ACADEMIA DE LAS CIENCIAS
Y LAS ARTES MILITARES

Comunicaciones académicas

Ciberoperaciones hostiles transfronterizas

¿Estamos ante un vacío normativo o tiene el Derecho Internacional algo que decir?

Jerónimo Domínguez Bascoy
Academia de las Ciencias y las Artes Militares
Sección de Pensamiento y Moral Militar

15 de abril de 2024

Con el título «Avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional», presentó en el año 1998 la Federación Rusa, en la Primera Comisión sobre Desarme y Seguridad Internacional de la Asamblea General de las Naciones Unidas, un proyecto de resolución, aprobado el 4 de enero de 1999, en el que se invitaba a todos los Estados miembro a que hicieran llegar al Secretario General sus opiniones y observaciones sobre la conveniencia de que se elaborasen principios internacionales para aumentar la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayudar a luchar contra el terrorismo y la delincuencia en la esfera de la información, entre otras cosas.

Se inició, entonces, un proceso intergubernamental, que aún continúa, tendente a velar por la seguridad internacional «en la esfera de la información y las telecomunicaciones», alambicada fórmula para evitar mencionar lo que comúnmente conocemos como «ciberespacio», por ser éste un término con el que Rusia y China no se acomodan, pues más que por la «ciberseguridad», que, respetando el libre flujo de información, promueven las democracias liberales, Rusia y China están más preocupadas por la «seguridad de la información», con el propósito de posibilitar el ejercicio de una vigilancia y censura sobre los contenidos.

En el marco del citado proceso, desde el año 2004 se han constituido seis Grupos de Expertos Gubernamentales, que han acordado informes en los años 2010, 2013, 2015 y 2021, y dos Grupos de Trabajo de Composición Abierta, el primero de los cuales presentó un informe en el año 2021, continuando el segundo con sus actividades hasta el año 2025, en que se espera presente su informe. Los aspectos sobre los que han venido centrando su atención son los relativos a la identificación de las amenazas, al establecimiento de normas, reglas y principios de comportamiento responsable de los Estados, adopción de medidas de fomento de la confianza, desarrollo de capacidades y lo que constituye el objeto de la presente comunicación: «la aplicación del Derecho internacional en el uso de las Tecnologías de Información y Comunicaciones (TIC), por parte de los Estados». Fue, precisamente, este último aspecto, el de la aplicación del Derecho Internacional, el que, debido a las discrepancias manifestadas por los representantes de los Estados de la órbita de Rusia y China, hizo descarrilar el informe que el quinto grupo de expertos debía haber presentado en el año 2017, y que provocó de este modo la bifurcación del proceso, con la constitución de los dos grupos de trabajo.

En cuanto a la aplicación del Derecho Internacional en el ciberespacio, se pasó de las vacilaciones iniciales a una práctica unanimidad. Si bien en un primer momento se cuestionó la viabilidad de aplicar a las actividades de los Estados en el ciberespacio las normas de derecho internacional surgidas en la era pre- digital, algunos estados de la Organización de Cooperación de Shanghái presentaron en 2011 y 2015, ante la Asamblea General de las Naciones Unidas, sendos proyectos sobre un «Código Internacional de Conducta para la Seguridad de la Información». Finalmente, se ha considerado que, frente a esas nuevas normas –con las que se persigue desarrollar un sistema «multilateral» para la gobernanza de Internet, así como legitimar la censura y el control estatal sobre Internet– el vigente Derecho internacional aplicable a las actividades en el «mundo físico», sirva también para regular las llevadas a cabo en ese «mundo virtual» que es el ciberespacio.

Estados Unidos, por boca del Asesor Jurídico del Departamento de Estado, Harold Hongju Koh, en la presidencia de Obama, negó de forma rotunda que el ciberespacio fuera a ser una zona no sometida a normas jurídicas, afirmando, por el contrario, que en aquél espacio es aplicable el Derecho internacional existente. En una conferencia pronunciada en Fort Meade (Maryland), sede del Mando de Ciberdefensa norteamericano en septiembre de 2012, Harold Koh indicó que a pesar de que algunos Estados piensan que el Derecho internacional existente no sirve para dar respuesta a las cuestiones que plantea Internet, por lo que se necesitarían nuevos tratados para imponer un conjunto único de reglas para el ciberespacio, los Estados Unidos entienden, por el contrario, que los principios establecidos del Derecho internacional son aplicables en aquél. Además, destacó

que el ciberespacio no es una zona «al margen de la ley» donde cualquiera pueda realizar actividades hostiles sin estar sometido a reglas ni restricciones. Estados Unidos considera que se debe articular y generar un consenso acerca de cómo se aplica el derecho internacional y reevaluar a partir de ahí si se necesitan interpretaciones adicionales.

