor No Estatal.

6. DETECCIÓN DE LOS PRINCIPALES PROBLEMAS Y PROPOSICIÓN DE LÍNEAS GENERALES DE RESOLUCIÓN.

En el apartado anterior se han determinado una serie de aspectos característicos del actual sistema de atribución que ponen de manifiesto la necesidad de avanzar hacia una interpretación extensiva de la regla de "control efectivo" para poder seguir siendo exitosos en el campo de aquellas ciberoperaciones que, por su carácter o efectos, son consideradas como leves ─esto es, no son constitutivas del uso de la fuerza ni pueden ser consideradas ataques armados─. Por tal de diseñar propuestas razonables y efectivas, conviene primero sintetizar los principales problemas identificados:

1. La existencia y aplicación actualmente de una regla de "control efectivo" demasiado restrictiva, cuyas consecuencias ante ciberoperaciones leves son, por un lado, la difícil atribución de responsabilidad a un Estado y, por otro lado, el acceso limitado a contramedidas que permite al Estado damnificado.

2. Las ciberoperaciones "de poca escala" están poco reguladas; pero cada vez son más frecuentes. Por otro lado, aunque se trate de intrusiones de pequeña escala, su reiteración multiplica el efecto negativo de las mismas.

3. Existe una dificultad generalizada por identificar al autor al haber operado a través del ciberespacio. Pero esta dificultad se agrava si, además, el Estado que tiene que identificar al autor dispone de unos recursos tecnológicos limitados.

4. Actualmente, es el Estado-víctima quien tiene la carga de la prueba en el proceso de atribución de la responsabilidad a un tercer Estado, y quien debe asumir los costes derivados de este proceso ─que, paradójicamente, al tratarse de ciberoperaciones leves, la demostración en sí puede llegar a ser tanto o más costosa que el daño causado─.

5. El proceso de denuncia ante un tribunal internacional competente y la posterior obtención de una sentencia que atribuya la responsabilidad es lento y, además, se afianza la aplicación de una prueba de control que resulta ser desfavorable a aquellos Estados que se ven obligados a buscar amparo ante estas instituciones como único recurso.

6. La proliferación de declaraciones nacionales en las que se asume la cuestión atributiva como una decisión nacional supone *de facto* un fracaso del Derecho Internacional, por no haber sido capaz de alinear las intenciones de la Comunidad Internacional con las necesidades que los Estados tienen ante este tipo de ciberoperaciones.

La determinación de la responsabilidad no podrá ser tratada adecuadamente sin un sistema de atribución que tenga en cuenta y solvente debidamente los problemas que han sido identificados a lo largo de esta investigación y que se han indicado anteriormente. Para que se atribuya de manera correcta y con éxito la responsabilidad ante ciberoperaciones de carácter leve debe impulsarse un cambio de paradigma atributivo. Este debe estar fundamentado en una regla de atribución propia y específica para las ciberoperaciones, basada en una interpretación más extensiva de lo que se entiende como "control efectivo" actualmente.

En este sentido, se establecen a continuación una serie de propuestas, en forma de líneas generales de resolución, diseñadas teniendo especialmente en cuenta esta necesidad de actualizar el sistema de atribución de la responsabilidad existente para este tipo de ciberoperaciones ─pero que, sin duda, puede servir para mejorar la atribución de todas ellas─ para hacerlo más efectivo y más justo.

En primer lugar, el hecho de que la regla de "control efectivo" resulte restrictiva en la práctica y ciertamente ineficaz ante este tipo de ciberoperaciones conduce a la necesidad de modificar la actual regla de atribución y ampliar indudablemente el umbral de "control efectivo". Para ello sería imprescindible establecer una serie de parámetros técnicos a observar y analizar, y mediante los cuales un grupo de especialistas pudiesen determinar con un grado de significación en concreto el vínculo entre un determinado Estado y un determinado Actor No Estatal. Y para diseñar el protocolo de rastreo y determinación del vínculo a través del ciberespacio sería decisivo contar con el soporte de ingenieros, técnicos y especialistas en informática y en telecomunicaciones, puesto que son ellos, y no los juristas, los que conocen con mayor precisión y exactitud el modo de llevar a cabo una indagación exhaustiva en estos términos en el ciberespacio.

