Hack-back: ¿legítima ciberdefensa en empresas?

Andrés Montero | Presidente de la Fundación Concepto.

Tema

Los Estados y las empresas han desarrollado sistemas, principalmente defensivos, frente a los ciberataques recibidos. Pero ahora se plantean realizar acciones ofensivas contra los atacantes (hack-back).

Resumen

Las empresas estratégicas y de infraestructuras críticas son el objeto preferente de los ciberataques, con el apoyo implícito o explícito de Estados con geopolíticas agresivas, que utilizan cepas sofisticadas de *malware* (virus informáticos) para atacar y vulnerar los sistemas tecnológicos de esas empresas, robar información de alto valor (ciberespionaje), destruir sus datos o distorsionar sus procesos críticos. Los Estados y las empresas han desplegado y robustecido capacidades de ciberseguridad y de ciberdefensa, pero no logran impedir ciberataques cada vez más sofisticados y dañinos.

Algunos Estados están considerando o incluyendo directamente en sus estrategias nacionales de ciberseguridad, capacidades de disuasión ofensiva (*deterrence by punishment*) como paquete de medidas adicionales a la defensa reactiva a fin de contener las operaciones de las ciberamenazas. En ese contexto de superación o complementación de las medidas de defensa reactivas, surge el debate de si las empresas también podrían adoptar mecanismos y procedimientos de defensa ofensiva activa que sean útiles y no contraproducentes, pero sobre todo legales y legítimos. Este ARI proporcionará los elementos para sustanciar el debate sobre esta cuestión.

Análisis

El derecho a la autodefensa de los Estados está reconocido y regulado. Se admite la posibilidad de que sus fuerzas armadas desplieguen las medidas de fuerza necesarias y proporcionadas en caso de una agresión armada. Sin embargo, la aplicación del derecho se complica cuando la agresión no es militar directa ni se realiza por Estados, caso de las agresiones llevadas a cabo por los grupos terroristas como al-Qaeda o el Estado Islámico o de amenazas hibridas en las que participan actores no estatales. En estos casos, los Estados están desarrollando sistemas de respuesta híbrida que combinan instrumentos policiales y judiciales con acciones militares, actuaciones preventivas y reactivas, ofensivas y defensivas.

Dentro de los Estados, las fuerzas de seguridad o los propios ciudadanos pueden defenderse ante violencia lesiva, directa e inminente, en circunstancias tasadas y excepcionales en la mayoría de países de nuestra tradición jurídica, aunque con algunas particularidades en el caso de EEUU. o de la cultura anglosajona. Lo hacen para ejercer el derecho a la legítima defensa, que no es otra cosa que el uso limitado –inmediato y

proporcionado– de la fuerza para evitar un daño lesivo a ejercer por un atacante que emplea la violencia contra quien se defiende o contra terceras personas. La legitimidad de la autodefensa depende de la proporcionalidad de los medios empleados, de su finalización cuando cesa el riesgo y de la falta de provocación suficiente por parte de quien se defiende. También tiene que ser en respuesta a una amenaza actual o inminente, por lo que la legítima defensa siempre es posterior a la agresión. No puede realizarse de forma premeditada ni anticipada, aunque las fuerzas y cuerpos de seguridad y los ciudadanos pueden dotarse de los instrumentos de protección que disuadan a los atacantes potenciales de cometer la agresión.

En la actualidad, las instituciones políticas gobierno de numerosos países son objetivo de ciberataques y se sospecha que algunos Estados les apoyan con su agenda desestabilizadora propia, como fue el caso de la agresión cibernética contra el Comité Nacional Demócrata en el contexto de las últimas elecciones presidenciales en EEUU en 2016. No obstante, el mayor volumen mundial de ciberataques tiene una intención económica. Ya en 2011, Paul Cornish advertía sobre la vulnerabilidad que presentan los países desarrollados a una ciberguerra económica. En el mismo sentido, el Informe Anual de Evaluación de la Ciberamenaza, OCTA) de Europol destaca que la cibercriminalidad europea tiene a las empresas como principales objetivos de sus ciberataques. Por lo tanto, se ha abierto un debate sobre si los Estados y las empresas pueden articular un derecho a la legítima ciberdefensa que incluya acciones ofensivas en defensa propia y sobre la regulación de las condiciones en las que podrían ejercerlo de forma legítima y legal.