Esa posición de EE. UU. con el paso de los años ha venido a constituirse en la mantenida de forma mayoritaria por los Estados y que puede sintetizarse señalando que la cuestión no es si el Derecho internacional es aplicable en el ciberespacio, si no la de cómo se aplica. Las peculiaridades de las ciberoperaciones hacen que surjan muchas dudas acerca de cómo deben interpretarse, en relación con las actividades de los Estados en el ciberespacio, reglas esenciales del Derecho internacional, tales como la de la soberanía estatal, el principio de no intervención en los asuntos internos y externos de otros Estados, la prohibición del uso de la fuerza o las contenidas en el Derecho de los Conflictos Armados o Derecho Internacional Humanitario, muy especialmente las referidas a lo que podríamos denominar Derecho del targeting (proceso de identificación y selección de objetivos).

Michael N. Schmitt, quizás la mayor autoridad en esta materia, indica que siendo muy escasas las perspectivas de que, en el actual escenario, se adopten nuevas normas internacionales aplicables al ciberespacio, parece claro que la mayor parte del progreso se producirá por vía de interpretación, principalmente por parte de los Estados, de normas del Derecho internacional. Añade que es probable que esta interpretación esté motivada por la percepción predominante de que el Derecho internacional es un útil cortafuegos normativo contra ciberoperaciones hostiles atribuibles a (o lanzadas desde) otros Estados y que, aunque, el proceso se topará, sin duda, con obstáculos, cree que hay motivos para ser optimistas, al observar cómo el alcance y ritmo de esos esfuerzos interpretativos está aumentando, lo que pone de manifiesto el compromiso de muchos Estados a la hora de garantizar que el ciberespacio sea un dominio regido por el imperio de la ley.

En el plano puramente académico, aunque con el impulso y respaldo del Cooperative Cyber Defence Centre of Excellence de la OTAN, es, precisamente, el citado Michael N. Schmitt quien ha dirigido los proyectos que han fructificado en las que, con toda seguridad, son las obras en que con mayor detalle y profundidad se han llevado a cabo la citada labor interpretativa. Nos referimos a las dos ediciones del conocido «Manual de Tallin», de 2013, sobre el Derecho internacional aplicable a la ciberguerra, y, la segunda, de 2017, con un mayor alcance, sobre el Derecho internacional aplicable a las ciberoperaciones en general. También bajo la dirección de Michael N. Schmitt, en 2021 el Centro de Excelencia puso en marcha una

iniciativa de cinco años que implicará la revisión de los capítulos existentes y la exploración de nuevos temas en la redacción de un tercer Manual.

Examinemos el estado de la cuestión en el seno de organizaciones internacionales o supranacionales (ONU, OTAN y UE). Empezando por la ONU, la aplicación del Derecho internacional en el ciberespacio en los trabajos acometidos en el ámbito de las Naciones Unidas destaca los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, informe del año 2013 del Grupo de Expertos, donde se hizo mención a las «normas derivadas del derecho internacional vigente que sean pertinentes para el uso de las tecnologías de la información y las comunicaciones por parte de los Estados», reconociéndose que la aplicación de dichas normas es «fundamental con el fin de reducir los riesgos para la paz, la seguridad y la estabilidad internacionales». La declaración del informe más relevante por ser la primera formulada en un ámbito intergubernamental con presencia de representantes de Estados de muy distintas sensibilidades, es la de que «El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías».

