CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

PROTEGER LOS DATOS FINANCIEROS EN EL CIBERESPACIO: ¿UN PRECEDENTE PARA MAYORES AVANCES EN MATERIA DE CIBERNORMAS?

MICHAEL SCHMITT Y TIM MAURER | AUGUST 24, 2017

Esta artículo fue publicada originalmente por Just Security.

Identificar las normas legales que se aplican en el ciberespacio sigue siendo una tarea sumamente difícil. El reciente colapso del 5.º Grupo de Expertos Gubernamentales (GEG) de la ONU sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional es un ejemplo de las dificultades constantes que tienen los Estados para ponerse de acuerdo incluso sobre principios fundamentales, como el derecho de legítima defensa en el ciberespacio y la aplicación del derecho internacional humanitario durante un conflicto armado.

En lo que respecta a la identificación de normas, las ciberoperaciones orientadas a los datos están entre las cuestiones más problemáticas, tanto en tiempo de paz como de guerra. Entre estas, merecen especial mención aquellas relacionadas con datos financieros, en gran parte debido a la interdependencia del sistema financiero mundial. En respuesta a esta situación, el Fondo Carnegie para la Paz Internacional (Carnegie Endowment for International Peace) ha exhortado a los Estados a comprometerse a no realizar actividades que "menoscaben la integridad de datos y algoritmos de instituciones financieras, tanto en tiempo de paz como de guerra", así como la disponibilidad de sistemas financieros críticos, como las cámaras de compensación. También se pide a los Estados que asumen ese compromiso que respondan oportunamente a las solicitudes pertinentes de asistencia formulados por otro Estado cuando ocurran este tipo de incidentes.

Creemos que se trata de una propuesta valiosa. Tal vez igualmente importante es que, al generar consenso y cooperación respecto de un tema acotado —la estabilidad financiera— ante la actual indefinición jurídica, este enfoque podría allanar el camino para alcanzar acuerdos más generales con respecto a otras actividades. En este artículo, destacamos los retos jurídicos que supone aplicar el derecho internacional a cuestiones relacionadas con datos, describimos la propuesta de Carnegie y reflexionamos sobre cómo ese enfoque podría proporcionar una vía de salida de la confusión que reina actualmente e impide alcanzar un consenso sobre cibernormas jurídicas.

DATOS Y DERECHO INTERNACIONAL

El derecho internacional, como se explica en el Manual Tallinn 2.0, establece un extenso catálogo de prohibiciones que se aplican a las ciberoperaciones, incluidas aquellas que afectan a

Sobre los autores

Michael Schmitt *es titular de la cátedra de Derecho Internacional Público en la Facultad de Derecho de la Universidad de Exeter en el Reino Unido; docente Charles H. Stockton en el Centro Stockton para el Estudio del Derecho Internacional de la Escuela de Guerra Naval de EE. UU.; académico distinguido Francis Lieber en la Academia Militar de EE. UU. en West Point; y director de Asuntos Legales de Cyber Law International. Sígalo en Twitter (@Schmitt_ILaw).*

Tim Maurer *es codirector de la Iniciativa sobre Ciberpolíticas del Fondo Carnegie para la Paz Internacional (Carnegie Endowment for International Peace). Sígalo en Twitter (@maurertim).*

los datos, en tiempo de paz. Las tres prohibiciones que es más probable que se vean afectadas por esas operaciones son las vinculadas con la soberanía, la intervención coercitiva y el uso de la fuerza.

Las violaciones de la soberanía se manifiestan de dos formas. En primer lugar, la soberanía preserva la integridad territorial, por ejemplo, prohibiendo ciberoperaciones remotas que perjudiquen la infraestructura cibernética ubicada en el territorio de otro Estado o, posiblemente, una interferencia sustancial en la funcionalidad de dicha infraestructura. La manipulación, alteración o eliminación de datos podrían generar tales resultados, por ejemplo, cuando se provocan problemas de funcionamiento en un sistema SCADA (un sistema de control industrial que se utiliza habitualmente para gestionar y controlar los procesos de una planta, maquinarias, etc.). En segundo lugar, una violación de la soberanía se produce cuando un Estado interfiere con las funciones propiamente gubernamentales de otro Estado, o las usurpa. Un ejemplo sería la alteración o eliminación de datos que hayan sido recopilados para fines de aplicación de la ley.