Entre la disuasión y la defensa activa

El ciberespacio tiene peculiaridades propias que afectan a la legalidad y legitimidad de las acciones de respuesta a los ciberataques, sean de los Estados encargados de preservar la seguridad nacional como de los actores privados responsables de proteger sus intereses económicos. La mayoría de los países han establecido ya, con mayor o menor desarrollo, mandos militares de ciberdefensa, para actuar en situaciones de conflicto bélico, y agencias de ciberseguridad, para proteger el funcionamiento diario de los servicios públicos y las infraestructuras críticas. Por su parte, las empresas han desarrollado sus propios sistemas de autoprotección. El principal problema de estas adaptaciones a las realidades cibernéticas es que se intenta abordar una realidad del siglo XXI con conceptos del siglo XX y, así las cosas, las piezas no suelen encajar.

Entre otras, se puede mencionarse que la OTAN ha elaborado una doctrina específica para incorporar operaciones militares ciberofensivas en la defensa colectiva de los Estados Miembros de la Alianza Atlántica (“The Role of Offensive Cyber Operations in NATO’s Collective Defence”). Además, como vía para encontrar una capa adicional de protección de los Estados ante la tolerancia que demuestran las ciberamenazas avanzadas ante la defensa reactiva actual, tanto la ciberseguridad como la ciberdefensa de los Estados se están orientando hacia la ciberdisuasión, hacia la articulación de bases legales y de protocolos y recursos operativos que incluyan medidas tanto defensivas como ofensivas para hacer desistir a potenciales atacantes. Esa ciberdisuasión tiene capacidad para desarrollar un amplio abanico de soluciones muchas de ellas adaptadas de la disuasión propia de la realidad analógica, que van

desde la Cyber Diplomacy Toolkit de la Unión Europea. con posibilidad de aplicar sanciones a países sobre los que se pueda realizar una atribución de apoyo de ciberataques; pasando por la provisión de nuevos mecanismos legales –por ejemplo en el Congreso de EEUU– para sustanciar jurídicamente capacidades de ciberdisuasión; hasta llegar a las reflexiones en el denominado Cibersecurity Package de la Unión Europea sobre "crear una respuesta europea de ley penal y de ciberdisuasión para proteger mejor a los ciudadanos, empresas e instituciones de Europa".

No obstante, tanto la ciberdisuasión como cualquier acción ofensiva de respuesta en el ámbito cibernético se están encontrando con la dificultad de atribuir la autoría del ciberataque con la requerida precisión. Sin una clara atribución resulta difícil responder con la fuerza de sanciones, de la ley penal o con ciberataques regulados tanto por presupuestos militares como de seguridad interior. El atolladero principal de la atribución de una agresión cibernética reside en que, ante los ciberataques más graves, los agresores son por lo común actores no directamente estatales y su definición como agresores presenta contornos difusos. A veces se apoyan por Estados hostiles sin integrarse necesariamente en estructuras estatales y su adscripción a ellas requiere de complejos procesos de investigación para obtener evidencias de atribución. Además, lo más habitual es que combinen ciberataques en favor de algún Estado con ciberataques destinados a prácticas más propiamente cibercriminales, conformando amenazas híbridas. Complicando aún más el escenario, la mayoría de los ataques de esas ciberamenazas avanzadas con apoyo estatal más o menos explícito están dirigidos a los sistemas económicos de otros países, a empresas y tecnologías, sobre las que tienen objetivos de ciberespionaje o sobre las que producen un daño para servir a intereses estratégicos del país que patrocina el ciberataque.

Nuestros ordenamientos jurídicos tienen dificultades para encuadrar la *legitima ciberdefensa* frente a estas agresiones económicas dentro del campo de la defensa militar o de la defensa de la ley. Las fuerzas de seguridad utilizan la tecnología para investigar y desarticular estructuras cibercriminales y las unidades de ciberdefensa pueden contener los ciberataques, pero ninguno puede aplicar fuerza defensiva sobre el agresor. En esta situación, han tenido que abordar el mismo debate que ya tuvieron para adaptarlos a las amenazas analógicas del terrorismo y del crimen organizado. Ante amenazas tan complejas hubo que reconvertir mecanismos policiales reactivos y diseñados para la investigación *post-facto* de delitos para desarrollar dispositivos ágiles de inteligencia preventiva y prospectiva destinados no sólo a desarticular bandas terroristas y criminales sino a negarles espacio de operaciones y aumentarles el coste de sus actividades ilícitas. Para hacerlo se combinaron medidas tradicionales de seguridad defensiva y de investigación policial con procedimientos propios de los servicios de inteligencia y, en numerosos escenarios internacionales, con la combinación de la acción de capacidades militares de operaciones especiales (no es anecdótico que en Estados Unidos se compare el desarrollo que debería tener el Mando de Ciberdefensa con el que ha tenido el Mando de Operaciones Especiales del mismo país). La reflexión está más encarrilada y es más intuitiva cuando se piensa en fuerzas militares y de policía, pero ¿qué sucede en el supuesto de ciberagresiones avanzadas y persistentes a personas jurídicas, a empresas, que son las más afectadas actualmente por la plaga de ciberataques con propósitos de ciberespionaje, de lucro económico ilícito o de destrucción de datos e infraestructuras?