De hecho, actualmente ya existen órganos como, por ejemplo, el *National Cyber Security Centre* del Reino Unido que disponen de recursos tecnológicos lo suficientemente avanzados como para realizar, a través de una exploración cibernética, siguiendo unas directrices y parámetros específicos, un análisis ciertamente fidedigno acerca del vínculo entre dos actores de la esfera internacional en el marco de una ciberoperación perpetrada.

Quizá haya que aceptar que mediante la conocida regla de "control efectivo" no se va a poder determinar nunca, con total seguridad, la existencia del vínculo que actualmente se requiere para la atribución de responsabilidad. Y, más aún, cuando el esfuerzo de los perpetradores reside cada vez más en el modo de ocultación, en el sigilo y en el anonimato con

el que se lleva a cabo la ciberoperación, y no tanto en otros aspectos tales como la potencia en sí de la intervención. En este sentido, la ampliación del umbral de "control efectivo" podría materializarse mediante la aceptación de que este "control efectivo" se logra acreditar si un análisis del vínculo entre actores ─como el mencionado anteriormente─ consigue probar con un nivel de confianza estipulado previamente ─y que debe ser lo suficientemente elevado para que el margen de error sea poco significativo─ su existencia. O, dicho de otro modo, que se entienda que existe "control efectivo" por parte de un Estado sobre un Actor No Estatal cuando el resultado de una investigación en estos términos concluya que existe un vínculo de este tipo entre ambos actores, a un nivel de confianza general y comúnmente aceptado ─como podría ser el 75%─. En cualquier caso, este índice podría pactarse atendiendo a la opinión de expertos en tecnología sobre el porcentaje de fiabilidad a partir del cual resultara intuitivo, adecuado y prudente atribuir la responsabilidad ante este tipo de ciberoperaciones.

En segundo lugar, sería necesaria la existencia de más regulación internacional sobre ciberoperaciones de pequeña escala. Generalmente se suele poner mayor énfasis en la regulación de los problemas con peores consecuencias ─y es comprensivo y razonable que así sea─, pero no por ello debe descuidarse el debido tratamiento de otras cuestiones, como las ciberoperaciones leves, cuyos efectos quizá no lleguen a ser tan devastadores como los que puede tener un ciberataque, pero que, sin embargo, están deviniendo cada vez más frecuentes. Y no sólo esto, sino que, además, la reincidencia en ciberoperaciones leves puede llegar a tener, en suma, consecuencias tanto o más perjudiciales y dañinas para un Estado que un ciberataque aislado. Por ello, debería penalizarse la reincidencia y multirreincidencia, con independencia de que esta se produzca sobre un mismo Estado o no.

Además, debería establecerse un sistema de sanciones a nivel internacional para aquellos Estados que sucesivamente aparecen en indicios de estar implicados en ciberoperaciones llevadas a cabo sobre terceros Estados, incluso aunque estas no hayan podido acreditarse. El planteamiento sería el siguiente: ¿por qué en distintos análisis acerca del origen de diferentes ciberoperaciones efectuadas por Actores No Estatales han aparecido indicios de que el Estado X está detrás ─incluso aunque el resultado final del informe técnico paramétrico no haya sido concluyente debido a un nivel asociado de confianza inferior al establecido─? Se estará de acuerdo en que, cuanto menos, resulta una anomalía que debe inspeccionarse. Y ciertamente supondría una excepción a la presunción de inocencia, pero lo cierto es que los Estados reincidentes usan esta presunción como escudo ante la perpetración ilícita de

ciberoperaciones de carácter leve, puesto que es, además, esta presunción lo que fundamenta que la carga de la prueba la ostente el Estado víctima. Y es comprensible que la presunción de inocencia exista, pero debe aplicarse de un modo inteligente y estratégico, evitando que pueda distorsionarse por ser utilizada fraudulentamente por todo tipo de sujetos de Derecho Internacional con comportamientos ilícitos. Además, esta medida de sancionar a nivel internacional a aquellos Estados que aparezcan repetidamente en distintas indagaciones como potenciales implicados en ciberoperaciones ilícitas cometidas por Actores No Estatales debería provocar un efecto disuasorio que forzase a los Estados a tomar medidas de precaución y de valoración previa acerca de las entidades con las que se tiene o se entabla relación, prestando especial atención a su actividad, al modo de desarrollarla, así como a sus objetivos y metas.