Sin embargo, no resulta claro si las operaciones cibernéticas contra datos que provocan efectos por debajo del primer umbral constituyen violaciones de la soberanía. Es improbable que las acciones orientadas a manipular la integridad de los datos financieros generen daños físicos o deterioren la funcionalidad de la infraestructura cibernética (aun así, podrían mellar la confianza en las instituciones financieras y tener un grave efecto desestabilizador); por ende, se ubican en esta situación de indefinición jurídica. Asimismo, el límite entre las actividades financieras que constituyen actos propiamente gubernamentales y aquellas que no lo son no es nítido. Aunque los datos financieros relacionados con el sistema tributario del Estado, por ejemplo, quedarían claramente alcanzados por la protección, los datos alojados en los servidores de bancos estatales podrían no estarlo.

La segunda prohibición es aquella contra la intervención ilegítima de un Estado en los asuntos internos o externos de otro Estado. La violación de esta prohibición, que fue reconocida por la Corte Internacional de Justicia en su sentencia sobre Nicaragua, supone que haya actos "coercitivos" relacionados con el "ámbito de incumbencia exclusiva" (*domaine réservé*) de otro Estado. El término coercitivo alude a actos que provocan que un Estado participe en actividades que, de lo contrario, no llevaría a cabo, o se abstenga de aquellas en las que normalmente participaría. El ámbito de incumbencia denota actividades reservadas al Estado, es decir, que están por fuera de la esfera del derecho internacional. Un ejemplo paradigmático de una intervención cibernética prohibida es la manipulación de resultados electorales. En el contexto de los datos financieros, un ejemplo de una intervención cibernética prohibida podría ser una operación contra la integridad de los datos financieros de los sistemas de jubilación o de bienestar social para exigir que el Estado objeto de estas acciones adopte una determinada política interna.

Lamentablemente, los conceptos de coerción y ámbito de incumbencia exclusiva no son en absoluto precisos. Por ejemplo, una ciberoperación que solamente ponga en tela de juicio la validez de esos datos —a diferencia de una que los manipule— posiblemente provocaría desacuerdos con respecto a si se cumple el criterio coercitivo, mientras que no sería claro que una ciberoperación dirigida a los datos de una empresa privada que brinda planes de jubilación a empleados del Estado reúna las características de una intrusión en el ámbito de incumbencia exclusiva.

Uno de los pilares del derecho internacional en tiempos de paz es la prohibición del uso de la fuerza estipulada en el artículo 2(4) de la Carta de las Naciones Unidas y en el derecho internacional consuetudinario. Pese a la vacilación del GEG, pareciera existir un amplio consenso de que una operación cibernética destructiva o perniciosa lanzada por un Estado contra otro trascendería el umbral de uso de la fuerza y, si es lo suficientemente severa para constituir un "ataque armado", podría dar lugar a enérgicas respuestas cibernéticas o cinéticas al amparo del derecho de legítima defensa conforme al derecho internacional consuetudinario, que se refleja en el artículo 51 de la Carta. Del mismo modo, parecería haber consenso en cuanto a que la mera destrucción de datos no constituye, por sí sola, el tipo de acción prohibida contemplada por la prohibición de uso de la fuerza.