El hack-back

El debate en torno a la ciberdisuasión aplicable ante los ciberataques a Estados y empresas se relanzó tras el ataque global del *malware* destructivo Wannacry de 2017 (EEUU ha imputado ese ataque a Corea del Norte) y, aunque sea tímidamente, se está reflexionando sobre el derecho de los atacados a ejercer algún tipo de legítima ciberdefensa. Precisamente a raíz de Wannacry, el congresista Tom Graves propuso en la Cámara de Representantes de EEUU la Active Cyber Defense Certainty Act, un proyecto legislativo actualmente en una etapa muy temprana de discusión que pretende, en resumidas cuentas, sentar las bases legales para lo que se conoce como hack-back.

El *hack-back* (devolver el hackeo) sería la acción de utilizar la fuerza cibernética para contener el ciberataque de un agresor en un contexto de legítima ciberdefensa. Tendría por tanto paralelos con los mismos componentes que la legítima defensa personal en el terreno analógico, con la salvedad de que los defensores en este caso serían personas jurídicas y empresas. Actualmente las empresas se defienden, tienen desplegadas medidas activas y pasivas para detectar, contener, mitigar ciberataques, pero todas esas medidas son defensivas y no utilizan la fuerza contra el agresor para neutralizarlo, sino que se orienta a minimizar sus efectos. Las empresas también se están planteando la conveniencia de diseñar políticas específicas de ciberdisuasión que aumenten a los atacantes el coste de atacar a empresas.

Pero el debate sobre el *hack-back* cibernético en empresas apenas está en sus inicios y podría adoptar diversas formas de respuesta como:

- capacidades públicas de ciberseguridad encargadas de ejercer una ciberdefensa legítima mediante acciones de *hack-back* sobre ciberatacantes;

- capacidades privadas de ciberseguridad preparadas para que las empresas actúen ofensivamente de acuerdo a las condiciones legales que se establezcan; e

- incluso, como una combinación de capacidades público-privadas como ya sucede en el ámbito de la protección de infraestructuras críticas.

Respecto del *hack-back*, la mayoría de las reacciones, tanto en prensa como de profesionales, han sido de llamar a la cautela y de advertir del riesgo de que el *hack-back* pueda convertirse en un “salvaje ciber-oeste”. Estos llamamientos a la prudencia son comprensibles y siempre han acompañado al desarrollo de cibercapacidades para disuadir a atacantes mediante una represalia ofensiva, al igual que el uso de la fuerza por los Estados ha sido objeto de debate durante decenios. Entre las objeciones más frecuentes, figura la de que dejar el uso de la fuerza en manos privadas incentiva la violencia, sin contemplar que la clave es tasar y protocolizar estrictamente el ejercicio de ese derecho como en todos los supuestos reglados de legítima defensa. Por ejemplo, en países de la Unión Europea tan poco sospechosos de violencia como Finlandia o Suiza, pero con arraigada cultura de posesión de armas (45,3 y 45,7 ciudadanos armados por cada 100 habitantes, respectivamente), la legítima defensa está tan regulada como en un país mucho más restrictivo con las armas como España, y en ninguno de ellos el derecho a la legítima defensa del ciudadano combinada con el alto

porcentaje social de posesión de armas ha conducido a una incentivación de la violencia. En consecuencia, la disponibilidad de una capacidad de legítima autodefensa en las empresas no tienen por qué fomentar necesariamente la violencia si está estrictamente regulada.