En tercer lugar, sería conveniente la creación de una Agencia Internacional de Ciberseguridad dependiente de Naciones Unidas con medios económicos y tecnológicos suficientes para examinar debidamente, a petición de todo Estado que lo requiera, el origen de una ciberoperación sufrida en el territorio de su Estado, con el objetivo de recibir un informe de esta que sirviese como prueba fidedigna y concluyente para acreditar, ante el tribunal internacional que corresponda, el vínculo entre un Estado y un Actor No Estatal, en caso de que este exista. El funcionamiento, a nivel operativo, podría ser similar al de los centros nacionales de Ciberseguridad ─tales como el del Reino Unido, anteriormente mencionado─, pero con la principal diferencia de servir a la Comunidad Internacional en su conjunto. De este modo también se superarían los problemas derivados del coste asociado a la investigación de la identidad real del autor que actualmente padecen los Estados en vías de desarrollo o con menos capacidades tecnológicas, puesto que la única condición necesaria para que un Estado pudiese recurrir a esta agencia debería ser haber sufrido la perpetración de una ciberoperación.

Para determinar un potencial vínculo entre actores en el ciberespacio, esta Agencia debería seguir la interpretación extensiva de ese umbral que supone la constatación de un "control efectivo" a través de una acreditación por medio del proceso indiciario y paramétrico de indagación cibernética descrito en la primera propuesta, y siempre que se haya alcanzado el nivel de confianza requerido a tales efectos. De este modo, la atribución de responsabilidad seguiría estando en manos de los distintos tribunales competentes en cada caso, y determinándose por medio de una sentencia motivada. Pero, en este sentido, esta Agencia, de carácter imparcial y de acceso universal, como se ha indicado, podría actuar como órgano emisor de un informe o dictamen que pudiera aportarse como prueba fehaciente, acerca de la

existencia ─o no─ del vínculo de "control efectivo" que puede haber ejercido un Estado sobre un Actor No Estatal, ante los respectivos tribunales que estén conociendo del caso en concreto sobre la ciberoperación internacionalmente ilícita de que se trate. Pero, para ello, resultaría imprescindible que se diesen dos circunstancias. Por un lado, que a esta Agencia Internacional de Ciberseguridad se le proveyera de los medios y recursos necesarios para realizar su trabajo de la forma más rápida posible, pero asegurando siempre la más alta calidad tanto en el proceso como en el resultado final de la investigación. Y, por otro lado, que se reconociese el prestigio de esta Agencia a nivel internacional, de modo que los tribunales internacionales que conozcan de este tipo de casos realmente tomen en consideración lo dispuesto en el informe de diagnóstico emitido, aportado por la parte que corresponda en el proceso.

Se deberían crear unos protocolos de actuación por tal de optimizar tareas, recursos y tiempo y ganar en efectividad, eficacia y eficiencia. De este modo, el éxito atributivo estaría basado en la celeridad y en la calidad del análisis del potencial vínculo por parte de esta Agencia, así como por la consideración y aceptación, por parte de los tribunales, del informe emitido como prueba fehaciente.

Esta agencia podría desarrollar adicionalmente tareas de soporte a los Estados en cuestiones de implantación de sistemas de ciberseguridad. E incluso podrían establecerse tareas de cibervigilancia, de modo que constituyera, a su vez, una especie de cuerpo internacional de ciberpolicía analítica, cuyas funciones y cuyo alcance deberían concretarse. Esta especie de vigilancia de oficio podría incluso tener iniciativa procesal ante los tribunales internacionales, hecho que permitiría relajar y suavizar la carga de la prueba que actualmente tienen los países que han sufrido la perpetración de una ciberoperación en su territorio.

En suma, si se tendiera hacia un sistema de atribución de la responsabilidad ante ciberoperaciones conformado del modo indicado en estas líneas generales propuestas, se ganaría en eficacia atributiva y permitiría la alineación de intereses entre (1) las intenciones del conjunto de la Comunidad Internacional y Naciones Unidas, y (2) las necesidades que los Estados tienen cuando sufren este tipo de actos, cuando existe una amenaza de sufrirlos, o cuando se sienten desprotegidos por una normativa que les es desfavorable. Y esto implicaría la recuperación de la confianza en el Derecho Internacional, basada en la propagación del reconocimiento de la práctica efectiva de la tutela que este debe a los Estados cuando estos están en una situación de vulnerabilidad provocada ilícitamente por un tercer Estado.