Sin embargo, persiste el debate acerca de si las operaciones cibernéticas que no comporten destrucción física constituyen igualmente instancias prohibidas de uso de la fuerza. En

particular, podría decirse que lo importante no es tanto la naturaleza de las consecuencias (destructiva o no) sino su severidad. Desde este enfoque, una operación cibernética dirigida a datos financieros que provoca, por ejemplo, una grave inestabilidad financiera y perturbaciones económicas generalizadas podría constituir un uso prohibido de la fuerza. Sin embargo, este enfoque está lejos de estar aceptado universalmente, y sigue habiendo divergencias, incluso entre sus defensores, en cuanto a cuál es el umbral que convertiría a una operación cibernética en una operación suficientemente severa.

En cuanto al contexto de un conflicto armado internacional, el marco normativo para el tratamiento de datos es igualmente controvertido. En este sentido, se advierten tres obstáculos. En primer lugar, la mayor parte de las prohibiciones del derecho internacional humanitario relativas a la determinación de objetivos se formulan en términos de "ataque", incluida aquella que prohíbe un ataque contra bienes de carácter civil. En este sentido, existe consenso de que las operaciones cibernéticas que causan destrucción física constituyen ataques y, por lo tanto, no pueden estar dirigidas a bienes de carácter civil. Esto incluiría la alteración o eliminación de datos que redunden en un daño físico a la infraestructura cibernética que depende de ellos, o la pérdida permanente de funcionalidad de dicha infraestructura. No obstante, hay diferencias de criterio con respecto a las operaciones que no provocan destrucción física. En particular, no resulta claro si una operación cibernética que menoscaba la integridad de datos financieros, pero no afecta la infraestructura cibernética asociada, constituiría un ataque y, por ende, estaría sujeta a la prohibición de ataques contra bienes de carácter civil.

En segundo lugar, hay descuerdo con respecto a si los datos constituyen un "bien", y si la prohibición de atacar bienes de carácter civil acaso se aplica. Por un lado, están quienes aquellos sostienen que los datos son intangibles y que, por ende, no se encuadran —al menos por el momento— dentro del significado raso de la palabra "bien". Otros sostienen lo contrario, en cuanto a que, por ejemplo, los datos pueden ser almacenados, transferidos físicamente en medios como una memoria USB y destruidos (ver aquí y aquí). La diferencia de interpretación es clave, pues si los datos financieros y otros datos de carácter civil no reúnen las características de bienes, podrían ser determinados como blanco sin que, salvo algunas pocas excepciones, esto suponga una violación del derecho internacional humanitario.

Por último, si asumimos únicamente a efectos de este análisis que los datos son un "bien" susceptible de ser "atacado" conforme a la definición legal de ataque, se plantea el interrogante de cuáles datos serían "objetivos militares" legalmente pasibles de ataque. Sin duda, los datos empleados para entablar una guerra ("combate bélico"), como aquellos presentes en un sistema de mando y control o una base de datos de orientación, reunirían las características de un objetivo militar. También lo harían aquellos que apoyan de manera directa el esfuerzo bélico ("apoyo bélico"), como el caso de los datos que son indispensables para el funcionamiento de una planta de municiones. Sin embargo, hay un largo debate sobre los denominados bienes de "sostenimiento bélico". Estados Unidos entiende (ver párr. 5.6.6.2 del Manual del Departamento de Defensa) que cuando un bien contribuye al sostenimiento bélico eso lo convierte en blanco legítimo, como sucede con el petróleo de exportación, pues las utilidades obtenidas de su venta posibilitan mantener el esfuerzo bélico. Muchos otros Estados, al igual que numerosos expertos en derecho internacional humanitario, no están dispuestos a ampliar a ese extremo el concepto de objetivos militares. El tema reviste importancia directa para el contexto de los datos, debido a que las operaciones cibernéticas que tienen como objetivo el sistema financiero de un enemigo podrían obstaculizar de manera directa su capacidad de sostener el conflicto. De hecho, su efecto probablemente sería mayor que el de ataques cinéticos o cibernéticos contra recursos petroleros o de otro tipo que contribuyen indirectamente al sustento económico del esfuerzo bélico.