Estas cuestiones se encuentran en un estado embrionario de reflexión, pero ya se han podido observar -aunque sea indirectamente- algunas manifestaciones en el terreno práctico que alertan sobre los riesgos del *hack-back*. Por ejemplo, Microsoft desarrolló en 2014 una iniciativa activa contra las botnets NJrat y NJw0rm -dos infraestructuras para diseminación masiva de *malware* (virus informáticos)- y, tras llevar a cabo una atribución equivocada sobre el origen de la amenaza, solicitó una acción legal para paralizar la infraestructura de dominios web de otra empresa, Vitalwerks Internet Solutions, sospechando que alojaba a las *botnets* distribuidoras del malware. La reacción ofensiva de Microsoft no tuvo que ver con el *hack-back*, sino con la interposición de una denuncia judicial para bloquear activos tecnológicos potencialmente dañinos de otra empresa que, posteriormente, se demostró que la empresa sospechosa no tenía relación con el ciberataque. Pero el caso ha sido suficientemente ilustrativo de la complejidad que se mencionaba respecto del factor más importante en un supuesto de legítima ciberdefensa: actuar contra quien realmente te está atacando.

En todo caso, la formalización potencial del *hack-back* requerirá mucha reflexión jurídica, al igual que precisó en su momento la legítima defensa analógica y se encontrará con numerosos obstáculos procedimentales y de técnica jurídica antes de que pueda utilizarse por las empresas dentro de un Estado de Derecho. De entre estas dificultades, sólo por mencionar un par, destacan la complejidad actual de realizar atribuciones precisas sobre el origen de un ciberataque, lo que trastoca directamente la legitimidad de una defensa por la fuerza; o el escollo de la necesaria inmediatez para que la fuerza ejercida por un defensor contra un atacante sea considerada legítima y no punible (en la mayoría de ciberataques avanzados, identificar siquiera desde dónde se realiza un ataque ya requiere un lapso bastante prolongado de tiempo, lo que compromete la inmediatez de una respuesta de fuerza que sea legítima).

Conclusiones

El mundo actual hiperconectado vive en un estado de ciber-agresión permanente. No se le denomina ciberguerra porque los contendientes no son actores directamente estatales, sino configuraciones dinámicas, cambiantes y adaptables de actores que en ocasiones sirven a intereses estratégicos, geopolíticos o económicos de algunos Estados, países que generalmente coinciden en ajustarse a su medida o ligeramente –por expresarlo con diplomacia– a lo que se consideran estándares democráticos o de comercio internacionales.

Como motivación económica de las ciberamenazas no únicamente hay que entender la monetarización que pueden obtener grupos cibercriminales a partir del diseño y diseminación de sofisticadas piezas de *malware* (como el *ransomware*), sino ciberataques avanzados que tienen propósito de ciberespionaje industrial, de destrucción de activos de datos o de distorsión de procesos en infraestructuras críticas

industriales en empresas con valor estratégico nacional o multinacional. Además del ya mencionado Wannacry, son célebres en los últimos años los ataques con las cepas de *malware* destructivo Industroyer en Ucrania en 2016 o Triton en 2017 sobre Oriente Medio, ambos contra infraestructuras energéticas. Estos incidentes sugieren que una porción muy relevante de las agresiones globales por parte de ciberamenazas avanzadas se despliega en un claro vector de ciberguerra económica, una ciberguerra que ya no respeta las habituales reglas de la guerra analógica: ni es declarada formalmente, ni es directamente atribuible a un Estado (aunque la patrocine), ni encaja en paradigmas tradicionales de reglas de enfrentamiento o de definiciones de combatiente.

Esta realidad híbrida está provocando una carrera acelerada por producir nuevos conceptos de seguridad y defensa que no sean meras adaptaciones sobrevenidas de marcos doctrinales analógicos, forzados a encajar sin lograrlo en realidades que desbordan las definiciones tradicionales. Entre estos nuevos conceptos podría estar el derecho a la legítima ciberdefensa por parte del conjunto de victimización más perjudicado por la ciberguerra económica: el colectivo de empresas estratégicas y de infraestructuras críticas. No obstante, no será suficiente desarrollar un nuevo concepto, sino que su eventual desarrollo –que aún está por ver– implicará nuevas nociones de técnica jurídica combinadas con protocolos muy estudiados de tácticas, procedimientos y tecnologías para asegurar que una respuesta de fuerza cibernética por parte de una empresa agredida es necesaria, proporcional, oportuna y sin intención de producir daño, es decir, legítima.