CONCLUSIONES.

El análisis llevado a cabo en el Capítulo I refleja la necesidad de comenzar la investigación realizando unas precisiones terminológicas ciertamente importantes para poder asentar las bases conceptuales de lo que se desarrollaría posteriormente. El ámbito cibernético se revela como un dominio operativo más en el que intervienen todo tipo de actores, con objetivos muy diversos. Las principales amenazas hoy en día son la ciberguerra, el ciberterrorismo, el ciberespionaje y el cibercrimen. Además, conviene destacar que las actuaciones que se llevan a cabo en el ciberespacio, o a través de él, son cada vez más frecuentes. De ahí la necesidad de establecer una regulación al respecto y salvar la situación de ciberinseguridad que puede derivarse de ello.

Por otro lado, cabe destacar que sigue existiendo hoy en día un cierto debate doctrinal en cuanto a la naturaleza del ciberespacio. Sin embargo, la posición de Naciones Unidas, manifestada a través de su "Tercer Grupo de Expertos Gubernamentales" (GEG), es que, a pesar de esta falta de consenso en cuanto a su naturaleza, en el ciberespacio se aplica el principio de soberanía estatal, puesto que depende de una infraestructura física sujeta a control soberano.

En cuanto al uso de la fuerza, es comúnmente aceptado que si las ciberoperaciones tienen efectos análogos a los que se derivarían del empleo de armas convencionales, como daños físicos o funcionales, estas quedarían comprendidas en la prohibición expresada en el artículo 2.4 de la Carta de Naciones Unidas (1945). Pero, por otro lado, sigue sin haber acuerdo por parte de la Comunidad Internacional acerca de cómo, cuándo y por qué las ciberoperaciones que no causan muertes, lesiones ni destrucción deben equivaler al "uso de la fuerza", puesto que resulta manifiestamente más complicado establecer una analogía con las operaciones convencionales. Por otro lado, en relación con la actualización del concepto de ataque armado, debe entenderse que el ciberespacio, además de un campo de batalla, puede constituir *per se* "el arma" requerida para que una ciberoperación sea considerada un "ataque armado" dependiendo de la intención con la que se use. La caracterización debe hacerse teniendo en cuenta la "escala y efectos" de la ciberoperación. Asimismo, se acepta el derecho de legítima defensa ante estos casos, pero se descarta el derecho a una legítima defensa preventiva.

En el Capítulo II se ha realizado un estudio del régimen de atribución de la responsabilidad ante ciberoperaciones llevadas a cabo por Estados a través de Actores No Estatales, con dos focos principales: la normativa aplicable en materia de atribución y el grado

de control necesario para poder atribuir la responsabilidad a un Estado. Respecto del primero, se constata que los artículos del texto de la Comisión de Derecho Internacional de Naciones Unidas ─*Responsibility of States for Internationally Wrongful Acts* (2001)─ sin duda se aplican al ámbito del ciberespacio. Así lo confirma el *Manual de Tallinn 2.0* (2017) en su capítulo 4.

En relación con el Manual de Tallinn 2.0, el estudio se ha centrado en la Regla 17. En concreto, se han identificado las aportaciones que esta regla hace, como *lex specialis*, al artículo 8 de los artículos de 2001 de la Comisión de Derecho Internacional, mencionada anteriormente, y se han analizado las diferentes situaciones que contiene su Regla 17 que, con carácter *numerus clausus*, conllevan la atribución de responsabilidad a un Estado por ciberoperaciones realizadas aparentemente por Actores No Estatales. También se proporciona un listado no exhaustivo de circunstancias que no generan por sí solas responsabilidad a un Estado, a entender del Grupo Internacional de Expertos.

Además, se ha examinado el estado de la cuestión atributiva en las recientes declaraciones realizadas por Francia y Países Bajos. De ellas se puede destacar la asunción por parte de Francia de la atribución como una "decisión política nacional"; así como la indiscutible incorporación de preceptos del Derecho Internacional existente ─incluidos los de algunos textos de *soft law*─ en la normativa interna que se desprende de la declaración de Países Bajos.

