Ciberdiligencia debida: ¿una actualización necesaria para el Derecho Internacional del ciberespacio?

Andrea Cocchini | Profesor ayudante doctor de Derecho Internacional Público y Derecho de la Unión Europea, Universidad de Navarra

Tema[1]

El problema de la atribución de la responsabilidad internacional a ciberatacantes respaldados por Estados sigue sin una solución eficaz. Se sugiere que el estándar de la "ciberdiligencia debida" podría ser una posible respuesta.

Resumen

Si ya es difícil atribuir técnicamente un ciberataque a un grupo de ciberatacantes que opere en el territorio de otro Estado, no es más fácil atribuírselo jurídicamente debido a la regulación internacional aplicable al ciberespacio. Por ello, este ARI estudia las dificultades que existen para atribuir un ciberataque según los instrumentos del Derecho Internacional disponibles en la actualidad. Sugiere, entonces, recurrir al estándar de la "ciberdiligencia debida", que conllevaría para todo Estado la obligación de prevenir, mediante actividades de monitoreo, posibles ciberamenazas provenientes de grupos privados radicados en el territorio de un Estado.

Análisis

En una sociedad internacional cada vez más sometida a la economía digital no sorprende que aumenten los problemas de ciberseguridad[2]. Los ciberataques tienen objetivos muy dispares y provienen de entidades heterogéneas, ya sean actores estatales o internos[3]. Entre ellos, los que perpetran los actores-Estado y los grupos de actores no estatales respaldados por Estados representan una de las principales ciberamenazas en la comunidad internacional. Estos utilizan el ciberespacio para realizar, junto con actividades ya clásicas de ciberguerra, ciberespionaje y sabotaje, también operaciones de influencia en la opinión pública entre los nacionales de otros Estados mediante la desinformación[4]. Pese a que la casuística en estos ámbitos ya sea

[1] Este ARI se basa en el artículo publicado por el autor en la revista *UNISCI*, n.º 55, enero de 2021, pp. 69-98.

[2] El Ministerio del Interior de Australia calcula que los ciberincidentes contra las pequeñas, medianas y grandes empresas privadas podrían costar a la economía australiana hasta 29.000 millones de dólares anuales, equivalentes al 1,9% de su PIB. "Australia's Cyber Security Strategy 2020", pp. 7 y 10.

[3] El CCN-CERT identifica los ámbitos principales en los que han operado durante 2020 en España en su "Informe de Ciberamenazas y Tendencias 2020", pp. 10-14.

[4] Para más ejemplos, ver Russell Buchan (2012), "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions", *Journal of Conflict & Security Law*, vol. 17, pp. 211-227; Samantha Bradshaw y Philip N. Howard (2019), "The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation", Working Paper, Project on Computational Propaganda, Universidad de Oxford.

muy amplia[5], el Derecho Internacional aún no cuenta con una regulación internacional obligatoria que permita resolver las dificultades jurídicas que nacen de estos tipos de ciberamenazas.

Es cierto que, en el ámbito ciberespacial, se aplican la Carta de la ONU y los demás principios derivados de la soberanía estatal[6]. No obstante, debido a las características específicas del ciberespacio, las normas consuetudinarias sobre la responsabilidad internacional del Estado no siempre resultan adecuadas para regularlo de forma satisfactoria. Y, aunque parece estar formándose un deseo común por parte de algunos Estados de ajustar la reglamentación internacional[7], la realidad internacional actual necesita soluciones jurídicas eficaces en lugar de criterios un tanto obsoletos. Así parece pedirlo, por ejemplo, la última Estrategia Nacional de Ciberseguridad (ENCS) de 2019, cuya sexta línea de acción propone fomentar el multilateralismo a nivel internacional y regional para reforzar la aplicación del Derecho internacional al ciberespacio[8].

En consecuencia, el material al que podemos acudir sigue siendo el *Manual de Tallin sobre Derecho Internacional aplicable a la ciberguerra* (2013) y, sobre todo, el *Manual de Tallin 2.0 sobre Derecho Internacional aplicable a las operaciones cibernéticas* (2017). Éstos, pese a no ser instrumentos jurídicos obligatorios, cuentan con la autoridad de los especialistas que los elaboraron, recogen algunas disposiciones que ya se consideran costumbres internacionales del ciberespacio y se adoptaron en el seno de la OTAN, organización neurálgica para facilitar la cooperación internacional en ciberseguridad junto con otras organizaciones multilaterales que se enumeran en la mencionada Estrategia Nacional de Ciberseguridad.