Debido a esa incertidumbre tanto en tiempo de paz como de guerra, el derecho internacional, al menos en lo que atañe a los datos, sencillamente no está preparado para salvaguardar a los sistemas financieros nacionales, regionales y globales interdependientes.

LA PROPUESTA DE CARNEGIE

Ante esta ambigüedad normativa, Carnegie ha presentado su propuesta, la cual toma en cuenta que, independientemente de cuál sea la interpretación correcta de la ley, las operaciones cibernéticas hostiles que afectan la integridad de los datos de las instituciones financieras, ya sea en tiempo de paz o de

conflicto armado, pueden tener consecuencias devastadoras mucho más allá de las fronteras del Estado donde se encuentra la institución financiera que ha sido blanco de la acción. Este riesgo se extiende a la falta de disponibilidad de algunos sistemas que son cruciales para la estabilidad financiera. Algunos ejemplos de efectos de contagio incluyen el impacto que tuvo en toda Asia el colapso de la moneda tailandesa en 1997 y la crisis financiera mundial propiciada por la caída, en 2008, de la compañía global de servicios financieros Lehman Brothers. Las operaciones cibernéticas ofensivas podrían disparar crisis de características similares en el futuro.

La ejecución de tales operaciones durante los conflictos armados también podría tener amplias consecuencias. Esto quedó ilustrado hace más de un siglo, durante la Primera Guerra Mundial, cuando los británicos aprovecharon su poderío e influencia en el comercio y el sistema financiero mundial para librar una guerra económica contra Alemania. En pocos meses, se desistió de esa estrategia debido a sus efectos ulteriores, que se sintieron incluso sobre Gran Bretaña. En los conflictos bélicos modernos, sin duda una operación cibernética contra el sistema financiero de una parte beligerante tendrá efectos adversos sobre otros Estados no involucrados en el conflicto. Esto plantea el serio interrogante de si tales operaciones serían congruentes con el objeto y fin del derecho internacional humanitario y el principio de neutralidad.

El acuerdo propuesto por Carnegie tendría un alcance modesto. En su redacción actual, está dirigido únicamente a los Estados del G20, pues es en este ámbito donde sería viable que progresara inicialmente, y porque un acuerdo entre ellos tendría un fuerte valor como precedente ante otros Estados. A su vez, el acuerdo estaría limitado al sector financiero. Ese sector sería muy propicio para un enfoque de ese tipo, pues la interdependencia que lo distingue, además de acentuar la vulnerabilidad del sector, hace que alcanzar un acuerdo para su protección resulte de interés común.

Un dato relevante es que la propuesta contempla únicamente la integridad de los datos de instituciones financieras y la disponibilidad de sistemas financieros críticos que podrían tener efectos de desestabilización similares. En particular, no incluye la prohibición de realizar operaciones cibernéticas que se limiten a bloquear el acceso a datos durante un breve período o que violen la confidencialidad. Carnegie entiende —según creemos, acertadamente— que los riesgos asociados con la manipulación de datos financieros son mucho más graves que la mayoría de las operaciones que tienen como resultado que los datos no estén disponibles o ya no sean confidenciales. Por ejemplo, los ataques distribuidos de denegación de servicio tienen carácter temporario y reversible y, salvo algunas excepciones, no suponen un riesgo significativo para la estabilidad financiera. Asimismo, la propuesta de Carnegie reconoce que, en algunas situaciones, los Estados podrían tener motivos defendibles para impedir que algunos datos financieros no estén disponibles temporariamente o para violar la confidencialidad de datos, como en el supuesto en el que se pretende coartar el financiamiento del terrorismo o reunir datos de inteligencia necesarios para la seguridad nacional.