Y, respecto del grado de control, se debe concluir, tal y como se establece en la Regla 17, comentario 5 y 6, del Manual de Tallinn 2.0, que deberá acreditarse un "control efectivo" para poder atribuir la responsabilidad a un Estado ante ciberoperaciones llevadas a cabo por Actores No Estatales. En este sentido, se ha examinado el origen de este concepto, que se halla en la sentencia de la CIJ en el Caso *Nicaragua*, y se ha realizado un análisis acerca de la adecuación de la aplicabilidad de este concepto en el ciberespacio. La principal conclusión es que esta regla de "control efectivo" no fue concebida para la atribución en el ciberespacio, y esto genera una serie de problemas, de entre los cuales conviene destacar, en primer lugar, la difícil determinación del vínculo debido al anonimato que opera en el ciberespacio; y, en segundo lugar, el acceso limitado a contramedidas de que dispone el Estado damnificado al no poder atribuir la responsabilidad.

El Capítulo III parte de este análisis mencionado e introduce en forma de ensayo la necesidad de avanzar hacia la ampliación del umbral de "control efectivo". Las principales razones son: (1) que actualmente la regla de "control efectivo" es demasiado restrictiva, y que

esto comporta principalmente los dos problemas mencionados; (2) que las ciberoperaciones leves están poco reguladas y, sin embargo, son cada vez más frecuentes; (3) que existen serias dificultades, debido a la naturaleza del ciberespacio, para acreditar el vínculo en el grado que requiere el "control efectivo"; (4) que actualmente es el Estado-víctima quien tiene la carga de la prueba; (5) que el proceso de denuncia ante los tribunales internacionales es lento ─siendo el tiempo un factor clave─ y que sin embargo es el único recurso al que pueden acogerse determinados Estados; y (6) que la asunción de la atribución por parte de los Estados como una decisión nacional, y no como una mera calificación, supone un fracaso del Derecho Internacional, especialmente si a esta le sucede la adopción de contramedidas unilaterales.

Y, para solventar esta situación, se han sugerido unas propuestas que pretenden reformar el sistema atributivo con la intención de hacerlo más ágil y eficaz, así como para devolver a los Estados una confianza suficiente en el Derecho Internacional sustentada en la búsqueda de la alineación de las intenciones de la Comunidad Internacional con las necesidades que los Estados tienen ante este tipo de ciberoperaciones. Estas propuestas también procuran implantar un mayor nivel de justicia en el proceso atributivo. No es razonable ni coherente que a un Estado que proporciona instrumentos cibernéticos a un Actor No Estatal, que le identifica los objetivos y que hasta selecciona la fecha en la que la ciberoperación debe llevarse a cabo, aún hoy, no se le pueda atribuir la responsabilidad, debido a que, para ello, se requiere la determinación y acreditación del vínculo de control por medio de un umbral tan restrictivo que lo convierte en prácticamente indemostrable. Algunos autores declaran que esta situación descrita podría corresponderse con la ciberintervención de *hacktivistas* rusos en Estonia en 2007.[116]

Por todo ello, puede concluirse que, aunque es obvio que existen países con una clara superioridad militar, económica o tecnológica, si el resto de la Comunidad Internacional presenta una respuesta valiente y conjunta a sus actuaciones ilícitas, estos países deberán reconsiderar sus planteamientos. La acción conjunta es la única respuesta posible.

Mientras no exista unidad internacional para hacer frente a los Estados que abusan de su posición de fuerza o superioridad ─ya sea militar, económica o tecnológica─ realizando ciberoperaciones con un sentimiento de inmunidad e impunidad flagrante, todos los esfuerzos de investigación, información y regulación al respecto serán estériles.

[116] Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*, CCDCOE. The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

REFERENCIAS BIBLIOGRÁFICAS.

Abass, A. (2008). *Proving State Responsibility for Genocide: The ICJ in Bosnia v . Serbia and the International Commission of Inquiry for Darfur*. Fordham International Law Journal, 31(4), 871-910

Boletín Oficial del Estado (2010). *Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001*. 78847-78896.