El problema de la atribución de los ciberataques

Según el CCN-CERT, la atribución y la responsabilidad son “dos de los aspectos más importantes cuando se trata de derrotar a los ciberatacantes”, porque sin riesgos y sin responsabilidad seguirán actuando[9].

En Derecho Internacional, el concepto de *atribución* no sirve para la identificación técnica de los ordenadores desde los cuales se lanzó un ciberataque y de las personas que lo ejecutaron materialmente. Indica, en cambio, la operación jurídica necesaria para

[5] Nicholas Tsagourias (2012), “Cyber-attacks, Self-defence and the Problem of Attribution”, *Journal of Conflict & Security Law*, vol. 17, pp. 229-244.

[6] Nicholas Tsagourias (2015), “The legal status of cyberspace”, en Nicholas Tsagourias y Rusell Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Edward Elgar Pub., pp. 13-29; cit. en p. 13.

[7] Para otros Estados que han manifestado su deseo de extender el principio precautorio también al ciberespacio véase, por ejemplo, Jutta Brunnée y Tamar Meshel (2015), “Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance”, *German Yearbook of International Law*, vol. 58, pp. 136-137.

[8] La ECSN “[a]bogará por la creación de un marco internacional para la prevención de los conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de la Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento no responsable de los Estados” (p. 39, con alusiones similares en pp. 20, 26, 30, 54 y 55).

[9] CCN-CERT (2019), “Informe de Ciberamenazas y Tendencias 2019”, p. 125.

entender si una cierta conducta de uno o más individuos es reconducible a un Estado específico. Es cierto que la demostración de la atribución técnica antecede a la verificación de la atribución jurídica como precondición para la imputabilidad de un ciberataque a un Estado concreto[10]. No obstante, aunque se consiguiera atribuir técnicamente un ciberataque a un grupo no estatal bajo la jurisdicción de otro Estado, aún más complicado podría ser atribuírselo jurídicamente debido a la insuficiente y un tanto envejecida normativa internacional de la que disponemos[11]. En efecto, ni siquiera el *Manual de Tallin 2.0* aclara el problema de la atribución y la responsabilidad, indicándonos algunos criterios para saber en qué circunstancias sería posible atribuir a los Estados la responsabilidad internacional por ciberataques de actores no estatales asentados en su territorio o bajo su jurisdicción. Por tanto, lo que este trabajo sugiere es la adopción de un nuevo estándar, llamado "ciberdiligencia debida" a partir de la extensión del criterio tradicional de "diligencia debida", que facilite saber cómo y cuándo atribuir la responsabilidad internacional a los Estados por los ciberataques mencionados.

La extensión de la diligencia debida al ciberespacio: la "ciberdiligencia debida"

Para intentar resolver este problema, viene en ayuda el estándar de la diligencia debida (*due diligence*)[12], que entraña para los Estados el deber de garantizar que, dentro de su territorio o jurisdicción, no se vulneren los intereses y los derechos de los demás Estados. En caso contrario, se les podrá atribuir la responsabilidad por no adoptar las medidas necesarias para evitar un hecho ilícito internacional[13]. En el presente estudio, se afirma que este estándar sería extensible por analogía a las operaciones cibernéticas bajo la forma de un nuevo criterio de "ciberdiligencia debida"[14]. Este concepto presenta dos ventajas importantes respecto a la regla tradicional de la atribución. En primer lugar, soslayaría el problema de la atribución técnica de un ciberataque, porque impondría a los Estados vigilar *a priori* las actividades informáticas potencialmente dañinas desarrolladas en su interior. En segundo lugar, la ciberdiligencia debida facilitaría la atribución jurídica, porque atribuiría la responsabilidad internacional al Estado que no adopte las medidas preventivas útiles para evitar un ciberataque que cause "daños significativos" a otro[15]. Todo ello sin necesidad de averiguar el "control efectivo"[16] del