En el informe presentado en 2015 por el siguiente Grupo de Expertos se incluyó un apartado específicamente dedicado a la «Aplicación del derecho internacional al uso de las Tecnologías de Información y Comunicaciones». Así, se señaló la importancia fundamental que tenían los compromisos de los Estados con los principios de la Carta de la ONU y otras normas del derecho internacional: la igualdad soberana; la solución de controversias internacionales por medios pacíficos de tal manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia; la abstención, en sus relaciones internacionales, 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; el respeto de los derechos humanos y libertades fundamentales; y la no intervención en los asuntos internos de otros Estados. Y, aunque se evitó hacer una mención explícita al Derecho Internacional Humanitario, sí aparece implícitamente en esta parte del informe cuando señala, en cuanto a la forma en que el Derecho internacional se aplica al uso de las TIC por los Estados, «que existen principios jurídicos internacionales establecidos, incluidos, si procede, los principios de humanidad, necesidad, proporcionalidad y distinción». Fórmula un tanto rebuscada, con la que al menos se consiguió la unanimidad dada la reticencia de ciertos Estados a reconocer de forma expresa que el Derecho Internacional Humanitario es aplicable a las ciberoperaciones que tienen lugar en conexión con un conflicto armado.

El siguiente Grupo de Expertos, que debía haber presentado su informe en 2017, fracasó porque no se pudo llegar a un acuerdo sobre un párrafo en el que se detallaba algo más cómo se aplica el Derecho internacional al uso de las TIC por parte de los Estados. Algunos Estados se negaron a respaldar dicho párrafo con la excusa de que la aplicación de los principios de la Carta de las Naciones Unidas sobre el uso de la fuerza y el Derecho Internacional Humanitario daría lugar a la «militarización» del ciberespacio. Un evidente paso atrás.

Así, habría que esperar hasta el año 2021, en el que, tras la referida bifurcación del proceso, fueron dos los informes presentados: uno, en el mes de marzo, del primer Grupo de Trabajo, y el otro, el del sexto Grupo de Expertos, en el mes de julio. En el primero de ellos, la búsqueda de la unanimidad con visiones muy diferentes hizo que apenas se progresara con respecto a lo que ya se había dicho en el informe citado de 2015. En 2021 se pidió a los Estados que evitaran y se abstuvieran de adoptar cualquier medida que no estuviera en consonancia con el Derecho internacional, y en particular con la Carta de las Naciones Unidas, y se apuntó que los Estados deberían seguir estudiando y debatiendo, en el marco de futuros procesos de las Naciones Unidas, cómo se aplica el Derecho internacional al uso de las Tecnologías de Información y Comunicaciones, como paso clave para aclarar y seguir desarrollando entendimientos comunes sobre la cuestión. Nada concreto, en definitiva.

El informe de julio de 2021, del sexto Grupo de Expertos, sí supuso, por el contrario, un avance significativo, al menos en cuanto al reconocimiento expreso de la aplicación al ciberespacio de ciertas normas cruciales del Derecho internacional. El apartado IV del informe, dedicado al Derecho internacional, contiene, en este sentido, importantes declaraciones:

a) De acuerdo con las obligaciones que les incumben, los Estados parte en una controversia internacional, incluidas las relativas al uso de las TIC, cuya continuación sea susceptible de poner en peligro el mantenimiento de la paz y la seguridad internacionales deben tratar de buscarle solución, ante todo, por los medios contemplados en la Carta de las Naciones Unidas, es decir, la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección.

b) La soberanía de los Estados y las normas y principios internacionales que de ella dimanan son aplicables a la realización por los Estados de actividades relacionadas con las TIC y a su jurisdicción sobre la infraestructura relativa a esas tecnologías que se halle en su territorio.

c) De conformidad con el principio de no intervención, los Estados no deben intervenir directa o indirectamente en los asuntos internos de otro Estado, incluso por medio de las TIC.

d) En su uso de las TIC, los Estados deben abstenerse de recurrir, en sus relaciones internacionales, 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.

e) Subrayando las aspiraciones de la comunidad internacional de que las TIC se utilicen pacíficamente para el bien común de la humanidad, se reconoce el derecho inherente de los Estados a adoptar medidas compatibles con el derecho internacional y reconocidas en la Carta, así como la necesidad de seguir estudiando esta cuestión.

f) Es necesario seguir estudiando cómo y cuándo los principios de humanidad, necesidad, proporcionalidad y distinción del Derecho Internacional Humanitario se aplican al uso de las TIC por parte de los Estados, lo que –frente a lo afirmado por algunos– no supone legitimar ni fomentar en absoluto los conflictos.

g) Los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar en virtud del derecho internacional, no deben recurrir a terceros para cometer hechos internacionalmente ilícitos utilizando las TIC, y deben tratar de garantizar que su territorio no sea utilizado por actores no estatales para realizar esos hechos.