Cassese, A. (2007). *The Nicaragua and Tadić Tests revisited in light of the ICJ judgment on genocide in Bosnia*. European Journal of International Law, 18(4), 649-668. https://doi.org/10.1093/ejil/chm034

Clarke, R. A., & Knake, R. K. (2010). C*yber War: the Next Threat To National Security and What To Do About It.* 2(6), 1-140. https://doi.org/10.22456/2178-8839.20585

Crawford, J. (2002). *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*. Cambridge University Press. https://doi.org/10.2307/3100134

Crawford, J. (2013). *State Responsibility: The General Part*. Cambridge University Press, Annexed to GA Resolution 56/83 of 2001, the International Law Commission's Articles on the Responsibility for Internationally Wrongful Acts. https://doi.org/https://doi.org/10.1017/CBO9781139033060

Dixon, M. (2007). *Textbook on International Law*. Oxford University Press.

Finnemore, M., & Hollis, D. B. (2016). *Constructing Norms for Global Cybersecurity*. American Journal of International Law, 110(3), 425-479. https://doi.org/10.1017/s0002930000016894

Fonseca, C. E. (2014). *El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra*. Revista de la ESG, 11. http://www.cefadigital.edu.ar/bitstream/123456789/993/1/Revista ESG no.588-2014_Fonseca_172.pdf

García Segura, C. (2020). *La construcción de normas globales, entre el avance del cosmopolitismo blando y el retorno de la geopolítica. La regulación global de la ciberseguridad*.

International Court of Justice (1986). *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America), merits. The International Court of Justice, The American Journal of International Law, 81(1). https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

International Law Commission (2001). *Draft articles on Responsibility of States for Internationally Wrongful Acts*, with commentaries, Fifty-third A/56/10 (2001). https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

International Law Commission (2001). *Responsibility of States for Internationally Wrongful Acts*. General Assembly, vol. II (Part Two). Annex to General Assembly resolution 56/83 of 12 December 2001.

Jensen, E. T. (2017). *The Tallinn Manual 2.0: Highlights and Inisghts*. Georgetown Journal of International Law, 43(3), 735-778. https://www.law.georgetown.edu/international-law-journal/in-print/volume-48-number-3-spring-2017/the-tallinn-manual-2-0-highlights-and-insights

Lewis, J., con el soporte de K. V. (2016). *Report of the International Security Cyber Issues Workshop Series*. UN Institute for Disarmament Research (UNIDIR); CSIS (Center for Strategic and International Studies) - Workshop Series. https://www.unidir.org/publication/report-international-security-cyber-issues-workshop-series

Melzer, N. (2011). *Cyberwarfare and International Law*. Cyberwarfare and International Law - UNIDIR Resources, 38.

Ministère des Armées; RÉPUBLIQUE FRANÇAISE. (2019). *Droit international appliqué aux opérations dans le cyberespace*.
https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf

Ministry of Foreign Affairs of the Kingdom of the Netherlands (2019a). *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace.*
https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

Ministry of Foreign Affairs of the Kingdom of the Netherlands (2019b). *Appendix: International law in cyberspace.* https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

Moussu, N., Llouquet, A.-L., & Chaumei, G. (2011). *Cyberespace, 5ème champ de bataille*. Armées d'aujourd'hui, 365/201.
https://www.irsem.fr/data/files/irsem/documents/document/file/790/ADA365.pdf

Office of the Chairman of the Joint Chiefs of Staff (2019). *DOD Dictionary of Military and Associated Terms*. Joint Education and Doctrine Division, J-7, April, 382. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*, CCDCOE. The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

REAL ACADEMIA ESPAÑOLA: Diccionario de la lengua española, 23.ª ed., [versión 23.3 en línea].

Schmitt, M. N. (2012). *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*. Harvard International Law Journal, 54 (December 2012), 13-36

Schmitt, M. N. (ed.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. https://doi.org/10.1017/9781316822524

Segura Serrano, A. (2017). *Ciberseguridad y Derecho internacional*. Revista Española de Derecho Internacional, 69(2), 291-299. https://doi.org/10.17103/redi.69.2.2017.2.02

Talmon, S. (2009). *The responsibility of outside powers for acts of secessionist entities*. International and Comparative Law Quarterly, 58(3), 493-517. https://doi.org/10.1017/S0020589309001171

The White House (2008). *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* (NSPD-54/HSPD23). Encyclopedia of Security and Emergency Management, 1, 1-9. https://doi.org/10.1007/978-3-319-69891-5_20-1

The White House (2009). Cyberspace Policy Review. *Assuring a Trusted and Resilient Information and Communications Infrastructure*. Security, 3, 1-37. https://fas.org/irp/eprint/cyber-review.pdf