[10] Zhxiong Huang (2014), "The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations", *Baltic Yearbook of International Law*, vol. 14, pp. 41-54; cit. en pp. 42-43.
[11] Sin entrar en un análisis detallado, baste con mencionar, por lo que a la atribución se refiere, las siguientes sentencias internacionales: Sentencia CIJ *Actividades militares y paramilitares en Nicaragua y contra Nicaragua*, 27 de junio de 1986, párr. 115; Sentencia del Tribunal Penal Internacional para la Antigua Yugoslavia (ICTY Judgment) *Prosecutor v. Dusko Tadic*, 15 de julio de 1999, párrs. 131-137; Sentencia CIJ *República Democrática del Congo v. República de Uganda*, 19 de diciembre de 2005, párr. 146; Sentencia CIJ *Aplicación de la Convención para la prevención y la represión del crimen de genocidio (Bosnia y Herzegovina v. Serbia y Montenegro)*, 26 de febrero de 2007, párrs. 385-395 y 398-412.
[12] Timo Koivurova (2010), "Due Diligence", en Anne Peters (ed.), *Max Planck Encyclopedia of Public International Law*, Oxford UP, Oxford.
[13] International Law Association (2016), *Study Group on Due Diligence in International Law* (2.ª ed.), relator: Tim Stephens, pp. 5-6.
[14] Paulina Starski (2015), "Right to Self-Defense, Attribution and the Non-State Actor – Birth of the 'Unable or Unwilling' Standard?", *Heidelberg Journal of International Law*, vol. 75, n.º 3, p. 475.
[15] Sentencia de la Corte Internacional de Justicia (CIJ) *Plantas de celulosa en el río Uruguay*, 20 de abril de 2010, párr. 101.
[16] Sentencia CIJ *Actividades militares y paramilitares en Nicaragua y contra Nicaragua*, 27 de junio de 1986, párr. 115.

Estado territorial sobre el grupo no estatal autor del ciberataque, como pide la regla clásica de la atribución[17].

El inconveniente principal del *Manual de Tallin 2.0* es que rechaza la aplicación en el ciberespacio del criterio de precaución –una de las concreciones del estándar de diligencia debida–, que conlleva el deber de todo Estado de *prevenir* las actividades ilícitas contra terceros Estados que se originen en su territorio. Sin embargo, el *Manual* prevé que los Estados deban obviar solo aquellas ciberamenazas que podrían tener "consecuencias graves" para los demás Estados[18]. Con lo cual, no se cargaría a los Estados con una responsabilidad objetiva para *todo* tipo de daño derivado de sus territorios; la responsabilidad estatal se daría solo cuando el daño llegase a constituir una "preocupación legítima en las relaciones entre Estados", es decir, algo más que "un simple inconveniente"[19]. En efecto, en la mayoría de los casos, las actividades cibernéticas transfronterizas no provocan ningún daño importante o tan solo daños mínimos a los demás Estados, como la desfiguración de una página web o denegaciones de servicios no esenciales. Dicho de otra forma, no se trataría de eludir *todo* ciberataque potencial, sino solo los que un Estado "razonable" podría evitar según una serie de elementos circunstanciales como la gravedad de la posible amenaza, los medios técnicos a su disposición o su conocimiento de un cierto riesgo[20].

Los comentarios a la regla 7 del *Manual* subrayan que las "medidas practicables" excluyen la del monitoreo de las infraestructuras cibernéticas estatales como condición para cumplir con la diligencia debida. No obstante, parece ser este uno de los límites más importantes del *Manual* al no impulsar un deber general de prevenir los ciberataques mediante un deber de monitoreo. A falta de un tratado internacional, debería poder imputarse a los Estados la responsabilidad internacional por transgredir el estándar de ciberdiligencia debida cuando omitan evitar, también mediante acciones de monitoreo informático, los ciberataques de grupos privados radicados en su territorio. Si un Estado esperase al conocimiento cierto de la inminencia de un ciberataque determinado –lo que pide el *Manual 2.0*–, podría ser demasiado tarde. Por eso, entre las medidas "razonablemente" posibles para los Estados, habría que incluir la adopción de una legislación interna específica que cree órganos judiciales y administrativos dedicados especialmente a la prevención, monitoreo y sanción de los ciberataques organizados en su territorio contra otros Estados.