En este informe se alienta, además, a todos los Estados a que sigan compartiendo voluntariamente sus opiniones y evaluaciones nacionales acerca de la cuestión de cómo se aplica el Derecho internacional al uso de las TIC por los Estados. Es decir, a la fijación de posiciones nacionales, como las que, desde la de los Estados Unidos del 2012, a que antes nos hemos referido, se han venido produciendo hasta el presente, especialmente en los últimos cuatro años. Las más recientes, en el contexto de los trabajos del actual Grupo de Trabajo, como es el caso, muy significativo, de la posición común que la Unión Africana ha adoptado en enero de 2024.

En cuanto a la OTAN y la aplicación del Derecho internacional en el ciberespacio, en la declaración que el 5 de septiembre de 2014 realizaron los Jefes de Estado y de Gobierno participantes en la reunión del Consejo del Atlántico Norte celebrada en Gales, los miembros de la Alianza reconocieron que el Derecho internacional, incluido el Derecho Internacional Humanitario y la Carta de las Naciones Unidas, se aplica en el ciberespacio. Tras valorar que el impacto de un ciberataque podría ser tan dañino para las sociedades modernas como un ataque convencional,

afirmaron, además, que la ciberdefensa forma parte de la misión central de la OTAN de defensa colectiva y que el Consejo del Atlántico Norte decidiría, caso por caso, cuándo un ataque cibernético daría lugar a la invocación del artículo 5. En otras palabras, se admitió la posibilidad de que una ciberoperación hostil alcanzara la dimensión de un «ataque armado», justificando de esta forma una respuesta en uso del derecho a la legítima defensa colectiva.

Casi dos años después, en la declaración de 9 de julio de 2016, formulada al término de la reunión en la cumbre de Varsovia, la Alianza reafirmó ese mandato defensivo y reconoció el ciberespacio como un dominio de operaciones en el que la OTAN debe defenderse con la misma eficacia que lo hace en el aire, en la tierra y en la mar. Se reafirmó, además, el compromiso de actuar de conformidad con el Derecho internacional, incluida la Carta de las Naciones Unidas, el Derecho Internacional Humanitario y las normas de los derechos humanos, según corresponda.

Al margen de estas declaraciones políticas, el documento OTAN en el que, con mayor nivel de detalle, se contempla la aplicación del Derecho internacional en el ciberespacio es la publicación aliada 3.20, adoptada en enero de 2020, en la que se contiene la Allied Joint Doctrine for Cyberspace Operations. Su capítulo 3, sobre planeamiento y conducción de ciberoperaciones, dedica toda una sección, la segunda, a las consideraciones de naturaleza jurídica, que fueron objeto de un interesante análisis por parte de Michael N. Schmitt, al que nos remitimos. Destacaremos, tan solo, algunas de las consideraciones que se hacen en esta AJP-3.20:

a) Si bien muchos de los efectos de las ciberoperaciones probablemente caen por debajo del umbral del uso de la fuerza o del ataque armado, algunas pueden crear efectos equivalentes a un uso de la fuerza conforme al Artículo 2(4) de la Carta de las Naciones Unidas o a un ataque armado, dando lugar al derecho inherente a la legítima defensa individual o colectiva previsto en el artículo 51 de la Carta. Los criterios que podrían considerarse al realizar esta evaluación incluyen la escala y efectos del ataque, que podrían tener en cuenta factores tales como la interferencia con infraestructuras o su funcionalidad, la gravedad y reversibilidad de los efectos, la inmediatez de las consecuencias, o, en fin, lo invasivo de esos efectos.

b) En consonancia con el reconocimiento por parte de los aliados de que el Derecho internacional se aplica en el ciberespacio, los principios fundamentales del Derecho de los Conflictos Armados de necesidad militar, humanidad, proporcionalidad y distinción se aplican a las ciberoperaciones (sobre cuya aplicación el documento proporciona aclaraciones en relación con los objetos de «doble uso», tan abundantes en el ciberespacio, o la estimación de daños colaterales).