Podría decirse que la exigencia de responder rápidamente a una solicitud de asistencia de otro Estado cuando ocurran tales incidentes ya forma parte del principio de debida diligencia. Es cierto que ese principio, tal como se aplica en el contexto cibernético, es algo controvertido. Pero aun así, se debe destacar que el GEG de la ONU de 2015, un órgano que incluye los cinco miembros permanentes del Consejo de Seguridad, recomendó en términos exhortativos que los Estados "deberían procurar garantizar que su territorio no sea utilizado por agentes no estatales" realizar actividades ilegales.

A fin de evitar que los Estados se inquieten por la aplicación del acuerdo en un supuesto de conflicto armado, subrayamos que únicamente incluiría la integridad de los datos y la disponibilidad de sistemas financieros críticos cuando un ataque sobre estos tendría efectos de contagio que probablemente afecten la estabilidad financiera. No prohibiría las acciones que tengan como blanco datos financieros diferenciados que utilicen exclusivamente las fuerzas militares, ni tampoco los Estados aceptarían una prohibición de ese tipo. Por ejemplo, los datos o algoritmos financieros que son exclusivos de las fuerzas armadas, como los algoritmos necesarios para pagar los salarios de los soldados, serían un blanco admisible.

¿UN MODELO PARA FUTUROS AVANCES?

El éxito de la propuesta podría servir de modelo para extender el acuerdo más allá de los confines de los datos de las instituciones financieras. Por ejemplo, el GEG de la ONU ha destacado reiteradamente la importancia de proteger la

infraestructura crítica. Claramente, un acuerdo sobre estos temas sería más complejo que el expuesto precedentemente.

Sin embargo, parecería factible alcanzar un consenso, por ejemplo, en cuanto a la protección de los datos utilizados por los sistemas de atención sanitaria o de distribución de alimentos y agua. El mismo criterio podría aplicarse a la integridad de las elecciones, al menos en tiempo de paz. Y con respecto a los conflictos armados, uno de nosotros ha propuesto que los Estados acepten, como política, la prohibición de efectuar operaciones cibernéticas contra datos que sustenten "funciones civiles esenciales", como los servicios bancarios o de transporte que no estén relacionados con el conflicto armado, y esta sugerencia posteriormente fue replicada por el Comité Internacional de la Cruz Roja en un importante informe sobre derecho humanitario. Ciertamente, definir el concepto de "funciones civiles esenciales" sería casi tan difícil como ponerse de acuerdo sobre el alcance del término infraestructura cibernética crítica para su aplicación en tiempo de paz. No obstante, al igual que en el caso anterior, sería factible un acuerdo sobre funciones esenciales específicas. Estos acuerdos eludirían hábilmente los vacíos legales que se observan en la aplicación del derecho internacional a los datos.

Lo clave es que las deficiencias del derecho internacional no deberían interponerse a la posibilidad de convenir políticas para la protección de los valores que son comunes a nuestras sociedades, tanto en tiempo de paz como de conflicto armado. Incluso tales acuerdos podrían evolucionar a lo largo del tiempo, hasta el punto en que el cumplimiento nazca de un sentido de obligación jurídica. Si esto fuera así, la norma en cuestión se materializaría como derecho internacional consuetudinario vinculante. Ante la intransigencia de la comunidad de Estados para acordar normas jurídicas, la iniciativa Carnegie podría servir de modelo para una vía alternativa que conduzca en la misma dirección.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

El Fondo Carnegie para la Paz Internacional (Carnegie Endowment for International Peace) es una red mundial única de centros dedicados a la investigación de políticas en Rusia, China, Europa, Oriente Medio, la India y Estados Unidos. Desde hace más de cien años, nuestra misión ha consistido en promover la paz mediante el análisis y el desarrollo de nuevas ideas en materia de políticas y la participación y colaboración directas con quienes toman decisiones en gobiernos, empresas y en la sociedad civil. Nuestros centros, mediante el trabajo en conjunto, aportan una diversidad sumamente valiosa de puntos de vista nacionales sobre temas bilaterales, regionales y globales.

@CarnegieEndow **facebook.com/CarnegieEndowment**