Admitiendo las actividades de monitoreo como parte integrante de la ciberdiligencia debida, el Estado víctima de un ciberataque podría esgrimir que el Estado desde cuyo territorio se lanzó omitió tomar las medidas de conocimiento previo necesarias para evitarlo. Si el Estado responsable no demostrase haber adoptado estas medidas, habría violado el estándar de ciberdiligencia debida, con lo que se le podría atribuir responsabilidad internacional por el ciberataque y evitar a la vez una posible escalada

[17] Rusell Buchan (2016), "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm", *Journal of Conflict & Security Law*, vol. 21, n.º 3, pp. 431-432.
[18] Michael N. Schmitt (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge UP, Cambridge, regla 6, comentario 5, pp. 30-32.
[19] Scott J. Shackelford *et al*. (2016), "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors", *Chicago Journal of International Law*, vol. 17, n.º 1, p. 11.
[20] Michael N. Schmitt (2017), *Tallinn Manual 2.0*, *op. cit*., regla 6, comentario 42, pp. 41-42.

en las tensiones. En caso contrario, si el Estado responsable alega haber cumplido con estas medidas de conocimiento previo, el Estado víctima podría esgrimir la prueba del "conocimiento constructivo", es decir, aquel que se puede esperar razonablemente de todo Estado[21].

Así, los Estados malintencionados ya no podrían aprovechar las brechas jurídicas de la diligencia debida del *Manual* para permitir, más o menos voluntariamente, que grupos de actores no estatales utilicen su territorio como trampolín para lanzar sus ciberataques contra otros Estados. En este caso, podrían considerarse responsables del hecho ilícito internacional porque su inacción los convertiría en santuarios para los ciberatacantes. Además, su responsabilidad permitiría a los Estados afectados recurrir a todos los medios que pone a su disposición el Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícito (2001), desde la solicitud de reparación del daño a las contramedidas, hasta llegar, dependiendo de la gravedad del acto, a la legítima defensa del artículo 51 de la Carta de la ONU[22].

Conclusiones

Frente a un Derecho Internacional que no sabe dar una respuesta eficaz ante el problema, cada vez más apremiante, de cómo atribuir responsabilidad internacional al Estado por los ciberataques originados en su territorio, este análisis propone la aplicación del concepto de "ciberdiligencia debida". Dicho estándar incluiría un deber de reaccionar *junto con* el de prevenir, como ya se reconoce en otros ámbitos del Derecho Internacional contemporáneo. Por ejemplo, en el Derecho del medioambiente[23], en el que el respeto de la diligencia debida supone no solo la adopción de una legislación nacional adecuada, sino la *vigilancia* estricta de su cumplimiento por parte de los operadores públicos y privados involucrados en actividades peligrosas para el medioambiente[24].

Desde este prisma, no faltan propuestas esperanzadoras, como las mencionadas a propósito de la última Estrategia Nacional de Ciberseguridad, que apuestan decididamente por desarrollar el Derecho Internacional del ciberespacio y fomentar los mecanismos que permitan la oportuna investigación y persecución de los autores de ciberataques para incrementar las posibilidades de atribución, unos instrumentos por desarrollar en asociación con otras actuaciones preventivas que disuadan o dificulten la comisión de ciberataques.

[21] Sentencia CIJ *Canal de Corfú*, 9 de abril de 1949, p. 18.
[22] Matthew J. Sklerov (2009), "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent", *Military Law Review*, vol. 201, n.º 1, pp. 12-13.
[23] Véase, por ejemplo, Sentencia CIJ *Plantas de celulosa en el río Uruguay*, 20 de abril de 2010, párr. 101.
[24] Karine Bannelier-Christakis (2014), "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?", *Baltic Yearbook of International Law*, vol. 14, p. 8.

Parece así que exista cierta voluntad de algunos Estados –¿tal vez ya su *opinio juris*?– de querer adecuar el Derecho Internacional a la realidad del ciberespacio, que exige adoptar respuestas jurídicas eficaces en lugar de preservar estándares jurídicos ya superados por los tiempos. Estas respuestas podrían concretarse en las actividades de monitoreo descritas arriba, fundamentadas jurídicamente en la noción de "ciberdiligencia debida".