Finalmente en cuanto a la UE y la aplicación del Derecho internacional en el ciberespacio, en la primitiva Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro, del año 2013, la UE afirmaba que, en su política internacional del ciberespacio, promovería la libertad en Internet, alentaría las actividades de elaboración de normas de conducta y aplicaría el Derecho internacional existente, añadiendo, además, que, en caso de que los conflictos armados se extendieran al ciberespacio, se aplicarían el Derecho internacional humanitario y, en su caso, el Derecho internacional en materia de derechos humanos.

En la vigente Estrategia de Ciberseguridad de la UE para la Década Digital, de 2020, se destaca que la UE continúa trabajando con sus socios internacionales para avanzar y promover un ciberespacio global, abierto, estable y seguro en el que se respete el Derecho internacional, en concreto la Carta de las Naciones Unidas, y se cumplan las normas voluntarias, reglas y principios de conducta responsable de los Estados. Se añade, también, que la UE es la más indicada para avanzar, coordinar y consolidar las posturas de los Estados miembros en los foros internacionales y debe desarrollar una postura común sobre la aplicación del Derecho internacional en el ciberespacio.

Tras recordar que, en 2018, la UE había identificado el ciberespacio como un dominio de operaciones, se alude en la Estrategia a una próxima Visión y estrategia militar en el ciberespacio como un dominio de operaciones, a desarrollar por el Comité Militar de la UE, en la que se debería definir aún más cómo el ciberespacio permite que se realicen las misiones y operaciones militares de la UE. Ese documento fue aprobado en septiembre de 2021 y, a los efectos que ahora nos interesan, merece destacarse el párrafo en el que se afirma que, por encima de cualquier otra consideración, el Derecho internacional, incluida la Carta de las Naciones Unidas en su totalidad, el Derecho Internacional Humanitario, el Derecho internacional de los derechos humanos y el Derecho aplicable a los conflictos armados, se aplica en el ciberespacio, por lo que los principios establecidos de necesidad, distinción y proporcionalidad vinculan a toda la Política Común de Seguridad y Defensa de la UE. Además, se añade, los mandos militares deberán llevar a cabo cualquier acción en el ciberespacio de conformidad con el mandato de la operación y bajo unas «reglas de enfrentamiento» políticamente acordadas.

En cuanto a esa postura común acerca de la aplicación del Derecho internacional en el ciberespacio que, según la vigente Estrategia, deberá desarrollar la Unión Europea, existen datos que permiten ser optimistas en cuanto a su efectiva concreción. Sobre la base de un estudio –cuya publicación se espera para mayo-junio de 2024–, encargado a Michael N. Schmitt y Liis Vihul por el Instituto de Estudios de Seguridad de la UE, acerca de los puntos de convergencia y

divergencia entre los doce Estados miembros que, hasta el momento, han hecho públicas sus posiciones nacionales, se ha adoptado el pasado 8 de abril un borrador de la posición de la UE sobre la aplicación del Derecho Internacional al Ciberespacio. Se adelantan en este documento los aspectos debatidos sobre los que la UE habrá de fijar su posición: la soberanía nacional, el principio de no intervención, la diligencia debida, el uso de la fuerza, el Derecho Internacional Humanitario, el Derecho internacional de los derechos humanos, así como las distintas opciones de respuesta, una vez resuelto el problema de la atribución: medios pacíficos, retorsión, contramedidas, estado de necesidad y legítima defensa. Para ello, se anima a los Estados miembro que no lo hayan hecho aún (entre ellos, España) a que desarrollen posiciones nacionales en las que se aborden en profundidad las cuestiones que, en relación con esos aspectos, plantea la aplicación del Derecho internacional a las ciberoperaciones.

En una futura comunicación académica, una vez que se haya acordado y hecha pública la posición española y la común de la UE, será la ocasión apropiada para concretar cuáles son los debates planteados hasta entonces. Seguramente, en el seno del actual Grupo de Trabajo se habrán también presentado otras posiciones nacionales, que permitan apreciar si ya hay tendencias dominantes en cuanto a cómo interpretar, en su aplicación al ciberespacio, normas básicas para el mantenimiento de unas relaciones internacionales pacíficas y seguras. ▮